Introduction aux bases de Gröbner, complexité et application à la cryptographie

École de printemps, Journées C2 2014

Magali Bardet

Laboratoire LITIS - Université de Rouen
Équipe C&A

17-18 mars 2014

Plan

Références

- D. Cox, J. Little, and D. O'Shea. Ideals, Varieties, and Algorithms. 2008 (3ème édition).
- A. Joux, Algorithmic Cryptanalysis. 2009

Système d'équations algébriques

Notations

- $\mathbb{K}$ un corps, $x_1, \ldots, x_n$ des variables,

Système d'équations algébriques

Notations

- $\mathbb{K}$ un corps, $x_1, \ldots, x_n$ des variables,
- $\mathbb{K}[x_1, \ldots, x_n]$ l'anneau des polynômes en n variables.

Système d'équations algébriques

Notations

- $\mathbb{K}$ un corps, $x_1, \ldots, x_n$ des variables,
- $\mathbb{K}[x_1, \ldots, x_n]$ l'anneau des polynômes en n variables.
- un monôme : $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ avec $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$

Système d'équations algébriques

Notations

- $\mathbb{K}$ un corps, $x_1, \ldots, x_n$ des variables,
- $\mathbb{K}[x_1, \ldots, x_n]$ l'anneau des polynômes en n variables.
- un monôme : $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ avec $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$
- un terme : $c \cdot x^\alpha$ où x^α est un monôme, $c \in \mathbb{K}$ non nul.

Système d'équations algébriques

Notations

- $\mathbb{K}$ un corps, $x_1, \ldots, x_n$ des variables,
- $\mathbb{K}[x_1, \ldots, x_n]$ l'anneau des polynômes en n variables.
- un monôme : $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ avec $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$
- un terme : $c \cdot x^\alpha$ où x^α est un monôme, $c \in \mathbb{K}$ non nul.
- un polynôme :

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$$

avec $c_\alpha \in \mathbb{K}$ (un nombre fini non nuls).

Système d'équations algébriques

Notations

- $\mathbb{K}$ un corps, $x_1, \ldots, x_n$ des variables,
- $\mathbb{K}[x_1, \ldots, x_n]$ l'anneau des polynômes en n variables.
- un monôme : $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ avec $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$
- un terme : $c \cdot x^\alpha$ où x^α est un monôme, $c \in \mathbb{K}$ non nul.
- un polynôme :
$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$$
avec $c_\alpha \in \mathbb{K}$ (un nombre fini non nuls).
- le degré
$$\begin{cases} \deg(x^\alpha) = |\alpha| = \sum_{i=1}^n \alpha_i & \text{si } \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \\ \deg(f) = \max_{c_\alpha \neq 0}(\deg(c_\alpha x^\alpha)) \end{cases}$$

Système d'équations algébriques

Système d'équations algébriques

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

où $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ est un corps dans lequel on sait calculer (par exemple $\mathbb{Q}$, ou un corps fini $\mathbb{F}_q$).

Système d'équations algébriques

Système d'équations algébriques

$$\begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases}$$

où $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ est un corps dans lequel on sait calculer (par exemple $\mathbb{Q}$, ou un corps fini $\mathbb{F}_q$).

Résoudre sur un domaine $\mathbb{D} \supset \mathbb{K}$

C'est trouver l'ensemble n-uplets de $\mathbb{D}^n$ qui annulent tous les polynômes $f_1, \ldots, f_m$.

Systèmes algébriques et cryptographie

C. Shannon « Communication Theory of Secrecy Systems » 1949

Thus, if we could show that solving a certain system requires at least as much work as solving a system of simultaneous equations in a large number of unknowns, of a complex type, then we would have a lower bound of sorts for the work characteristic.

Systèmes algébriques et cryptographie

C. Shannon « Communication Theory of Secrecy Systems » 1949

Thus, if we could show that solving a certain system requires at least as much work as solving a system of simultaneous equations in a large number of unknowns, of a complex type, then we would have a lower bound of sorts for the work characteristic.

Modélisation algébrique

- algorithme de chiffrement symétrique par bloc (e.g. DES)

$$Enc : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

- sur $\mathbb{F}_q^n$, toute fonction est polynomiale !
- Cryptosystème à clef publique de McEliece : système d'équations dont la clef privée est solution.

Systèmes algébriques et cryptographie

Intérêt de la modélisation algébrique

- attaque à (clair, chiffré) connu : la clef secrète est solution ;
- si résoudre est difficile, peut-on l'utiliser pour construire une fonction à sens unique (à trappe) ?

Systèmes algébriques et cryptographie

Intérêt de la modélisation algébrique

- attaque à (clair, chiffré) connu : la clef secrète est solution ;
- si résoudre est difficile, peut-on l'utiliser pour construire une fonction à sens unique (à trappe) ?

Problèmatique de la modélisation

- y a-t-il au moins une solution au système ? un nombre fini ? infini ?
- y a-t-il beaucoup de solutions parasites ?
- quelle est la complexité de la résolution d'un système d'équations algébriques ?
- et sur corps fini ? avec plus d'équations que de variables ?
- impact des différentes modélisations possibles ?

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : 10 équations, 10 variables, degré 2, degré secret 3.

$$\begin{cases}
x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_1x_8 + x_2x_3 + x_2x_6 + x_3x_5 + x_3x_7 + x_3x_8 + x_3x_{10} + x_3 + x_4x_7 + x_4 \\
x_1x_3 + x_1x_5 + x_1x_7 + x_1x_8 + x_1x_9 + x_2x_5 + x_2x_9 + x_2x_{10} + x_2 + x_3x_4 + x_3x_5 + x_3x_6 + x_3x_7 + x_3 \\
x_1x_2 + x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 + x_1x_8 + x_1x_9 + x_2x_5 + x_2x_6 + x_2x_8 + x_2x_9 + x_2x_{10} + x_2 + x_3 \\
x_1x_3 + x_1x_4 + x_1x_6 + x_1x_9 + x_1x_{10} + x_2x_4 + x_2x_6 + x_2x_8 + x_2x_{10} + x_3x_5 + x_3x_6 + x_3x_8 + x_3x_{10} \\
x_1x_2 + x_1x_4 + x_1x_6 + x_1x_8 + x_1x_9 + x_2x_3 + x_2x_4 + x_2x_9 + x_2 + x_3x_5 + x_3x_6 + x_3x_7 + x_3x_8 + x_3 \\
x_1x_2 + x_1x_4 + x_1x_5 + x_1x_8 + x_1x_9 + x_2x_3 + x_2x_4 + x_2x_9 + x_2 + x_3x_4 + x_3x_5 + x_3x_6 + x_3x_7 + x_3 \\
x_1x_3 + x_1x_5 + x_1x_6 + x_1x_{10} + x_2x_4 + x_2x_8 + x_2x_9 + x_3x_6 + x_3x_8 + x_4x_5 + x_4x_7 + x_4x_9 + x_5x_8 + \\
x_1x_2 + x_1x_4 + x_1x_5 + x_1 + x_2x_7 + x_2x_8 + x_2x_9 + x_2x_{10} + x_3x_8 + x_3x_{10} + x_4x_5 + x_4x_6 + x_4x_7 + x_4 \\
x_1x_2 + x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 + x_1x_8 + x_1 + x_2x_4 + x_2x_7 + x_2x_8 + x_2x_{10} + x_3x_4 + x_3x_5 + x_3 \\
x_1x_2 + x_1x_7 + x_1x_9 + x_1 + x_2x_5 + x_2x_8 + x_2x_9 + x_2 + x_3x_7 + x_3x_8 + x_3x_9 + x_4x_5 + x_4x_6 + x_4x_8 +
\end{cases}$$

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2
- attaquer : résoudre $c_1 = f_1(\mathbf{x}),\ldots,c_m = f_m(\mathbf{x})$
- clef secrète : un système facile à résoudre et une "transformation".

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2
- attaquer : résoudre $c_1 = f_1(\mathbf{x}),\ldots,c_m = f_m(\mathbf{x})$
- clef secrète : un système facile à résoudre et une "transformation".

Sécurité ?

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2
- attaquer : résoudre $c_1 = f_1(\mathbf{x}),\ldots,c_m = f_m(\mathbf{x})$
- clef secrète : un système facile à résoudre et une "transformation".

Sécurité ? Au moins 80 variables pour une sécurité en 2^{80}

Classes de complexité de problèmes algébriques

Problème `Ideal MemberShip (IM)`

Entrée : $f, f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$
Question : existe-t-il $q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n]$ tq $f = \sum_{i=1}^{m} q_i f_i$?

Classes de complexité de problèmes algébriques

Problème `Ideal MemberShip (IM)`

Entrée : $f, f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$
Question : existe-t-il $q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n]$ tq $f = \sum_{i=1}^{m} q_i f_i$?

Théorème (Mayr and Meyer, 82, 89)

IM est EXPSPACE-complet.

Classes de complexité de problèmes algébriques

Problème Ideal MemberShip (IM)

Entrée : $f, f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$
Question : existe-t-il $q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n]$ tq $f = \sum_{i=1}^{m} q_i f_i$?

Théorème (Mayr and Meyer, 82, 89)

IM est EXPSPACE-complet.

Rappels sur les classes de complexité

$$\mathtt{P} \subset \mathtt{NP} \subset \mathtt{PSPACE} = \mathtt{NPSPACE} \subset \mathtt{DEXPTIME} \subset \mathtt{EXPSPACE}$$

Classes de complexité de problèmes algébriques

IM est EXPSPACE-complet

- Mayr and Meyer, « The complexity of the word problems for commutative semigroups and polynomial ideals », 1982.
  $\rightarrow$ IM est EXPSPACE-dur.

Classes de complexité de problèmes algébriques

IM est EXPSPACE-complet

- Mayr and Meyer, « The complexity of the word problems for commutative semigroups and polynomial ideals », 1982. $\rightarrow$ IM est EXPSPACE-dur.
- Mayr, « Membership in polynomial ideals over Q is exponential space complete », 1989. $\rightarrow$ IM est EXPSPACE.

Classes de complexité de problèmes algébriques

IM est EXPSPACE-complet

- Mayr and Meyer, « The complexity of the word problems for commutative semigroups and polynomial ideals », 1982. $\rightarrow$ IM est EXPSPACE-dur.
- Mayr, « Membership in polynomial ideals over Q is exponential space complete », 1989. $\rightarrow$ IM est EXPSPACE.
- Pire cas : complexité doublement exponentielle en la taille de l'entrée ($\mathbb{K}$ infini) ;

Classes de complexité de problèmes algébriques

IM est EXPSPACE-complet

- Mayr and Meyer, « The complexity of the word problems for commutative semigroups and polynomial ideals », 1982. $\rightarrow$ IM est EXPSPACE-dur.
- Mayr, « Membership in polynomial ideals over Q is exponential space complete », 1989. $\rightarrow$ IM est EXPSPACE.
- Pire cas : complexité doublement exponentielle en la taille de l'entrée ($\mathbb{K}$ infini) ;

Classes de complexité de problèmes algébriques

IM est EXPSPACE-complet

- Mayr and Meyer, « The complexity of the word problems for commutative semigroups and polynomial ideals », 1982. $\rightarrow$ IM est EXPSPACE-dur.
- Mayr, « Membership in polynomial ideals over Q is exponential space complete », 1989. $\rightarrow$ IM est EXPSPACE.
- Pire cas : complexité doublement exponentielle en la taille de l'entrée ($\mathbb{K}$ infini) ;

Nombre fini de solutions (y compris à l'infini)

- Lazard 1983, Giusti 1984 : simplement exponentiel (pire cas, à changement près de coordonnées).
- cas particulier des solutions dans $\mathbb{F}_q$: pire cas simplement exponentielle ! (recherche exhaustive)

Classes de complexité de problèmes algébriques

Cas particulier : $f = 1$, y a-t-il une solution ?

Classes de complexité de problèmes algébriques

Cas particulier : $f = 1$, y a-t-il une solution ?

Problème `Hilbert's Nullstellensatz` (HM) sur $\mathbb{F}_q$

Entrée : $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$
Question : le système $f_1 = 0, \ldots, f_m = 0$ a-t-il une solution $\in \mathbb{F}_q^n$?

HM_d la restriction de HM à des polynômes f_i de degré au plus d.

Classes de complexité de problèmes algébriques

Cas particulier : $f = 1$, y a-t-il une solution ?

Problème `Hilbert's Nullstellensatz` (HM) sur $\mathbb{F}_q$

Entrée : $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$
Question : le système $f_1 = 0, \ldots, f_m = 0$ a-t-il une solution $\in \mathbb{F}_q^n$?

HM_d la restriction de HM à des polynômes f_i de degré au plus d.

Théorème

HM est NP-complet.
HM_2 est également NP-complet.

Deux approches cryptographiques

Cryptanalyse algébrique

- modélisation (système algébrique dont un secret est solution) ;
- analyse de la complexité de résolution du système ;
- ajustement des paramètres cryptographiques.

Conception de cryptosystèmes

En utilisant les *instances difficiles* d'un problème NP-complet.

Deux approches cryptographiques

Cryptanalyse algébrique

- modélisation (système algébrique dont un secret est solution) ;
- analyse de la complexité de résolution du système ;
- ajustement des paramètres cryptographiques.

Conception de cryptosystèmes

En utilisant les *instances difficiles* d'un problème NP-complet.

Les besoins

- effectivité de la résolution de systèmes algébriques (algorithmes) ;
- complexité du problème (cas générique, cas particuliers) ;

Système d'équations algébriques

Système d'équations algébriques

$$\begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases}$$

où $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ un corps.

Système d'équations algébriques

Système d'équations algébriques

$$\begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases}$$

où $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ un corps.

Cas simples

- les f_i sont de degré 1 : système d'équations linéaires.

Système d'équations algébriques

Système d'équations algébriques

$$\begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases}$$

où $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ un corps.

Cas simples

- les f_i sont de degré 1 : système d'équations linéaires.
- $n = 1$, système de polynômes en une variable.

Cas simple : les systèmes d'équations linéaires

Résolution : écriture sous forme matricielle

$$\begin{array}{llll} (x_1 > & x_2 > & \cdots > x_n & > 1) \\ c_{1,1}x_1 + & c_{1,2}x_2 + \ldots + & c_{1,n}x_n + & c_{1,n+1} \\ & \vdots & & \\ c_{n,1}x_1 + & c_{n,2}x_2 + \ldots + & c_{n,n}x_n + & c_{n,n+1} \end{array}$$

Cas simple : les systèmes d'équations linéaires

Résolution : écriture sous forme matricielle

$$[A|b] = \begin{pmatrix} (x_1 > & x_2 > & \cdots > x_n & > 1) \\ c_{1,1} & c_{1,2} & \cdots & c_{1,n} & c_{1,n+1} \\ & & \vdots & & \\ c_{n,1} & c_{n,2} & \cdots & c_{n,n} & c_{n,n+1} \end{pmatrix}$$

Cas simple : les systèmes d'équations linéaires

Résolution : écriture sous forme matricielle

$$[A|b] = \left(\begin{array}{cccc} (x_1 > & x_2 > & \cdots > x_n & > 1) \\ c_{1,1} & c_{1,2} & \cdots & c_{1,n} \quad c_{1,n+1} \\ & \vdots & & \\ c_{n,1} & c_{n,2} & \cdots & c_{n,n} \quad c_{n,n+1} \end{array}\right)$$

Espace des solutions

- aucune solution
- ou l'ensemble des solutions forme un sous-espace vectoriel affine de $\mathbb{K}^n$ de dimension $n - \text{rang}(A)$.

Systèmes linéaires vs systèmes polynomiaux

	Système linéaire	Système polynomial
objet	espace vectoriel $V = \mathrm{Vect}_{\mathbb{K}}(f_1, \ldots, f_m)$	Idéal $I = \langle f_1, \ldots, f_m \rangle$
solutions	sous-espace vectoriel de $\mathbb{K}^n$	variété algébrique de $\mathbb{K}^n$
algorithme	base triangulaire de V	base de Gröbner de I

Systèmes linéaires vs systèmes polynomiaux

	Système linéaire	Système polynomial
objet	espace vectoriel $V = \mathrm{Vect}_{\mathbb{K}}(f_1, \ldots, f_m)$	Idéal $I = \langle f_1, \ldots, f_m \rangle$
solutions	sous-espace vectoriel de $\mathbb{K}^n$	variété algébrique de $\mathbb{K}^n$
algorithme	base triangulaire de V	base de Gröbner de I

- idéal, variété algébrique ;
- ordre sur les monômes.

Idéaux, Variétés

Idéal associé à un système d'équations $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$

$$I(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle = \left\{ \sum_{k=1}^{m} g_k \cdot f_k : g_k \in \mathbb{K}[x_1, \ldots, x_n] \right\}$$

C'est le plus petit idéal de $\mathbb{K}[x_1, \ldots, x_n]$ contenant les f_i.

Idéaux, Variétés

Idéal associé à un système d'équations $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$

$$I(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle = \left\{ \sum_{k=1}^{m} g_k \cdot f_k : g_k \in \mathbb{K}[x_1, \ldots, x_n] \right\}$$

C'est le plus petit idéal de $\mathbb{K}[x_1, \ldots, x_n]$ contenant les f_i.

Variété algébrique associée à un idéal I sur un corps $\mathbb{D} \supset \mathbb{K}$

$$\mathscr{V}_{\mathbb{D}}(I) = \{(a_1, \ldots, a_n) \in \mathbb{D}^n : f(a_1, \ldots, a_n) = 0 \; \forall f \in I\}$$

Idéaux, Variétés

Idéal associé à un système d'équations $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$

$$I(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle = \left\{ \sum_{k=1}^{m} g_k \cdot f_k : g_k \in \mathbb{K}[x_1, \ldots, x_n] \right\}$$

C'est le plus petit idéal de $\mathbb{K}[x_1, \ldots, x_n]$ contenant les f_i.

Variété algébrique associée à un idéal I sur un corps $\mathbb{D} \supset \mathbb{K}$

$$\mathscr{V}_{\mathbb{D}}(I) = \{(a_1, \ldots, a_n) \in \mathbb{D}^n : f(a_1, \ldots, a_n) = 0 \; \forall f \in I\}$$

Idéal associé à un sous-ensemble $V \subset \mathbb{K}^n$

$$\mathscr{I}(V) = \{g \in \mathbb{K}[x_1, \ldots, x_n] : \; g(a) = 0 \text{ pour tout } a \in V\}$$

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,

$$I = \langle x^6 + x^5 + x^4 + x^2 + x + 1, x^5 - x^4 + x - 1 \rangle = \langle x^4 + 1 \rangle$$

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,
- division euclidienne entre polynômes : unicité quotient/reste ;

$$I = \langle x^6 + x^5 + x^4 + x^2 + x + 1, x^5 - x^4 + x - 1 \rangle = \langle x^4 + 1 \rangle$$
$$(f_1 = (x+2)f_2 + 3(x^4+1) \text{ et } f_2 = (x-1)(x^4+1))$$

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,
- division euclidienne entre polynômes : unicité quotient/reste ;
- les monômes sont triés par ordre décroissant de degré ;

$$I = \langle x^6 + x^5 + x^4 + x^2 + x + 1, x^5 - x^4 + x - 1 \rangle = \langle x^4 + 1 \rangle$$

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,
- division euclidienne entre polynômes : unicité quotient/reste ;
- les monômes sont triés par ordre décroissant de degré ;

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,
- division euclidienne entre polynômes : unicité quotient/reste ;
- les monômes sont triés par ordre décroissant de degré ;

Espace des solutions

- l'ensemble des solutions du système est l'ensemble des racines du polynôme $f(x)$;

---

a. comptées avec multiplicité

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,
- division euclidienne entre polynômes : unicité quotient/reste ;
- les monômes sont triés par ordre décroissant de degré ;

Espace des solutions

- l'ensemble des solutions du système est l'ensemble des racines du polynôme $f(x)$;
- il y en a $\deg(f)$ dans $\overline{\mathbb{K}}$;[a]

a. comptées avec multiplicité

Cas simple : système de polynômes en une variable

Résolution $I = \langle f_1, \ldots, f_m \rangle = \langle f(x) \rangle \subset \mathbb{K}[x]$

- tout idéal propre de $\mathbb{K}[x]$ est principal,
- division euclidienne entre polynômes : unicité quotient/reste ;
- les monômes sont triés par ordre décroissant de degré ;

Espace des solutions

- l'ensemble des solutions du système est l'ensemble des racines du polynôme $f(x)$;
- il y en a $\deg(f)$ dans $\overline{\mathbb{K}}$; [a]
- il y en a un nombre indéterminé dans $\mathbb{D} \subsetneq \overline{\mathbb{K}}$ (entre 0 et $\deg(f)$) ;

a. comptées avec multiplicité

Exemple

$$I = \langle x^4 + 1 \rangle$$

On a alors :

- $\mathscr{V}_{\mathbb{C}}(I) = \left\{ e^{k \cdot i \cdot \frac{\Pi}{4}}, k \in \{1,3,5,7\} \right\}$

Exemple

$$I = \langle x^4 + 1 \rangle$$

On a alors :

- $\mathscr{V}_{\mathbb{C}}(I) = \left\{ e^{k \cdot i \cdot \frac{\Pi}{4}}, k \in \{1,3,5,7\} \right\}$
- $\mathscr{V}_{\mathbb{R}}(I) = \emptyset$

Exemple

$$I = \langle x^4 + 1 \rangle$$

On a alors :

- $\mathscr{V}_{\mathbb{F}_2}(I) = \{1\}$
- $\mathscr{V}_{\overline{\mathbb{F}_2}}(I) = \{1\}$

Exemple

$$I = \langle x^4 + 1 \rangle$$

On a alors :

- $\mathscr{V}_{\mathbb{F}_2}(I) = \{1\}$
- $\mathscr{V}_{\overline{\mathbb{F}_2}}(I) = \{1\}$

Variété $\neq$ Idéal

Un idéal contient plus d'information qu'une variété : sur $\mathbb{F}_2$, $x^4 + 1 = (x+1)^4$.

- $I = \langle x^4 + 1 \rangle$, $\mathscr{V}_{\overline{\mathbb{F}_2}}(I) = \{1\}$
- $I_1 = \langle x + 1 \rangle \neq I$, $\mathscr{V}_{\overline{\mathbb{F}_2}}(I_1) = \{1\} = \mathscr{V}_{\overline{\mathbb{F}_2}}(I) = \{1\}$

Lorsqu'on passe à la variété, on pert la notion de multiplicité.

Système d'équations algébriques

Domaines de résolution possibles $\mathbb{D} \supset \mathbb{K}$

- $\mathbb{D} = \overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$
  (par exemple, $\mathbb{D} = \mathbb{C}$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{D} = \overline{\mathbb{Q}}$ pour $\mathbb{K} = \mathbb{Q}$)

Système d'équations algébriques

Domaines de résolution possibles $\mathbb{D} \supset \mathbb{K}$

- $\mathbb{D} = \overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$
  (par exemple, $\mathbb{D} = \mathbb{C}$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{D} = \overline{\mathbb{Q}}$ pour $\mathbb{K} = \mathbb{Q}$)
- $\mathbb{D} = \mathbb{R}$ géométrie réelle, problème non algébrique !

Système d'équations algébriques

Domaines de résolution possibles $\mathbb{D} \supset \mathbb{K}$

- $\mathbb{D} = \overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$
  (par exemple, $\mathbb{D} = \mathbb{C}$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{D} = \overline{\mathbb{Q}}$ pour $\mathbb{K} = \mathbb{Q}$)
- $\mathbb{D} = \mathbb{R}$ géométrie réelle, problème non algébrique !
- $\mathbb{D} = \mathbb{Q}$ est un problème indécidable (cf. équation de Fermat $x^n + y^n = 1$, nombre fini de solutions dans $\mathbb{Q}$).

Système d'équations algébriques

Domaines de résolution possibles $\mathbb{D} \supset \mathbb{K}$

- $\mathbb{D} = \overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$
  (par exemple, $\mathbb{D} = \mathbb{C}$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{D} = \overline{\mathbb{Q}}$ pour $\mathbb{K} = \mathbb{Q}$)
- $\mathbb{D} = \mathbb{R}$ géométrie réelle, problème non algébrique !
- $\mathbb{D} = \mathbb{Q}$ est un problème indécidable (cf. équation de Fermat $x^n + y^n = 1$, nombre fini de solutions dans $\mathbb{Q}$).
- si $\mathbb{K} = \mathbb{F}_q$ et $\mathbb{D} = \mathbb{F}_{q^i}$, on ajoute les équations de corps

$$\left\{ x_1^{q^i} - x_1, \ldots, x_n^{q^i} - x_n \right\}$$

Nombre nécessairement fini de solutions (au plus q^{in})

Exemple de système

On cherche les solutions sur $\mathbb{F}_2$:

$$\begin{cases} x_1x_2 + x_1x_4 + x_2x_4 + x_3 + x_4 + 1 & = & 0 \\ x_2x_3 + x_2x_4 + x_1 + x_4 & = & 0 \\ x_1x_2 + x_1x_3 + x_1x_4 + x_1 + x_2 + x_3 + 1 & = & 0 \\ x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 + x_1 + x_3 + x_4 + 1 & = & 0 \end{cases}$$

Exemple de système

On cherche les solutions sur $\mathbb{F}_2$:

$$\begin{cases} x_1x_2 + x_3 + 1 = 0 \\ x_2x_3 + x_1 = 0 \\ x_1x_2 + x_1x_3 + x_1 + x_2 + x_3 + 1 = 0 \\ x_1x_3 + x_1 + x_3 + 1 = 0 \end{cases}$$

$x_4 = 0$

Exemple de système

On cherche les solutions sur $\mathbb{F}_2$:

$$\begin{cases} x_1x_2 + x_3 + 1 = 0 \\ x_2x_3 + x_1 = 0 \\ x_1x_2 + x_1x_3 + x_1 + x_2 + x_3 + 1 = 0 \\ x_1x_3 + x_1 + x_3 + 1 = 0 \end{cases}$$

$x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 0$

Exemple de système

On cherche les solutions sur $\mathbb{F}_2$:

$$\begin{cases} x_1x_2 + x_1 + x_2 + x_3 = 0 \\ x_2x_3 + x_2 + x_1 + 1 = 0 \\ x_1x_2 + x_1x_3 + x_1 + x_1 + x_2 + x_3 + 1 = 0 \\ x_1x_3 + x_1 + x_2 + x_3 + x_1 + x_3 = 0 \end{cases}$$

$x_4 = 1$

Exemple de système

On cherche les solutions sur $\mathbb{F}_2$:

$$\begin{cases} x_1x_2 + x_1 + x_2 + x_3 = 0 \\ x_2x_3 + x_2 + x_1 + 1 = 0 \\ x_1x_2 + x_1x_3 + x_1 + x_1 + x_2 + x_3 + 1 = 0 \\ x_1x_3 + x_1 + x_2 + x_3 + x_1 + x_3 = 0 \end{cases}$$

$x_4 = 1$ pas de solution.

Hilbert Nullstellensatz

Théorème des zéros de Hilbert

Soit $\mathbb{K}$ un corps, $\overline{\mathbb{K}}$ sa clôture algébrique, $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_m \rangle$. Alors

1. $\mathscr{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ si et seulement si $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Hilbert Nullstellensatz

Théorème des zéros de Hilbert

Soit $\mathbb{K}$ un corps, $\overline{\mathbb{K}}$ sa clôture algébrique, $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_m \rangle$. Alors

1. $\mathscr{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ si et seulement si $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$
2. $\mathscr{I}(\mathscr{V}_{\overline{\mathbb{K}}}(I)) = \sqrt{I} = \{f \in \mathbb{K}[x_1, \ldots, x_n] : \exists \alpha \in \mathbb{N}^*, f^\alpha \in I\}$ le radical de I

Hilbert Nullstellensatz

Théorème des zéros de Hilbert

Soit $\mathbb{K}$ un corps, $\overline{\mathbb{K}}$ sa clôture algébrique, $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_m \rangle$. Alors

1. $\mathscr{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ si et seulement si $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$
2. $\mathscr{I}(\mathscr{V}_{\overline{\mathbb{K}}}(I)) = \sqrt{I} = \{f \in \mathbb{K}[x_1, \ldots, x_n] : \exists \alpha \in \mathbb{N}^*, f^\alpha \in I\}$ le radical de I

Hilbert Nullstellensatz

Théorème des zéros de Hilbert

Soit $\mathbb{K}$ un corps, $\overline{\mathbb{K}}$ sa clôture algébrique, $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_m \rangle$. Alors

1. $\mathscr{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ si et seulement si $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$
2. $\mathscr{I}(\mathscr{V}_{\overline{\mathbb{K}}}(I)) = \sqrt{I} = \{f \in \mathbb{K}[x_1, \ldots, x_n] : \exists \alpha \in \mathbb{N}^*, f^\alpha \in I\}$ le radical de I

Sur un corps fini $\mathbb{F}_q$

$I = \langle f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$ est radical, $\mathscr{V}_{\mathbb{F}_q}(I) = \mathscr{V}_{\overline{\mathbb{F}_q}}(I)$ est fini.

Weak Nullstellensatz

Preuve [1]

$\mathscr{V}_{\mathbb{K}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.

Weak Nullstellensatz

Preuve [1]

$\mathscr{V}_{\mathbb{K}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.
Pour $n = 1$, $I = \langle f(x) \rangle$ avec f unitaire implique $f = 1$ *car* $\overline{\mathbb{K}}$ *est algébriquement clos*.

Weak Nullstellensatz

Preuve 1

$\mathcal{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.
Pour $n = 1$, $I = \langle f(x) \rangle$ avec f unitaire implique $f = 1$ *car* $\overline{\mathbb{K}}$ *est algébriquement clos*.
Supposons le théorème vrai pour $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Soit $f \in I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ de degré d.

Weak Nullstellensatz

Preuve 1

$\mathcal{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.
Pour $n = 1$, $I = \langle f(x) \rangle$ avec f unitaire implique $f = 1$ *car* $\overline{\mathbb{K}}$ *est algébriquement clos*.
Supposons le théorème vrai pour $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Soit $f \in I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ de degré d.

- À changement de variable près (possible car $\overline{\mathbb{K}}$ infini), on peut écrire $f(x_1, \ldots, x_n) = x_n^d +$ termes de plus petit degré en x_n.

Weak Nullstellensatz

Preuve 1

$\mathcal{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.
Pour $n = 1$, $I = \langle f(x) \rangle$ avec f unitaire implique $f = 1$ *car* $\overline{\mathbb{K}}$ *est algébriquement clos*.
Supposons le théorème vrai pour $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Soit $f \in I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ de degré d.

- À changement de variable près (possible car $\overline{\mathbb{K}}$ infini), on peut écrire $f(x_1, \ldots, x_n) = x_n^d +$ termes de plus petit degré en x_n.
- $J = I \cap \overline{\mathbb{K}}[x_1, \ldots, x_{n-1}]$ est un idéal de $\overline{\mathbb{K}}[x_1, \ldots, x_{n-1}]$,

Weak Nullstellensatz

Preuve [1]

$\mathcal{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.
Pour $n = 1$, $I = \langle f(x) \rangle$ avec f unitaire implique $f = 1$ *car* $\overline{\mathbb{K}}$ *est algébriquement clos*.
Supposons le théorème vrai pour $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Soit $f \in I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ de degré d.

- À changement de variable près (possible car $\overline{\mathbb{K}}$ infini), on peut écrire $f(x_1, \ldots, x_n) = x_n^d +$ termes de plus petit degré en x_n.
- $J = I \cap \overline{\mathbb{K}}[x_1, \ldots, x_{n-1}]$ est un idéal de $\overline{\mathbb{K}}[x_1, \ldots, x_{n-1}]$,
- $V_{\overline{\mathbb{K}}}(J) = \emptyset$ puisque c'est la projection de $V_{\overline{\mathbb{K}}}(I)$ sur les dernières coordonnées et que toute solution devrait s'étendre.

Weak Nullstellensatz

Preuve 1

$\mathcal{V}_{\overline{\mathbb{K}}}(I) = \emptyset$ implique $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$

Par récurrence sur n.
Pour $n = 1$, $I = \langle f(x) \rangle$ avec f unitaire implique $f = 1$ *car* $\overline{\mathbb{K}}$ *est algébriquement clos*.
Supposons le théorème vrai pour $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Soit $f \in I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ de degré d.

- À changement de variable près (possible car $\overline{\mathbb{K}}$ infini), on peut écrire $f(x_1, \ldots, x_n) = x_n^d +$ termes de plus petit degré en x_n.
- $J = I \cap \overline{\mathbb{K}}[x_1, \ldots, x_{n-1}]$ est un idéal de $\overline{\mathbb{K}}[x_1, \ldots, x_{n-1}]$,
- $V_{\overline{\mathbb{K}}}(J) = \emptyset$ puisque c'est la projection de $V_{\overline{\mathbb{K}}}(I)$ sur les dernières coordonnées et que toute solution devrait s'étendre.
- par récurrence, $1 \in J \subset I$.

Strong Nullstellensatz

Preuve 2

$\mathscr{I}(\mathscr{V}_{\overline{\mathbb{K}}}(I)) \subset \sqrt{I}$

Soit $f \in \mathbb{K}[x_1, \ldots, x_n]$ qui s'annule sur toutes les solutions communes de $f_1, \ldots, f_m$ dans $\overline{\mathbb{K}}$. Posons $\tilde{I} = \langle f_1, \ldots, f_m, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$.

- Si $f_1(a) = 0, \ldots, f_m(a) = 0$ alors par hypothèse $f(a) = 0$ et donc $1 - yf(a) = 1$ pour toute valeur de y, donc $\mathscr{V}(\tilde{I}) = \emptyset$.

Strong Nullstellensatz

Preuve 2

$\mathscr{I}(\mathscr{V}_{\mathbb{K}}(I)) \subset \sqrt{I}$

Soit $f \in \mathbb{K}[x_1, \ldots, x_n]$ qui s'annule sur toutes les solutions communes de $f_1, \ldots, f_m$ dans $\overline{\mathbb{K}}$. Posons $\tilde{I} = \langle f_1, \ldots, f_m, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$.

- Si $f_1(a) = 0, \ldots, f_m(a) = 0$ alors par hypothèse $f(a) = 0$ et donc $1 - yf(a) = 1$ pour toute valeur de y, donc $\mathscr{V}(\tilde{I}) = \emptyset$.
- D'après le Weak Nullstellensatz, $1 \in \langle f_1, \ldots, f_m, 1 - yf \rangle$ donc

$$1 = \sum_{i=1}^{m} g_i(x_1, \ldots, x_n, y) f_i + g_{m+1}(x_1, \ldots, x_n, y)(1 - yf)$$

Strong Nullstellensatz

Preuve 2

$\mathscr{I}(\mathscr{V}_{\mathbb{K}}(I)) \subset \sqrt{I}$

Soit $f \in \mathbb{K}[x_1, \ldots, x_n]$ qui s'annule sur toutes les solutions communes de $f_1, \ldots, f_m$ dans $\overline{\mathbb{K}}$. Posons $\tilde{I} = \langle f_1, \ldots, f_m, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$.

- Si $f_1(a) = 0, \ldots, f_m(a) = 0$ alors par hypothèse $f(a) = 0$ et donc $1 - yf(a) = 1$ pour toute valeur de y, donc $\mathscr{V}(\tilde{I}) = \emptyset$.
- D'après le Weak Nullstellensatz, $1 \in \langle f_1, \ldots, f_m, 1 - yf \rangle$ donc

$$1 = \sum_{i=1}^{m} g_i(x_1, \ldots, x_n, y) f_i + g_{m+1}(x_1, \ldots, x_n, y)(1 - yf)$$

- En prenant $y = 1/f$ et en multipliant par f^α, on obtient $f^\alpha = \sum_{i=1}^{m} \tilde{g}_i(x_1, \ldots, x_n) f_i \in I$.

Les ordres monomiaux

Ordre monomial admissible

C'est un ordre total $<$ sur les monômes de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :

1. pour tout triplet de monômes m_1, m_2, m_3 alors

$$m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$$

Les ordres monomiaux

Ordre monomial admissible

C'est un ordre total $<$ sur les monômes de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :

1. pour tout triplet de monômes m_1, m_2, m_3 alors

$$m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$$

2. pour tout monôme m, $1 < m$.

Les ordres monomiaux

Ordre monomial admissible

C'est un ordre total $<$ sur les monômes de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :

1. pour tout triplet de monômes m_1, m_2, m_3 alors

$$m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$$

2. pour tout monôme m, $1 < m$.

2'. tout ensemble non vide de monômes admet un plus petit élément pour $<$.

Les ordres monomiaux

Ordre monomial admissible

C'est un ordre total $<$ sur les monômes de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :

1. pour tout triplet de monômes m_1, m_2, m_3 alors

$$m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$$

2. pour tout monôme m, $1 < m$.

2'. tout ensemble non vide de monômes admet un plus petit élément pour $<$.

2''. toute suite strictement décroissante de monômes est finie.

Les ordres monomiaux

Ordre monomial admissible

C'est un ordre total $<$ sur les monômes de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :

1. pour tout triplet de monômes m_1, m_2, m_3 alors

$$m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$$

2. pour tout monôme m, $1 < m$.

2'. tout ensemble non vide de monômes admet un plus petit élément pour $<$.

2''. toute suite strictement décroissante de monômes est finie.

Les ordres monomiaux

Ordre monomial admissible

C'est un ordre total $<$ sur les monômes de $\mathbb{K}[x_1, \ldots, x_n]$ vérifiant :

1. pour tout triplet de monômes m_1, m_2, m_3 alors
$$m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$$
2. pour tout monôme m, $1 < m$.
2'. tout ensemble non vide de monômes admet un plus petit élément pour $<$.
2''. toute suite strictement décroissante de monômes est finie.

les conditions 2, 2', 2'' étant équivalentes lorsque 1 est vérifiée (cf Lemme de Dickson pour 2).

Exemple d'ordres monomiaux

Ordre lexicographique $x_1 > \cdots > x_n$ — LEX

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n} \iff \exists j \geq 1 \, (\alpha_i = \beta_i \quad \forall i < j) \text{ et } \alpha_j < \beta_j,$$
$$(\alpha_1, \cdots, \alpha_n) <_{lex} (\beta_1, \cdots, \beta_n)$$

Exemple d'ordres monomiaux

Ordre lexicographique $x_1 > \cdots > x_n$ — LEX

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n} \iff \exists j \geq 1 \, (\alpha_i = \beta_i \quad \forall i < j) \text{ et } \alpha_j < \beta_j,$$
$$(\alpha_1, \cdots, \alpha_n) <_{lex} (\beta_1, \cdots, \beta_n)$$

Exemple d'ordres monomiaux

Ordre lexicographique $x_1 > \cdots > x_n$ LEX

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n} \iff \exists j \geq 1 \, (\alpha_i = \beta_i \quad \forall i < j) \text{ et } \alpha_j < \beta_j,$$
$$(\alpha_1, \cdots, \alpha_n) <_{lex} (\beta_1, \cdots, \beta_n)$$

Ordre degré-lexicographique $x_1 > \cdots > x_n$

$$x^\alpha <_{grlex} x^\beta \iff |\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } x^\alpha <_{lex} x^\beta)$$

Exemple d'ordres monomiaux

Ordre lexicographique $x_1 > \cdots > x_n$ LEX

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n} \iff \exists j \geq 1 \, (\alpha_i = \beta_i \quad \forall i < j) \text{ et } \alpha_j < \beta_j,$$
$$(\alpha_1, \cdots, \alpha_n) <_{lex} (\beta_1, \cdots, \beta_n)$$

Ordre degré-lexicographique $x_1 > \cdots > x_n$

$$x^\alpha <_{grlex} x^\beta \iff |\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } x^\alpha <_{lex} x^\beta)$$

Ordre du degré lexicographique inverse $x_1 > \cdots > x_n$ GREVLEX ou DRL

$$x^\alpha <_{grevlex} x^\beta \iff |\alpha| < |\beta| \text{ ou}$$
$$(|\alpha| = |\beta| \text{ et } \exists j \geq 1 \, (\alpha_i = \beta_i \quad \forall i > j) \text{ et } \alpha_j > \beta_j)$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$1 < x_3 < x_3^2 < x_3^3 < \dots$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$

Ordre grlex $x_1 > x_2 > x_3$

$1 < x_3 < x_2 < x_1$
$< x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$

Ordre grlex $x_1 > x_2 > x_3$

$1 < x_3 < x_2 < x_1$
$< x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2$
$< x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$

Ordre grevlex $x_1 > x_2 > x_3$

$1 < x_3 < x_2 < x_1$
$< x_3^2$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_1x_3$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_1x_3 < x_2^2 < x_1x_2 < x_1^2$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_1x_3 < x_2^2 < x_1x_2 < x_1^2 < x_3^3$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_1x_3 < x_2^2 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_1x_3^2$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_1x_3 < x_2^2 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_1x_3^2 < x_2^2x_3 < x_1x_2x_3 < x_1^2x_3$$

Exemple d'ordres monomiaux en 3 variables

Ordre lex $x_1 > x_2 > x_3$

$$1 < x_3 < x_3^2 < x_3^3 < \ldots < x_2 < x_2x_3 < x_2x_3^2 < \ldots < x_2^2 < x_2^2x_3 < \ldots < x_2^3 < \ldots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \ldots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \ldots < x_1^3 < \ldots$$

Ordre grlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_2^2 < x_1x_3 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_2^2x_3 < x_2^3 < x_1x_3^2 < x_1x_2x_3 < x_1x_2^2 < x_1^2x_3 < x_1^2x_2 < x_1^3$$

Ordre grevlex $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2x_3 < x_1x_3 < x_2^2 < x_1x_2 < x_1^2 < x_3^3 < x_2x_3^2 < x_1x_3^2 < x_2^2x_3 < x_1x_2x_3 < x_1^2x_3 < x_2^3 < x_1x_2^2 < x_1^2x_2 < x_1^3$$

Propriétés des ordres monomiaux

Ordre lex $x_1 > x_2 > \cdots > x_n$

Tout monôme contenant x_j est plus grand qu'un monôme ne contenant aucun $x_1, \ldots, x_j$ (ordre par blocs)

$1 < x_3 < x_3^2 < x_3^3 < \cdots < x_2 < x_2x_3 < x_2x_3^2 < \cdots < x_2^2 < x_2^2x_3 < \cdots < x_2^3 < \cdots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \cdots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \cdots < x_1^3 < \ldots$

Propriétés des ordres monomiaux

Ordre lex $x_1 > x_2 > \cdots > x_n$

Tout monôme contenant x_j est plus grand qu'un monôme ne contenant aucun $x_1, \ldots, x_j$ (ordre par blocs)

$1 < x_3 < x_3^2 < x_3^3 < \cdots < x_2 < x_2x_3 < x_2x_3^2 < \cdots < x_2^2 < x_2^2x_3 < \cdots < x_2^3 < \cdots < x_1 < x_1x_3 < x_1x_3^2 < \cdots < x_1x_2 < x_1x_2x_3 < \cdots < x_1x_2^2 < \cdots < x_1^2 < x_1^2x_3 < \cdots < x_1^2x_2 < \cdots < x_1^3 < \ldots$

Ordre grevlex $x_1 > x_2 > \cdots > x_n$

L'ordre grevlex sur n variables « étend » celui sur $n-1$ variables

$1 < x_3 < x_2 < x_1 <$
$x_3^2 < x_2x_3 < x_1x_3 < x_2^2 < x_1x_2 < x_1^2 <$
$x_3^3 < x_2x_3^2 < x_1x_3^2 < x_2^2x_3 < x_1x_2x_3 < x_1^2x_3 < x_2^3 < x_1x_2^2 < x_1^2x_2 < x_1^3$

Notations

Soit $<$ un ordre monomial sur $\mathbb{K}[x_1, \ldots, x_n]$ et $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$.

- le monôme de tête de f est
$$\mathrm{LM}(f) = \max_{\alpha \in \mathbb{N}^n, c_\alpha \neq 0} (x^\alpha)$$
- le coefficient de tête de f est
$$\mathrm{LC}(f) = c_\alpha \in \mathbb{K}$$
avec α tel que $\mathrm{LM}(f) = x^\alpha$.
- le terme de tête de f est
$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$
- pour un idéal I, $\mathrm{LT}(I) = \{\mathrm{LT}(f) : f \in I\}$.

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$:

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$: $f = \underbrace{-3}_{\text{LC}} \cdot \underbrace{x^3}_{\text{LM}} + 4x^2z^2 + xy^2z + 2z^2$

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$: $f = \underbrace{-3}_{\text{LC}} \cdot \underbrace{x^3}_{\text{LM}} + 4x^2z^2 + xy^2z + 2z^2$
- ordre grlex $x > y > z$:

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$: $f = \underbrace{-3}_{\text{LC}} \cdot \underbrace{x^3}_{\text{LM}} + 4x^2z^2 + xy^2z + 2z^2$
- ordre grlex $x > y > z$: $f = \underbrace{4}_{\text{LC}} \cdot \underbrace{x^2z^2}_{\text{LM}} + xy^2z - 3x^3 + 2z^2$

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$: $f = \underbrace{-3}_{\text{LC}} \cdot \underbrace{x^3}_{\text{LM}} + 4x^2z^2 + xy^2z + 2z^2$
- ordre grlex $x > y > z$: $f = \underbrace{4}_{\text{LC}} \cdot \underbrace{x^2z^2}_{\text{LM}} + xy^2z - 3x^3 + 2z^2$
- ordre grevlex $x > y > z$:

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$: $f = \underbrace{-3}_{\text{LC}} \cdot \underbrace{x^3}_{\text{LM}} + 4x^2z^2 + xy^2z + 2z^2$
- ordre grlex $x > y > z$: $f = \underbrace{4}_{\text{LC}} \cdot \underbrace{x^2z^2}_{\text{LM}} + xy^2z - 3x^3 + 2z^2$
- ordre grevlex $x > y > z$: $f = \underbrace{1}_{\text{LC}} \cdot \underbrace{xy^2z}_{\text{LM}} + 4x^2z^2 - 3x^3 + 2z^2$

Notations

$f = xy^2z + 2z^2 - 3x^3 + 4x^2z^2$

- ordre lex $x > y > z$: $f = \underbrace{-3}_{\text{LC}} \cdot \underbrace{x^3}_{\text{LM}} + 4x^2z^2 + xy^2z + 2z^2$
- ordre grlex $x > y > z$: $f = \underbrace{4}_{\text{LC}} \cdot \underbrace{x^2z^2}_{\text{LM}} + xy^2z - 3x^3 + 2z^2$
- ordre grevlex $x > y > z$: $f = \underbrace{1}_{\text{LC}} \cdot \underbrace{xy^2z}_{\text{LM}} + 4x^2z^2 - 3x^3 + 2z^2$

Pourquoi $2z^2$ ne peut-il jamais être terme de tête ?

Division dans $\mathbb{K}[x_1, \ldots, x_n]$

But : étendre la division euclidienne à $\mathbb{K}[x_1, \ldots, x_n]$.

Division euclidienne dans $\mathbb{K}[x]$

Division de $f \in \mathbb{K}[x]$ par $g \in \mathbb{K}[x]$ suivant les puissances décroissantes de x.

$$\underbrace{x^4 - x^2}_{f} = x(\underbrace{x^3 + 1}_{g})\underbrace{-x^2 + x}_{\text{reste}}$$

Il y a unicité du quotient et du reste.

Division dans $\mathbb{K}[x_1, \ldots, x_n]$

- diviser $f \in \mathbb{K}[x_1, \ldots, x_n]$ par $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$;
- pour un ordre monomial donné $<$;

Division dans $\mathbb{K}[x_1, \ldots, x_n]$

Soit $f \in \mathbb{K}[x_1, \ldots, x_n], F = \{f_1, \ldots, f_m\} \subset \mathbb{K}[x_1, \ldots, x_n]$ tous non nuls.
Si $\mathrm{LM}(f_i) | \mathrm{LM}(f)$ alors f peut être réduit par f_i :

$$g = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} \cdot f_i$$

et $g = 0$ ou $\mathrm{LT}(g) < \mathrm{LT}(f)$.

Division dans $\mathbb{K}[x_1, \ldots, x_n]$

Soit $f \in \mathbb{K}[x_1, \ldots, x_n], F = \{f_1, \ldots, f_m\} \subset \mathbb{K}[x_1, \ldots, x_n]$ tous non nuls.
Si $\mathrm{LM}(f_i) | \mathrm{LM}(f)$ alors f peut être réduit par f_i :

$$g = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} \cdot f_i$$

et $g = 0$ ou $\mathrm{LT}(g) < \mathrm{LT}(f)$.

Algorithme TOP-REDUCTION de f par $F = [f_1, \ldots, f_m]$ pour l'ordre $<$

si $f = 0$ retourner 0
pour $i = 1 \ldots m$ faire
  si $\mathrm{LM}(f_i) | \mathrm{LM}(f)$ alors
    retourner TOP-REDUCTION$(f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} \cdot f_i, F)$
retourner f

L'algorithme termine car $<$ est bien fondé (condition 2'').

Division dans $\mathbb{K}[x_1, \ldots, x_n]$

Exemple

- ordre lexicographique $x > y$.
- $f = xy^2 - x$, $I = \langle f_1 = xy + 1, f_2 = y^2 - 1 \rangle$.

$$\texttt{TOP}-\texttt{REDUCTION}(f, [f_1, f_2]) = \underbrace{xy^2 - x}_{f} - y(\underbrace{xy + 1}_{f_1}) = -x - y$$

$$\texttt{TOP}-\texttt{REDUCTION}(f, [f_2, f_1]) = \underbrace{xy^2 - x}_{f} - x(\underbrace{y^2 - 1}_{f_2}) = 0$$

Division dans $\mathbb{K}[x_1, \ldots, x_n]$

Exemple

- ordre lexicographique $x > y$.
- $f = xy^2 - x$, $I = \langle f_1 = xy + 1, f_2 = y^2 - 1 \rangle$.

$$\texttt{TOP}-\texttt{REDUCTION}(f, [f_1, f_2]) = \underbrace{xy^2 - x}_{f} - y(\underbrace{xy + 1}_{f_1}) = -x - y$$

$$\texttt{TOP}-\texttt{REDUCTION}(f, [f_2, f_1]) = \underbrace{xy^2 - x}_{f} - x(\underbrace{y^2 - 1}_{f_2}) = 0$$

- cela implique que $f \in I$ et donc $f_3 = x + y \in I$.
- $\texttt{TOP-REDUCTION}(f_3, [f_1, f_2]) = x + y \neq 0$.

$$LT(f_3) \in \mathrm{LT}(I) \text{ mais } \mathrm{LT}(f_3) \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$$

Bases de Gröbner

Proposition

Soit $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un idéal, $I \neq \{0\}$, $<$ ordre admissible.
Alors il existe $g_1, \ldots, g_s \in I$ tels que

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$$

(Il en découle le théorème de la base de Hilbert : $I = \langle g_1, \ldots, g_s \rangle$).

Bases de Gröbner

Proposition

Soit $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un idéal, $I \neq \{0\}$, $<$ ordre admissible.
Alors il existe $g_1, \ldots, g_s \in I$ tels que

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$$

(Il en découle le théorème de la base de Hilbert : $I = \langle g_1, \ldots, g_s \rangle$).

Définition

Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et $<$ un ordre admissible. Soit $G = \{g_1, \ldots, g_s\} \subset I$. Alors G est une base de Gröbner de I ssi

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle$$

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

Récurrence sur $n : n = 1$

$\beta = \min(A)$ (1 variable) et $I = \langle x^\beta \rangle$ car $\beta \leq \alpha \Rightarrow x^\beta | x^\alpha$.

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

$n > 1$ et on suppose le lemme vrai pour $n-1$.

$I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ idéal monomial.
« projection » : $J = \langle x^\alpha : \exists m, x^\alpha y^m \in I \rangle$

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

$n > 1$ et on suppose le lemme vrai pour $n-1$.

$I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ idéal monomial.
« projection » : $J = \langle x^\alpha : \exists m, x^\alpha y^m \in I \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$.

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

$n > 1$ et on suppose le lemme vrai pour $n-1$.

$I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ idéal monomial.
« projection » : $J = \langle x^\alpha : \exists m, x^\alpha y^m \in I \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$.
Pour $1 \leq i \leq s$, il existe m_i tq $x^{\alpha_i} y^{m_i} \in I$. Soit $m = \max_{1 \leq i \leq s}(m_i)$.

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

$n > 1$ et on suppose le lemme vrai pour $n-1$.

$I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ idéal monomial.
« projection » : $J = \langle x^\alpha : \exists m, x^\alpha y^m \in I \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$.
Pour $1 \leq i \leq s$, il existe m_i tq $x^{\alpha_i} y^{m_i} \in I$. Soit $m = \max_{1 \leq i \leq s}(m_i)$.
« tranches » : pour $0 \leq k < m$,

$$J_k = \langle x^\alpha : x^\alpha y^k \in I \rangle = \langle x^{\alpha_1^{(k)}}, \ldots, x^{\alpha_{s_k}^{(k)}} \rangle.$$

Preuve (cf Cox, Little, O'Shea 1997)

Lemme de Dickson (un idéal monomial possède une base finie)

Soit $A \subset \mathbb{N}^n$ et $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, alors

$$\exists \alpha_1, \ldots, \alpha_s \in A : \ I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$$

$n > 1$ et on suppose le lemme vrai pour $n-1$.

$I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ idéal monomial.

« projection » : $J = \langle x^\alpha : \exists m, x^\alpha y^m \in I \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$.

Pour $1 \leq i \leq s$, il existe m_i tq $x^{\alpha_i} y^{m_i} \in I$. Soit $m = \max_{1 \leq i \leq s}(m_i)$.

« tranches » : pour $0 \leq k < m$,

$$J_k = \langle x^\alpha : x^\alpha y^k \in I \rangle = \langle x^{\alpha_1^{(k)}}, \ldots, x^{\alpha_{s_k}^{(k)}} \rangle.$$

alors $I = \langle x^{\alpha_i} y^m : 1 \leq i \leq s, x^{\alpha_{j_k}^{(k)}} y^k : \ 0 \leq k \leq m, 1 \leq j_k \leq s_k \rangle$

Existence d'une base de Gröbner

Théorème

Soit $<$ un ordre monomial sur $\mathbb{K}[x_1, \ldots, x_n]$. Tout idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ autre que $\{0\}$ possède une base de Gröbner pour l'ordre $<$. Elle s'obtient par l'algorithme de Buchberger.

Existence d'une base de Gröbner

Notations

Le S-polynome de $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ est

$$S(f,g) = \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} \cdot f - \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} \cdot g$$

Notion fondamentale de l'algorithme de Buchberger.

Existence d'une base de Gröbner

Notations

Le S-polynome de $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ est

$$S(f,g) = \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} \cdot f - \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} \cdot g$$

Notion fondamentale de l'algorithme de Buchberger.

Exemple : $f_1 = xy + 1, f_2 = y^2 - 1$, ordre lexicographique $x > y$.

$$\begin{aligned} S(f_1, f_2) &= \frac{xy^2}{xy}(xy+1) - \frac{xy^2}{y^2}(y^2-1) \\ &= y(xy+1) - x(y^2-1) = x + y \end{aligned}$$

Algorithme de Buchberger

Entrée : $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ non nuls.
Sortie : $G = \{g_1, \ldots, g_s\}$ une base de Gröbner de $I = \langle f_1, \ldots, f_m \rangle$

$G := \{f_1, \ldots, f_m\}$;
`faire`
  $G' := G$;
  `pour tout` $(\mathrm{p}, \mathrm{q}) \in \mathrm{G'}^2, \mathrm{p} \neq \mathrm{q}$ `faire`
    $S := \mathtt{TOP} - \mathtt{REDUCTION}(S(p,q), G')$
    `si` $S \neq 0$ `alors` $G := G \cup \{S\}$
`tant que` $G \neq G'$.

Algorithme de Buchberger

Entrée : $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ non nuls.
Sortie : $G = \{g_1, \ldots, g_s\}$ une base de Gröbner de $I = \langle f_1, \ldots, f_m \rangle$

$G := \{f_1, \ldots, f_m\}$;
`faire`
  $G' := G$;
  `pour tout` $(\mathtt{p}, \mathtt{q}) \in \mathtt{G'}^2, \mathtt{p} \neq \mathtt{q}$ `faire`
    $S := \mathtt{TOP} - \mathtt{REDUCTION}(S(p,q), G')$
    `si` $S \neq 0$ `alors` $G := G \cup \{S\}$
`tant que` $G \neq G'$.

Terminaison : car $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$ à chaque itération.

Algorithme de Buchberger

Entrée : $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ non nuls.
Sortie : $G = \{g_1, \ldots, g_s\}$ une base de Gröbner de $I = \langle f_1, \ldots, f_m \rangle$

$G := \{f_1, \ldots, f_m\}$;
`faire`
  $G' := G$;
  `pour tout` $(\mathtt{p}, \mathtt{q}) \in \mathtt{G'}^2, \mathtt{p} \neq \mathtt{q}$ `faire`
    $S := \mathtt{TOP-REDUCTION}(S(p,q), G')$
    `si` $S \neq 0$ `alors` $G := G \cup \{S\}$
`tant que` $G \neq G'$.

Terminaison : car $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$ à chaque itération. Preuve de terminaison « non constructive », pas de borne de complexité ! Stratégies de sélection de l'ordre des paires critiques et des réductions essentielles !

Exemple

1. $G = F = \{f_1 = xy + 1, f_2 = y^2 - 1\}$, ordre lex $x > y$.
   Paire (f_1, f_2) :
   $S(f_1, f_2) = yf_1 - xf_2 = x + y$ déjà réduit.

Exemple

1. $G = F = \{f_1 = xy + 1, f_2 = y^2 - 1\}$, ordre lex $x > y$.
   Paire (f_1, f_2) :
   $S(f_1, f_2) = yf_1 - xf_2 = x + y$ déjà réduit.
2. $G = \{f_1, f_2, f_3 = x + y\}$
   $S(f_1, f_3) = f_1 - yf_3 = 1 - y^2$ se réduit à 0 (par f_2).
   $S(f_2, f_3) = xf_2 - y^2 f_3 = (f_3 - y)f_2 - (f_2 + 1)f_3 = -yf_2 - f_3$ se réduit à 0 (par f_3 et f_2).

Exemple

1. $G = F = \{f_1 = xy + 1, f_2 = y^2 - 1\}$, ordre lex $x > y$.
   Paire (f_1, f_2) :
   $S(f_1, f_2) = yf_1 - xf_2 = x + y$ déjà réduit.
2. $G = \{f_1, f_2, f_3 = x + y\}$
   $S(f_1, f_3) = f_1 - yf_3 = 1 - y^2$ se réduit à 0 (par f_2).
   $S(f_2, f_3) = xf_2 - y^2 f_3 = (f_3 - y)f_2 - (f_2 + 1)f_3 = -yf_2 - f_3$ se réduit à 0 (par f_3 et f_2).

Exemple

1. $G = F = \{f_1 = xy + 1, f_2 = y^2 - 1\}$, ordre lex $x > y$.
   Paire (f_1, f_2) :
   $S(f_1, f_2) = yf_1 - xf_2 = x + y$ déjà réduit.
2. $G = \{f_1, f_2, f_3 = x + y\}$
   $S(f_1, f_3) = f_1 - yf_3 = 1 - y^2$ se réduit à 0 (par f_2).
   $S(f_2, f_3) = xf_2 - y^2 f_3 = (f_3 - y)f_2 - (f_2 + 1)f_3 = -yf_2 - f_3$ se réduit à 0 (par f_3 et f_2).

$G = \{xy + 1, y^2 - 1, x + y\}$.

Exemple

1. $G = F = \{f_1 = xy + 1, f_2 = y^2 - 1\}$, ordre lex $x > y$.
   Paire (f_1, f_2) :
   $S(f_1, f_2) = yf_1 - xf_2 = x + y$ déjà réduit.
2. $G = \{f_1, f_2, f_3 = x + y\}$
   $S(f_1, f_3) = f_1 - yf_3 = 1 - y^2$ se réduit à 0 (par f_2).
   $S(f_2, f_3) = xf_2 - y^2 f_3 = (f_3 - y)f_2 - (f_2 + 1)f_3 = -yf_2 - f_3$ se réduit à 0 (par f_3 et f_2).

$G = \{xy + 1, y^2 - 1, x + y\}$.
$\{y^2 - 1, x + y\}$ est aussi une base de Gröbner de I.
Il n'y a pas unicité !

Forme normale

Algorithme FULL-REDUCTION de f par $F = [f_1, \ldots, f_m]$, l'ordre $<$

$g := 0$
tant que $f \neq 0$ faire
  $f = \mathrm{TOP-REDUCTION}(f, F)$
  $g = g + \mathrm{LT}(f)$
  $f = f - \mathrm{LT}(f)$
retourner g

Forme normale

Proposition (Forme Normale)

Si $G = \{g_1, \ldots, g_s\}$ est une base de Gröbner de I, alors tout polynôme $f \in \mathbb{K}[x_1, \ldots, x_n]$ s'écrit

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

où aucun des monômes de r n'appartient à $\mathrm{LT}(I)$.
r est unique et indépendant de G, il s'appelle la Forme Normale de g par rapport à I (et à l'ordre $<$).

$$r = \mathrm{NF}(f, G, <).$$

Les h_i ne sont pas uniques.

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

$$f = xy \quad = y(\underbrace{x - z}_{g_1}) + yz$$

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

$$f = xy \quad = y\underbrace{(x - z)}_{g_1} + yz = \quad yg_1 + z\underbrace{(y + z)}_{g_2} - z^2$$

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

$$f = xy \quad = y(\underbrace{x - z}_{g_1}) + yz = \quad yg_1 + z(\underbrace{y + z}_{g_2}) - z^2 = yg_1 + zg_2 - z^2$$

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

$$f = xy = y\underbrace{(x-z)}_{g_1} + yz = yg_1 + z\underbrace{(y+z)}_{g_2} - z^2 = yg_1 + zg_2 - z^2$$

$$= x\underbrace{(y+z)}_{g_2} - xz$$

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

$$f = xy = y\underbrace{(x-z)}_{g_1} + yz = yg_1 + z\underbrace{(y+z)}_{g_2} - z^2 = yg_1 + zg_2 - z^2$$
$$= x\underbrace{(y+z)}_{g_2} - xz = xg_2 - z\underbrace{(x-z)}_{g_1} - z^2$$

Exemple de forme normale

Exemple

$G = \{g_1 = x - z, g_2 = y + z\}$, $f = xy$, ordre lex $x > y > z$.

$$f = xy = y\underbrace{(x-z)}_{g_1} + yz = yg_1 + z\underbrace{(y+z)}_{g_2} - z^2 = yg_1 + zg_2 - z^2$$

$$= x\underbrace{(y+z)}_{g_2} - xz = xg_2 - z\underbrace{(x-z)}_{g_1} - z^2 = -zg_1 + xg_2 - z^2$$

- unicité du reste (forme normale) ;
- pas unicité du chemin de réduction.

Base de Gröbner réduite

Définition (Base de Gröbner réduite)

Soit G une base de Gröbner d'un idéal I pour l'ordre $<$. Alors G est réduite si :

1. $\mathrm{LC}(g) = 1 \forall g \in G$.
2. pour tout $g \in G$, aucun monôme de g n'appartient à $\langle \mathrm{LT}(G - \{g\}) \rangle$.

Base de Gröbner réduite

Définition (Base de Gröbner réduite)

Soit G une base de Gröbner d'un idéal I pour l'ordre $<$. Alors G est réduite si :

1. $\mathrm{LC}(g) = 1 \forall g \in G$.
2. pour tout $g \in G$, aucun monôme de g n'appartient à $\langle \mathrm{LT}(G - \{g\}) \rangle$.

Unicité de la base réduite

Tout idéal $I \neq \{0\}$ possède une unique base de Gröbner réduite.

Corollaire (pour tout ordre monomial $<$)

$\mathscr{V}(I) = \emptyset$ ssi la base de Gröbner réduite de I est $G = \{1\}$.

Caractérisation des bases de Gröbner

Propriété

Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et $<$ un ordre monomial. Soit $G = \{g_1, \ldots, g_s\} \subset I$. Alors les conditions suivantes sont équivalentes :

1. G est une base de Gröbner de I
2. $$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle$$
3. $\texttt{TOP-REDUCTION}(f, G) = 0$ si et seulement si $f \in I$.
4. Pour tout $f \in I$ il existe k tel que $\mathrm{LT}(g_k) | \mathrm{LT}(f)$.
5. Pour tout $i \neq j$, $\texttt{TOP-REDUCTION}(S(g_i, g_j), G) = 0$.

Nombre fini de solutions

Systèmes de dimension 0

Soit $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un idéal et G une base de Gröbner pour l'ordre $<$.
Alors I possède un nombre fini de solutions ssi pour toute variable x_i il existe un $g_i \in G$ dont le terme de tête est une puissance de x_i.

Propriétés des ordres monomiaux

Soit G une base de Gröbner réduite d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Ordre Lexicographique $x_1 > \cdots > x_n$

- Si $\mathrm{LT}(f) \in \mathbb{K}[x_i, \ldots, x_n]$ alors $f \in \mathbb{K}[x_i, \ldots, x_n]$.

Propriétés des ordres monomiaux

Soit G une base de Gröbner réduite d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Ordre Lexicographique $x_1 > \cdots > x_n$

- Si $\mathrm{LT}(f) \in \mathbb{K}[x_i, \ldots, x_n]$ alors $f \in \mathbb{K}[x_i, \ldots, x_n]$.
- Si $I \cap \mathbb{K}[x_n] \neq \{0\}$ alors $I \cap \mathbb{K}[x_n] = \langle g_n(x_n) \rangle$ et $g_n(x_n) \in G$.

Propriétés des ordres monomiaux

Soit G une base de Gröbner réduite d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Ordre Lexicographique $x_1 > \cdots > x_n$

- Si $\mathrm{LT}(f) \in \mathbb{K}[x_i, \ldots, x_n]$ alors $f \in \mathbb{K}[x_i, \ldots, x_n]$.
- Si $I \cap \mathbb{K}[x_n] \neq \{0\}$ alors $I \cap \mathbb{K}[x_n] = \langle g_n(x_n) \rangle$ et $g_n(x_n) \in G$.

Propriétés des ordres monomiaux

Soit G une base de Gröbner réduite d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Ordre Lexicographique $x_1 > \cdots > x_n$

- Si $\mathrm{LT}(f) \in \mathbb{K}[x_i, \ldots, x_n]$ alors $f \in \mathbb{K}[x_i, \ldots, x_n]$.
- Si $I \cap \mathbb{K}[x_n] \neq \{0\}$ alors $I \cap \mathbb{K}[x_n] = \langle g_n(x_n) \rangle$ et $g_n(x_n) \in G$.

Ordre gradué par le degré

G contient les polynômes de degré minimal (donc des polynômes linéaires s'il en existe).

Propriétés des ordres monomiaux

Soit G une base de Gröbner réduite d'un idéal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Ordre Lexicographique $x_1 > \cdots > x_n$

- Si $\mathrm{LT}(f) \in \mathbb{K}[x_i, \ldots, x_n]$ alors $f \in \mathbb{K}[x_i, \ldots, x_n]$.
- Si $I \cap \mathbb{K}[x_n] \neq \{0\}$ alors $I \cap \mathbb{K}[x_n] = \langle g_n(x_n) \rangle$ et $g_n(x_n) \in G$.

Ordre gradué par le degré

G contient les polynômes de degré minimal (donc des polynômes linéaires s'il en existe).

Ordre grevlex $x_1 > \cdots > x_n$

- si $x_n^m | \mathrm{LT}(f)$ alors $x_n^m | f$.
- si $\mathrm{LT}(f) = 0 \mod (x_i, \ldots, x_n)$ alors $f = 0 \mod (x_i, \ldots, x_n)$.

Élimination

Ordre d'élimination

$<$ est un ordre monomial d'élimination sur $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ pour les blocs $[x_1, \ldots, x_n] > [y_1, \ldots, y_m]$ si :

- $<$ est un ordre monomial admissible ;
- pour tous monômes $x^{\alpha_1} y^{\beta_1}$, $x^{\alpha_2} y^{\beta_2}$, si $x^{\alpha_1} < x^{\alpha_2}$ alors $x^{\alpha_1} y^{\beta_1} < x^{\alpha_2} y^{\beta_2}$.

L'ordre lexicographique $x_1 > x_2 > \cdots > x_n$

est un ordre d'élimination pour $[x_1, \ldots, x_i]$ et $[x_{i+1}, \ldots, x_n]$ pour tout i.

Élimination

Théorème d'élimination

Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ et G sa base de Gröbner pour un ordre d'élimination $[x_1, \ldots, x_n] > [y_1, \ldots, y_m]$. Alors l'ensemble

$$G_n = G \cap \mathbb{K}[y_1, \ldots, y_m]$$

est une base de Gröbner de l'idéal d'élimination $I_n = I \cap \mathbb{K}[y_1, \ldots, y_m]$.

Résolution par l'ordre Lex

Nombre fini de solutions

Forme générale de la base de Gröbner Lex $x_1 > \cdots > x_n$

$$
\begin{array}{rrrcr}
g_1(x_1, & x_2, & x_3, & \ldots, & x_n) \\
\vdots & & & & \\
g_p(x_1, & x_2, & x_3, & \ldots, & x_n) \\
 & g_{p+1}(x_2, & x_3, & \ldots, & x_n) \\
 & \vdots & & & \\
 & g_q(x_2, & x_3, & \ldots, & x_n) \\
 & & g_{q+1}(x_3, & \ldots, & x_n) \\
 & & \vdots & & \\
 & & & \vdots & \\
 & & & & g_r(x_n)
\end{array}
$$

Résolution par l'ordre Lex

Nombre fini de solutions, Shape position

I radical, à un changement de coordonnées près. Ordre lex $x_1 > \cdots > x_n$. G base réduite.

$$G = \begin{cases} x_1 & - & g_1(x_n) \\ & \vdots & \\ x_{n-1} & - & g_{n-1}(x_n) \\ & & g_n(x_n) \end{cases}$$

Cf Gianni, Mora 1987.
Becker, Mora, Marinari, Traverso 1994. « The shape of the shape lemma ».

Plan

Convention

Dans toute la suite :

- les polynômes f_i sont homogènes ;
- l'ordre monomial admissible $<$ est un ordre gradué.

Convention

Dans toute la suite :

- les polynômes f_i sont homogènes ;
- l'ordre monomial admissible $<$ est un ordre gradué.

Homogénéisation

On peut homogénéiser un polynôme affine :

$$x_1x_2 + x_3 + 1 \rightarrow x_1x_2 + x_3h + h^2$$

Convention

Dans toute la suite :

- les polynômes f_i sont homogènes ;
- l'ordre monomial admissible $<$ est un ordre gradué.

L'ordre lex n'est pas gradué !

Algorithme FGLM

Hypothèse : I a un nombre fini de solutions.
Algorithme de changement d'ordre : calcule une base de Gröbner de I pour $<_2$ à partir d'une base de I pour $<_1$.
Faugère, Giani, Lazard, Mora, JSC, 1994.

Complexité

Le nombre d'opérations dans $\mathbb{K}$ de l'algorithme FGLM est borné par

$$O(n\deg(I)^3)$$

où $\deg(I)$ est la dimension du $\mathbb{K}$-espace vectoriel $\mathbb{K}[x_1,\ldots,x_n]/I$.

Borne de Bezout : sur un corps algébriquement clos, si I a un nombre fini de solutions,

$$\deg(I) \leq \prod_{i=1}^{n} \deg(f_i)$$

Bases de Gröbner et algèbre linéaire

Système linéaire : écriture sous forme matricielle

$$\begin{array}{cccc} (x_1 > & x_2 > & \cdots > x_n & > 1) \\ c_{1,1}x_1 + & c_{1,2}x_2 + \ldots + & c_{1,n}x_n + & c_{1,n+1} \\ & \vdots & & \\ c_{n,1}x_1 + & c_{n,2}x_2 + \ldots + & c_{n,n}x_n + & c_{n,n+1} \end{array}$$

Bases de Gröbner et algèbre linéaire

Système linéaire : écriture sous forme matricielle

$$[A|b] = \begin{pmatrix} (x_1 > & x_2 > & \cdots > x_n & > 1) \\ c_{1,1} & c_{1,2} & \cdots & c_{1,n} & c_{1,n+1} \\ & & \vdots & & \\ c_{n,1} & c_{n,2} & \cdots & c_{n,n} & c_{n,n+1} \end{pmatrix}$$

Bases de Gröbner et algèbre linéaire

Matrice de Macaulay $\mathscr{M}(d)$ en degré d

polynôme $f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$

Bases de Gröbner et algèbre linéaire

Matrice de Macaulay $\mathscr{M}(d)$ en degré d

polynôme $f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$

ligne d'une matrice : $F_1 \begin{pmatrix} x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 \\ 1 & 1 & 2 & -1 & -3 & 4 \end{pmatrix}$

Bases de Gröbner et algèbre linéaire

Matrice de Macaulay $\mathscr{M}(d)$ en degré d

polynôme $f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$
polynôme $f_2 = +1x_1^2 + 2x_1x_2 - 3x_2^2 + 4x_1x_3 + 1x_2x_3 - 1x_3^2$

ligne d'une matrice :

$$\begin{array}{c} \\ F_1 \\ F_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 \end{array} \\ \begin{pmatrix} 1 & 1 & 2 & -1 & -3 & 4 \\ 1 & 2 & -3 & 4 & 1 & -1 \end{pmatrix} \end{array}$$

Monômes triés dans l'ordre grevlex $x_1 > \cdots > x_n$ décroissant.

Bases de Gröbner et algèbre linéaire

Matrice de Macaulay $\mathscr{M}(d)$ en degré d

polynôme $f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$
polynôme $f_2 = +1x_1^2 + 2x_1x_2 - 3x_2^2 + 4x_1x_3 + 1x_2x_3 - 1x_3^2$
$f_2 - f_1 = 0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$

ligne d'une matrice :

$$\begin{array}{c} \\ F_1 \\ F_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 \end{array} \\ \begin{pmatrix} 1 & 1 & 2 & -1 & -3 & 4 \\ 1 & 2 & -3 & 4 & 1 & -1 \end{pmatrix} \end{array}$$

Monômes triés dans l'ordre grevlex $x_1 > \cdots > x_n$ décroissant.

Bases de Gröbner et algèbre linéaire

Matrice de Macaulay $\mathscr{M}(d)$ en degré d

polynôme $f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$
polynôme $f_2 = +1x_1^2 + 2x_1x_2 - 3x_2^2 + 4x_1x_3 + 1x_2x_3 - 1x_3^2$
$f_2 - f_1 = 0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$

ligne d'une matrice :

$$\begin{array}{c} \\ F_1 \\ F_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x_1^2 & x_1x_2 & x_2^2 & x_1x_3 & x_2x_3 & x_3^2 \end{array} \\ \begin{pmatrix} 1 & 1 & 2 & -1 & -3 & 4 \\ 0 & 1 & -5 & 5 & 4 & -5 \end{pmatrix} \end{array}$$

Monômes triés dans l'ordre grevlex $x_1 > \cdots > x_n$ décroissant.
Et le S-polynôme $S(f_1, f_3)$?
$S(f_1, f_3) = x_2 f_1 - x_1 f_2$

Rappel : algorithme de Buchberger

Entrée : $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ non nuls.
Sortie : $G = \{g_1, \ldots, g_s\}$ une base de Gröbner de $I = \langle f_1, \ldots, f_m \rangle$

$G := \{f_1, \ldots, f_m\}$;
`faire`
  $G' := G$;
  `pour tout` $(\mathtt{p}, \mathtt{q}) \in \mathtt{G'}^2, \mathtt{p} \neq \mathtt{q}$ `faire`
    $S := \mathtt{TOP} - \mathtt{REDUCTION}(S(p,q), G')$
    `si` $S \neq 0$ `alors` $G := G \cup \{S\}$
`tant que` $G \neq G'$.

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

$$\begin{array}{c} \\ x_2F_1 \\ x_1F_2 \end{array} \begin{array}{c} \begin{array}{ccccccccccc} x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 & x_1^2x_3 & x_1x_2x_3 & x_2^2x_3 & x_1x_3^2 & x_2x_3^2 & x_3^3 \end{array} \\ \begin{pmatrix} & 1 & 1 & 2 & & -1 & -3 & & 4 & \\ & 1 & -5 & & 5 & 4 & & -5 & & \end{pmatrix} \end{array}$$

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_2F_1		1	1	2		-1	-3		4	
$\underline{x_1F_2}$			-5		5	4		-5		

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_2F_1		1	1	2		-1	-3		4	
$\underline{x_1F_2}$			-6		5	4		-5		

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_2F_1		1	1	2		-1	-3		4	
$\underline{x_1F_2}$			-6	-2	5	4		-5		

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_2F_1		1	1	2		-1	-3		4	
x_1F_2			-6	-2	5	5	3	-5	-4	

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

$$\begin{array}{c} \\ x_2F_1 \\ x_2F_2 \\ x_1F_2 \end{array} \begin{array}{c} \begin{array}{ccccccccccc} x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 & x_1^2x_3 & x_1x_2x_3 & x_2^2x_3 & x_1x_3^2 & x_2x_3^2 & x_3^3 \end{array} \\ \begin{pmatrix} & 1 & 1 & 2 & & -1 & -3 & & 4 & \\ & & 1 & -5 & & 5 & 4 & & -5 & \\ & & -6 & -2 & 5 & 5 & 3 & -5 & -4 & \end{pmatrix} \end{array}$$

Mais $x_1 f_2$ est réductible par f_2

Bases de Gröbner et algèbre linéaire

en degré trois : $S(f_1, f_3) = x_2 f_1 - x_1 f_2$

$x_2 F_1 \to x_2(1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2)$

$x_1 F_2 \to x_1(0x_1^2 + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2)$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_2F_1		1	1	2		-1	-3		4	
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	

Bases de Gröbner et algèbre linéaire

Pour simplifier : systèmes homogènes.
$I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$. Matrice de Macaulay en degré d :

$$\begin{matrix} & & \text{monômes de degré } d \\ (t, f_1) & & \\ (u, f_2) & & \\ \vdots & \text{avec } \deg(vf_i) = d & \\ (w, f_m) & & \end{matrix} \begin{pmatrix} & \\ & \\ & \end{pmatrix} = \mathscr{M}_d$$

F. S. Macaulay. On some formula in elimination. 1902.
F. S. Macaulay. The Algebraic Theory of Modular Systems. 1916.

Bases de Gröbner et algèbre linéaire

- La matrice de Macaulay généralise la matrice de Sylvester pour le calcul du résultant.
- Les calculs de l'algorithme de Buchberger $\leftrightarrow$ réductions de lignes de la matrice de Macaulay.

Algorithme F_4 (Faugère 1999)

- Utiliser des algorithmes de calcul de forme échelon comme stratégie de réduction.
- Pour la terminaison : même critère que pour l'algorithme de Buchberger.

Bases de Gröbner et algèbre linéaire

- La matrice de Macaulay généralise la matrice de Sylvester pour le calcul du résultant.
- Les calculs de l'algorithme de Buchberger $\leftrightarrow$ réductions de lignes de la matrice de Macaulay.

Algorithme F_4 (Faugère 1999)

- Utiliser des algorithmes de calcul de forme échelon comme stratégie de réduction.
- Pour la terminaison : même critère que pour l'algorithme de Buchberger.

Algorithme F_5 (Faugère 2002), version matricielle

- Construire une sous-matrice de la matrice de Macaulay de même rang en éliminant des lignes qui vont se réduire à 0.

Bases de Gröbner et algèbre linéaire

Encore des notations

- $\mathbb{K}[x_1, \ldots, x_n]_d$ l'ensemble des polynômes de degré d.
- $I_d = I \cap \mathbb{K}[x_1, \ldots, x_n]_d$. C'est un sous-espace vectoriel de $\mathbb{K}[x_1, \ldots, x_n]_d$.
- $\dim(\mathbb{K}[x_1, \ldots, x_n]_d) = \binom{n+d-1}{d}$ nombre de colonnes de $\mathscr{M}_d$.
- I_d est engendré par tous les tf_i, t monôme de degré $d - d_i$ où $d_i = \deg(f_i)$.

D-bases de Gröbner

Définition

$I \subset \mathbb{K}[x_1, \ldots, x_n]$ un idéal. Un ensemble fini $G \subset \mathbb{K}[x_1, \ldots, x_n]$ est une D-base de Gröbner si

$$\forall 0 \neq f \in I, \deg(f) \leq D \text{ il existe } g \in G \text{ tel que } \mathrm{LM}(g) | \mathrm{LM}(f)$$

D-bases de Gröbner

Définition

$I \subset \mathbb{K}[x_1, \ldots, x_n]$ un idéal. Un ensemble fini $G \subset \mathbb{K}[x_1, \ldots, x_n]$ est une D-base de Gröbner si

$$\forall 0 \neq f \in I, \deg(f) \leq D \text{ il existe } g \in G \text{ tel que } \mathrm{LM}(g) | \mathrm{LM}(f)$$

Propriété (Lazard 1983)

L'ensemble des polynômes correspondant aux lignes des matrices de Macaulay réduites en degré $d \leq D$ forme une D-base de Gröbner de I.

D-bases de Gröbner

Définition

$I \subset \mathbb{K}[x_1, \ldots, x_n]$ un idéal. Un ensemble fini $G \subset \mathbb{K}[x_1, \ldots, x_n]$ est une D-base de Gröbner si

$$\forall 0 \neq f \in I, \deg(f) \leq D \text{ il existe } g \in G \text{ tel que } \mathrm{LM}(g) | \mathrm{LM}(f)$$

Propriété (Lazard 1983)

L'ensemble des polynômes correspondant aux lignes des matrices de Macaulay réduites en degré $d \leq D$ forme une D-base de Gröbner de I.
Il existe un entier D tel que une D-base de Gröbner de I est une base de Gröbner de I.

Première borne de complexité

Proposition

$I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ homogène, $<$ ordre gradué.
Le nombre d'opérations dans le corps $\mathbb{K}$ nécessaires pour calculer une base de Gröbner de I jusqu'au degré D est borné par

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right), \text{ quand } D \to \infty$$

ω exposant de complexité de la multiplication matricielle sur $\mathbb{K}$.

Première borne de complexité

Proposition

$I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ homogène, $<$ ordre gradué.
Le nombre d'opérations dans le corps $\mathbb{K}$ nécessaires pour calculer une base de Gröbner de I jusqu'au degré D est borné par

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right), \text{ quand } D \to \infty$$

ω exposant de complexité de la multiplication matricielle sur $\mathbb{K}$.

Preuve : Élimination sur $\mathscr{M}_d$, $0 \leq d \leq D$.

- Nombre de colonnes : $C_d = \dim(\mathbb{K}[x_1, \ldots, x_n]_d) = \binom{n+d-1}{d}$.
- Nombre de lignes ($d_i = \deg(f_i)$) :
  $R_d = \dim(\mathbb{K}[x_1, \ldots, x_n]_{d-d_1}) + \cdots + \dim(\mathbb{K}[x_1, \ldots, x_n]_{d-d_m})$.

Preuve(suite)

$C_d = \binom{n+d-1}{d}$, croissant en d : $\frac{C_{d+1}}{C_d} = \frac{n+d}{d+1} \geq 1$

Preuve(suite)

$C_d = \binom{n+d-1}{d}$, croissant en d :
$R_d = C_{d-d_1} + \cdots + C_{d-d_m} \leq mC_d$

Preuve(suite)

$C_d = \binom{n+d-1}{d}$, croissant en d :
$R_d = C_{d-d_1} + \cdots + C_{d-d_m} \leq mC_d$

Storjohann 2000

Complexité du calcul d'une forme échelon réduite d'une matrice à C_d colonnes et R_d lignes :

$$O(R_d C_d r^{\omega-2})$$

où ω complexité de la multiplication matricielle, r rang de la matrice.

Preuve(suite)

$C_d = \binom{n+d-1}{d}$, croissant en d :
$R_d = C_{d-d_1} + \cdots + C_{d-d_m} \leq mC_d$

Storjohann 2000

Complexité du calcul d'une forme échelon réduite d'une matrice à C_d colonnes et R_d lignes :

$$O(R_d C_d r^{\omega-2})$$

où ω complexité de la multiplication matricielle, r rang de la matrice.

Majoration finale :

$$O(mDC_d^{\omega})$$

Première borne de complexité

Proposition

$I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ homogène, $<$ ordre gradué.
Le nombre d'opérations dans le corps $\mathbb{K}$ nécessaires pour calculer une base de Gröbner de I jusqu'au degré D est borné par

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right), \text{ quand } D \to \infty$$

ω exposant de l'algèbre linéaire sur $\mathbb{K}$.

Il reste à borner D.

Première borne de complexité

Proposition

$I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ homogène, $<$ ordre gradué.
Le nombre d'opérations dans le corps $\mathbb{K}$ nécessaires pour calculer une base de Gröbner de I jusqu'au degré D est borné par

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right), \text{ quand } D \to \infty$$

ω exposant de l'algèbre linéaire sur $\mathbb{K}$.

Il reste à borner D.

Définition : degré de régularité d_{reg}

Le plus petit D tel qu'une D-base de Gröbner soit une base de Gröbner est appelé degré de régularité de l'idéal (pour l'ordre $<$).

Remarques

Algèbre linéaire

- élimination de Gauss : $\omega = 3$;
- Strassen : $\omega = \log_2(7) \simeq 2.807$;
- algorithme de Coppersmith-Winograd (1990) : $\omega < 2.376$;

Remarques

Algèbre linéaire

- élimination de Gauss : $\omega = 3$;
- Strassen : $\omega = \log_2(7) \simeq 2.807$;
- algorithme de Coppersmith-Winograd (1990) : $\omega < 2.376$;

Comportement des algorithmes vis-à-vis de d_{reg}

- Des algorithmes comme l'algorithme de Buchberger ou F_4 peuvent effectuer des calculs en degré plus grand que d_{reg}.
- Critères pour prédire les lignes qui vont se réduire à zéro ? F_5
- Comment estimer d_{reg} ?

Syzygies

Lorsqu'une ligne de la matrice de Macaulay en degré d se réduit à zéro, c'est qu'on a une relation

$$\sum_{1 \leq i \leq m, t \text{ monôme}, \deg(tf_i)=d} \lambda_{t,i} tf_i = 0$$

Syzygies

Lorsqu'une ligne de la matrice de Macaulay en degré d se réduit à zéro, c'est qu'on a une relation

$$\sum_{1\leq i\leq m, t \text{ monôme}, \deg(tf_i)=d} \lambda_{t,i} tf_i = 0$$

En regroupant les termes, on a donc une relation

$$\sum_{i=1}^{m} g_i f_i = 0$$

Syzygies

Lorsqu'une ligne de la matrice de Macaulay en degré d se réduit à zéro, c'est qu'on a une relation

$$\sum_{1\leq i\leq m, t \text{ monôme}, \deg(tf_i)=d} \lambda_{t,i} t f_i = 0$$

En regroupant les termes, on a donc une relation

$$\sum_{i=1}^{m} g_i f_i = 0$$

Définition

$(g_1, \ldots, g_m)$ est une syzygie. On a $g_m f_m \in \langle f_1, \ldots, f_{m-1} \rangle$.
Si $g_m \notin \langle f_1, \ldots, f_{m-1} \rangle$, c'est un diviseur de zéro dans $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_{m-1} \rangle$.

Syzygies

Lorsqu'une ligne de la matrice de Macaulay en degré d se réduit à zéro, c'est qu'on a une relation

$$\sum_{1\leq i\leq m, t \text{ monôme}, \deg(tf_i)=d} \lambda_{t,i} t f_i = 0$$

En regroupant les termes, on a donc une relation

$$\sum_{i=1}^{m} g_i f_i = 0$$

Définition

$(g_1, \ldots, g_m)$ est une syzygie. On a $g_m f_m \in \langle f_1, \ldots, f_{m-1} \rangle$.
Si $g_m \notin \langle f_1, \ldots, f_{m-1} \rangle$, c'est un diviseur de zéro dans $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_{m-1} \rangle$.

Il existe au moins les syzygies triviales

Syzygies

Lorsqu'une ligne de la matrice de Macaulay en degré d se réduit à zéro, c'est qu'on a une relation

$$\sum_{1\leq i\leq m, t \text{ monôme}, \deg(tf_i)=d} \lambda_{t,i} t f_i = 0$$

En regroupant les termes, on a donc une relation

$$\sum_{i=1}^{m} g_i f_i = 0$$

Définition

$(g_1, \ldots, g_m)$ est une syzygie. On a $g_m f_m \in \langle f_1, \ldots, f_{m-1} \rangle$.
Si $g_m \notin \langle f_1, \ldots, f_{m-1} \rangle$, c'est un diviseur de zéro dans $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_{m-1} \rangle$.

Il existe au moins les syzygies triviales $f_i f_j - f_j f_i = 0$ en degré $d_i d_j$!

Bornes sur le degré de régularité

Définition : suite régulière (Macaulay 1916)

Une suite $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ de m polynômes homogènes est régulière si les conditions suivantes sont vérifiées :

- $\langle f_1, \ldots, f_m \rangle \neq \mathbb{K}[x_1, \ldots, x_n]$
- $\forall 1 \leq i \leq m$, si $g_i f_i = 0$ dans $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_{i-1} \rangle$ alors $g_i = 0$ dans $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_{i-1} \rangle$

Bornes sur le degré de régularité

Définition : suite régulière (Macaulay 1916)

Une suite $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ de m polynômes homogènes est régulière si les conditions suivantes sont vérifiées :

- $\langle f_1, \ldots, f_m \rangle \neq \mathbb{K}[x_1, \ldots, x_n]$
- $\forall 1 \leq i \leq m$, si $g_i f_i \in \langle f_1, \ldots, f_{i-1} \rangle$ alors $g_i \in \langle f_1, \ldots, f_{i-1} \rangle$

Cela revient à dire qu'il n'existe pas de relations algébriques entre les f_i autres que celles induites par les syzygies triviales.

Bornes sur le degré de régularité

Définition : suite régulière (Macaulay 1916)

Une suite $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ de m polynômes homogènes est régulière si les conditions suivantes sont vérifiées :

- $\langle f_1, \ldots, f_m \rangle \neq \mathbb{K}[x_1, \ldots, x_n]$
- $\forall 1 \leq i \leq m$, si $g_i f_i \in \langle f_1, \ldots, f_{i-1} \rangle$ alors $g_i \in \langle f_1, \ldots, f_{i-1} \rangle$

Exemples

- $f_1 = xy^2, f_2 = x^3y$ n'est pas régulière : $yf_2 = (x^2)xy^2 \in \langle f_1 \rangle$ mais $y \notin \langle f_1 \rangle$.
- $x_1^{d_1}, \ldots, x_n^{d_n}$ est une suite régulière.

Les suites régulières ont des propriétés très fortes.

Séries de Hilbert

Définition : fonction de Hilbert

La fonction de Hilbert de $I = \langle f_1, \ldots, f_m \rangle$ en degré d est définie par

$$\mathrm{HF}_I(d) = \dim_{\mathbb{K}} \left(\mathbb{K}[x_1, \ldots, x_n]/I\right)_d = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n])_d - \dim(I_d)$$

Séries de Hilbert

Définition : fonction de Hilbert

La fonction de Hilbert de $I = \langle f_1, \ldots, f_m \rangle$ en degré d est définie par

$$\mathrm{HF}_I(d) = \dim_{\mathbb{K}} \left(\mathbb{K}[x_1, \ldots, x_n]/I\right)_d = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n])_d - \dim(I_d)$$

Définition : série de Hilbert

La série de Hilbert de I est définie par

$$\mathrm{HS}_I(z) = \sum_{d \geq 0} \mathrm{HF}_I(d) z^d.$$

Propriétés de la série de Hilbert

Théorème : polynôme de Hilbert

Il existe $d_0 \in \mathbb{N}$ et un polynôme $p \in \mathbb{K}[x]$ tel que pour tout $d \geq d_0$,

$$\mathrm{HF}_I(d) = p(d)$$

Le plus petit de ces d_0 est noté $H(I)$ et s'appelle l'indice de régularité de I. La dimension de I est $\dim(I) = \deg(p)$.

Propriétés de la série de Hilbert

Théorème : polynôme de Hilbert

Il existe $d_0 \in \mathbb{N}$ et un polynôme $p \in \mathbb{K}[x]$ tel que pour tout $d \geq d_0$,

$$\mathrm{HF}_I(d) = p(d)$$

Le plus petit de ces d_0 est noté $H(I)$ et s'appelle l'indice de régularité de I. La dimension de I est $\dim(I) = \deg(p)$.

$$\begin{aligned} \mathrm{HS}_I(z) &= \sum_{d\geq 0} \mathrm{HF}_I(d) z^d = \sum_{d=0}^{d_0-1} HF_I(d) z^d + \sum_{d\geq d_0} p(d) z^d \\ \frac{1}{(1-z)^k} &= \frac{1}{k!} \sum_{d\geq 0} (d+1)(d+2)\cdots(d+k) z^d \end{aligned}$$

Propriétés de la série de Hilbert

Théorème : polynôme de Hilbert

Il existe $d_0 \in \mathbb{N}$ et un polynôme $p \in \mathbb{K}[x]$ tel que pour tout $d \geq d_0$,

$$\mathrm{HF}_I(d) = p(d)$$

Le plus petit de ces d_0 est noté $H(I)$ et s'appelle l'indice de régularité de I. La dimension de I est $\dim(I) = \deg(p)$.

Corollaire : dimension, degré

$\mathrm{HS}_I(z) = \frac{P(z)}{(1-z)^d}$, pour un polynôme $P \in \mathbb{K}[x]$ tel que $P(1) \neq 0$.

- d est la dimension de I,
- $P(1)$ est le degré de la variété $\mathscr{V}(I)$ (avec multiplicités).

Propriétés de la série de Hilbert

Fonction de Hilbert de $\langle \mathrm{LT}(I) \rangle$

$\langle \mathrm{LT}(I) \rangle$ a la même fonction de Hilbert que I (ordre gradué).

Propriétés de la série de Hilbert

Fonction de Hilbert de $\langle \mathrm{LT}(I) \rangle$

$\langle \mathrm{LT}(I) \rangle$ a la même fonction de Hilbert que I (ordre gradué).

Nombre fini de solutions

Si I a un nombre fini de solutions, alors

- $\mathrm{HS}_I(z) = P(z)$ est un polynôme.
- $\dim(I) = 0$.
- $P(1)$ est le nombre de solutions de I (dans $\overline{\mathbb{K}}$, comptées avec multiplicité).

Propriétés des suites régulières

Si $f_1, \ldots, f_m$ est une suite régulière homogène, $d_i = \deg(f_i)$, alors :

- la série de Hilbert de $f_1, \ldots, f_m$ est

$$\sum_{d \geq 0} \mathrm{HF}_I(d) z^d = \prod_{i=1}^{m} (1 - z^{d_i}) \Big/ (1 - z)^n \qquad (1)$$

.

Propriétés des suites régulières

Si $f_1, \ldots, f_m$ est une suite régulière homogène, $d_i = \deg(f_i)$, alors :

- la série de Hilbert de $f_1, \ldots, f_m$ est

$$\sum_{d \geq 0} \mathrm{HF}_I(d) z^d = \prod_{i=1}^{m} (1 - z^{d_i}) \Big/ (1 - z)^n \qquad (1)$$

- l'idéal $\langle f_1, \ldots, f_m \rangle$ est de dimension $n - m$,

.

Propriétés des suites régulières

Si $f_1, \ldots, f_m$ est une suite régulière homogène, $d_i = \deg(f_i)$, alors :

- la série de Hilbert de $f_1, \ldots, f_m$ est

$$\sum_{d \geq 0} \mathrm{HF}_I(d) z^d = \prod_{i=1}^{m} (1 - z^{d_i}) \Big/ (1-z)^n \qquad (1)$$

- l'idéal $\langle f_1, \ldots, f_m \rangle$ est de dimension $n - m$,
- le degré de I est $\prod_{i=1}^{m} d_i$ (borne de Bezout).

.

Propriétés des suites régulières

Si $f_1, \ldots, f_m$ est une suite régulière homogène, $d_i = \deg(f_i)$, alors :

- la série de Hilbert de $f_1, \ldots, f_m$ est

$$\sum_{d \geq 0} \mathrm{HF}_I(d) z^d = \prod_{i=1}^{m} (1 - z^{d_i}) \Big/ (1 - z)^n \qquad (1)$$

- l'idéal $\langle f_1, \ldots, f_m \rangle$ est de dimension $n - m$,
- le degré de I est $\prod_{i=1}^{m} d_i$ (borne de Bezout).
- « généricité » : presque toute suite est une suite régulière : l'ensemble des suites de n variables et degrés $d_1, \ldots, d_m$ qui sont régulières est un ouvert non vide de Zariski (donc dense).

.

Propriétés des suites régulières

Si $f_1, \ldots, f_m$ est une suite régulière homogène, $d_i = \deg(f_i)$, alors :

- la série de Hilbert de $f_1, \ldots, f_m$ est

$$\sum_{d \geq 0} \mathrm{HF}_I(d) z^d = \prod_{i=1}^{m} (1 - z^{d_i}) \Big/ (1 - z)^n \qquad (1)$$

- l'idéal $\langle f_1, \ldots, f_m \rangle$ est de dimension $n - m$,
- le degré de I est $\prod_{i=1}^{m} d_i$ (borne de Bezout).
- « généricité » : presque toute suite est une suite régulière : l'ensemble des suites de n variables et degrés $d_1, \ldots, d_m$ qui sont régulières est un ouvert non vide de Zariski (donc dense).
- il n'y a pas de réduction à zéro dans l'algorithme F_5.

.

Propriétés des suites régulières

Si $f_1, \ldots, f_m$ est une suite régulière homogène, $d_i = \deg(f_i)$, alors :

- la série de Hilbert de $f_1, \ldots, f_m$ est

$$\sum_{d \geq 0} \mathrm{HF}_I(d) z^d = \prod_{i=1}^{m} (1 - z^{d_i}) \Big/ (1 - z)^n \qquad (1)$$

- l'idéal $\langle f_1, \ldots, f_m \rangle$ est de dimension $n - m$,
- le degré de I est $\prod_{i=1}^{m} d_i$ (borne de Bezout).
- « généricité » : presque toute suite est une suite régulière : l'ensemble des suites de n variables et degrés $d_1, \ldots, d_m$ qui sont régulières est un ouvert non vide de Zariski (donc dense).
- il n'y a pas de réduction à zéro dans l'algorithme F_5.

caractérisation.

Complexité pour des systèmes réguliers

Proposition (Lazard 1983, Giusti 1994)

À un changement linéaire générique prêt de coordonnées, le degré de régularité de l'idéal est majoré par la borne de Macaulay :

$$d_{\text{reg}} \leq \sum_{i=1}^{m} (d_i - 1) + 1$$

Complexité simplement exponentielle en le nombre de variables !

Complexité pour des systèmes réguliers

Proposition (Lazard 1983, Giusti 1994)

À un changement linéaire générique prêt de coordonnées, le degré de régularité de l'idéal est majoré par la borne de Macaulay :

$$d_{\text{reg}} \leq \sum_{i=1}^{m} (d_i - 1) + 1$$

Complexité simplement exponentielle en le nombre de variables !

Cas $m = n$: $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ régulière, $\delta = (\sum_{i=1}^{n} d_i)/n$

La complexité du calcul de la base de Gröbner est bornée par

$$\left(\frac{\delta^\delta}{(\delta-1)^{\delta-1}} \right)^{\omega n} n^{2-\omega/2} \left((\delta-1) \left(\frac{\delta}{2\pi(\delta-1)^3} \right)^{\frac{\omega}{2}} + O(1/n) \right), \quad n \to \infty,$$

Complexité fine : algorithme F_5

- La matrice de Macaulay est très structurée : peut-on améliorer la complexité de l'algèbre linéaire utilisée ?
- Peut-on prédire les réductions à zéro de lignes ?

Complexité fine : algorithme F_5

- La matrice de Macaulay est très structurée : peut-on améliorer la complexité de l'algèbre linéaire utilisée ?
- Peut-on prédire les réductions à zéro de lignes ?

Algorithme F_5 (Faugère 2002)

- critère permettant d'éliminer toutes les syzygies triviales.
- pour des systèmes réguliers : aucune réduction à 0.
- algèbre linéaire incrémentale en i et d.

Analyse de complexité : résultats

- Systèmes réguliers ($m < n$) : coût de l'algèbre linaire de F_5.
- Systèmes de dimension 0 « semi-réguliers » : calcul du degré de régularité en fonction du nombre d'équations.

Position de Noether simultanée

Définition

Les variables $(x_1, \ldots, x_m)$ sont en *position de Noether* par rapport au système $(f_1, \ldots, f_m)$ si leurs images canoniques dans $k[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle$ sont des entiers algébriques sur $k[x_{m+1}, \ldots, x_n]$ et si $k[x_{m+1}, \ldots, x_n] \cap \langle f_1, \ldots, f_m \rangle = \langle 0 \rangle$.

Cela implique que $(f_1, \ldots, f_m, x_{m+1}, \ldots, x_n)$ est régulière.

Position de Noether simultanée

Définition

Les variables $(x_1, \ldots, x_m)$ sont en *position de Noether* par rapport au système $(f_1, \ldots, f_m)$ si leurs images canoniques dans $k[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle$ sont des entiers algébriques sur $k[x_{m+1}, \ldots, x_n]$ et si $k[x_{m+1}, \ldots, x_n] \cap \langle f_1, \ldots, f_m \rangle = \langle 0 \rangle$.

Cela implique que $(f_1, \ldots, f_m, x_{m+1}, \ldots, x_n)$ est régulière.

Position de Noether simultanée (PNS)

Les variables $(x_1, \ldots, x_n)$ sont en *position de Noether simultanée* par rapport au système $(f_1, \ldots, f_m)$ si les variables $(x_1, \ldots, x_i)$ sont en position de Noether par rapport à $(f_1, \ldots, f_i)$ pour tout $i \in \{1, \ldots, m\}$.

Position de Noether simultanée

Définition

Les variables $(x_1, \ldots, x_m)$ sont en *position de Noether* par rapport au système $(f_1, \ldots, f_m)$ si leurs images canoniques dans $k[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle$ sont des entiers algébriques sur $k[x_{m+1}, \ldots, x_n]$ et si $k[x_{m+1}, \ldots, x_n] \cap \langle f_1, \ldots, f_m \rangle = \langle 0 \rangle$.

Cela implique que $(f_1, \ldots, f_m, x_{m+1}, \ldots, x_n)$ est régulière.

Position de Noether simultanée (PNS)

Les variables $(x_1, \ldots, x_n)$ sont en *position de Noether simultanée* par rapport au système $(f_1, \ldots, f_m)$ si les variables $(x_1, \ldots, x_i)$ sont en position de Noether par rapport à $(f_1, \ldots, f_i)$ pour tout $i \in \{1, \ldots, m\}$.

Si $\mathbb{K}$ est infini, tout système régulier peut être mis en PNS par un changement linéaire générique de coordonnées.

L'algorithme F_5 matriciel, ordre grevlex

- Les lignes de $\mathscr{M}_d$ sont indexées par $(i, \tau) \in \{1, \ldots, m\} \times \mathscr{T}_{d-d_i}$ où $\mathscr{T}_d$ désigne l'ensemble des monômes de degré d.

L'algorithme F_5 matriciel, ordre grevlex

- Les lignes de $\mathscr{M}_d$ sont indexées par $(i, \tau) \in \{1, \ldots, m\} \times \mathscr{T}_{d-d_i}$ où $\mathscr{T}_d$ désigne l'ensemble des monômes de degré d.
- Les lignes sont triées selon leur index : $s' = (j', u') < s = (j, u)$ si $j' < j$ ou $(j = j'$ et $u' < u)$.

L'algorithme F_5 matriciel, ordre grevlex

- Les lignes de $\mathscr{M}_d$ sont indexées par $(i, \tau) \in \{1, \ldots, m\} \times \mathscr{T}_{d-d_i}$ où $\mathscr{T}_d$ désigne l'ensemble des monômes de degré d.
- Les lignes sont triées selon leur index : $s' = (j', u') < s = (j, u)$ si $j' < j$ ou $(j = j'$ et $u' < u)$.
- Les seules opérations autorisées sont, si on note L_s la ligne d'index s : $L_s \leftarrow L_s + \lambda L_{s'}$ avec $s' < s$, et l'index de L_s est inchangé.

L'algorithme F_5 matriciel, ordre grevlex

- Les lignes de $\mathscr{M}_d$ sont indexées par $(i,\tau) \in \{1,\ldots,m\} \times \mathscr{T}_{d-d_i}$ où $\mathscr{T}_d$ désigne l'ensemble des monômes de degré d.
- Les lignes sont triées selon leur index : $s' = (j',u') < s = (j,u)$ si $j' < j$ ou $(j = j'$ et $u' < u)$.
- Les seules opérations autorisées sont, si on note L_s la ligne d'index s : $L_s \leftarrow L_s + \lambda L_{s'}$ avec $s' < s$, et l'index de L_s est inchangé.
- Critère F_5 : soit L_s une ligne de $\mathscr{M}_{d-d_i}$ de terme de tête t (après réduction) avec $s < (i,1)$, alors la ligne $L_{(i,t)}$ se réduira à zéro.

L'algorithme F_5 matriciel, ordre grevlex

- Les lignes de $\mathscr{M}_d$ sont indexées par $(i,\tau) \in \{1,\ldots,m\} \times \mathscr{T}_{d-d_i}$ où $\mathscr{T}_d$ désigne l'ensemble des monômes de degré d.
- Les lignes sont triées selon leur index : $s' = (j',u') < s = (j,u)$ si $j' < j$ ou $(j = j'$ et $u' < u)$.
- Les seules opérations autorisées sont, si on note L_s la ligne d'index s : $L_s \leftarrow L_s + \lambda L_{s'}$ avec $s' < s$, et l'index de L_s est inchangé.
- Critère F_5 : soit L_s une ligne de $\mathscr{M}_{d-d_i}$ de terme de tête t (après réduction) avec $s < (i,1)$, alors la ligne $L_{(i,t)}$ se réduira à zéro.
- pour un système régulier, ce sont les seules.

Preuve du critère F_5

Critère F_5 : soit L_s une ligne de $\mathscr{M}_{d-d_i}$ de terme de tête t (après réduction) avec $s < (i,1)$, alors la ligne $L_{(i,t)}$ se réduira à zéro.

Par hypothèse, $t = \mathrm{LT}(h)$ avec $h = \sum_{k=1}^{i-1} h_k f_k$. Alors,

$$tf_i = hf_i + (t-h)f_i$$

Preuve du critère F_5

Critère F_5 : soit L_s une ligne de $\mathscr{M}_{d-d_i}$ de terme de tête t (après réduction) avec $s < (i,1)$, alors la ligne $L_{(i,t)}$ se réduira à zéro.

Par hypothèse, $t = \mathrm{LT}(h)$ avec $h = \sum_{k=1}^{i-1} h_k f_k$. Alors,

$$tf_i = hf_i + (t-h)f_i = \underbrace{\sum_{k=1}^{i-1} f_i h_k f_k} + \underbrace{(t-h)f_i}$$

Structure de la base de Gröbner

Remarque

Les éléments de la base de Gröbner sont les lignes qui sont réduites (et les polynômes de départ).

Structure de la base de Gröbner

Remarque

Les éléments de la base de Gröbner sont les lignes qui sont réduites (et les polynômes de départ).

Théorème (Bardet Faugère Salvy 2004-2014, arxiv 1312.1655)

Hypothèse : $(f_1, \ldots, f_m)$ en PNS.
Si g est un élément de la base de Gröbner de $f_1, \ldots, f_m$ calculé par l'algorithme F_5 pour l'ordre grevlex, soit $s = (i, t)$ l'index de la ligne ayant permis le calcul de g, alors

$$\mathrm{LT}(g) \in \mathbb{K}[x_1, \ldots, x_i] \text{ et } t \in \mathbb{K}[x_1, \ldots, x_{i-1}]$$

Exemple

$$f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$$
$$f_2 = \quad + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
x_1F_2		1	-5		5	4		-5		

Exemple

$$f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$$
$$f_2 = \quad + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	

Réduction de x_1F_2 par x_2F_1 et x_2F_2.

Exemple

$f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$
$f_2 = \quad + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	

Réduction de x_1F_2 par x_2F_1 et x_2F_2.
$\mathrm{LT}(x_1F_2) \in \mathbb{K}[x_1, x_2]$.

Exemple

$f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$
$f_2 = \quad + 1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	

Réduction de x_1F_2 par x_2F_1 et x_2F_2.
$\mathrm{LT}(x_1F_2) \in \mathbb{K}[x_1, x_2]$.
degré maximal : 3.

Exemple

$$f_1 = 1x_1^2 + 1x_1x_2 + 2x_2^2 - 1x_1x_3 - 3x_2x_3 + 4x_3^2$$
$$f_2 = +1x_1x_2 - 5x_2^2 + 5x_1x_3 + 4x_2x_3 - 5x_3^2$$
$$f_3 = 1x_2^2 + 1x_1x_3 - 2x_2x_3 + 3x_3^2$$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	
x_3F_3							1	1	-2	3
$\underline{x_2F_3}$				1		1	-2		3	
$\underline{x_1F_3}$			1		1	-2		3		

Exemple

$$f_1 = 1x_1^2+1x_1x_2+2x_2^2-1x_1x_3-3x_2x_3+4x_3^2$$
$$f_2 = +1x_1x_2-5x_2^2+5x_1x_3+4x_2x_3-5x_3^2$$
$$f_3 = 1x_2^2+1x_1x_3-2x_2x_3+3x_3^2$$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	
x_3F_3							1	1	-2	3
$\underline{x_2F_3}$								-573	355	-499
$\underline{x_1F_3}$			1		1	-2		3		

Réduction de x_2F_3 par x_1F_2 et x_3F_1, x_3F_2, x_3F_3.

Exemple

$$f_1 = 1x_1^2+1x_1x_2+2x_2^2-1x_1x_3-3x_2x_3+4x_3^2$$
$$f_2 = +1x_1x_2-5x_2^2+5x_1x_3+4x_2x_3-5x_3^2$$
$$f_3 = 1x_2^2+1x_1x_3-2x_2x_3+3x_3^2$$

	x_1^3	$x_1^2x_2$	$x_1x_2^2$	x_2^3	$x_1^2x_3$	$x_1x_2x_3$	$x_2^2x_3$	$x_1x_3^2$	$x_2x_3^2$	x_3^3
x_3F_1					1	1	2	-1	-3	4
x_2F_1		1	1	2		-1	-3		4	
x_1F_1	1	1	2		-1	-3		4		
x_3F_2						1	-5	5	4	-5
x_2F_2			1	-5		5	4		-5	
$\underline{x_1F_2}$				-32	5	35	27	-5	-34	
x_3F_3							1	1	-2	3
$\underline{x_2F_3}$								-573	355	-499
$\underline{x_1F_3}$									2029	452

Réduction de x_1F_3 par x_2F_2, x_1F_2, x_3F_1, x_3F_2, x_3F_3, x_2F_3.

Exemple

En degré 4 : les polynômes qui se réduisent sont :

- $x_1^2 F_2$ mais par les critères de F_5 il va se réduire à 0.
- $x_2^2 F_3$ qui donne x_3^4
- $x_1 x_2 F_3$ mais par les critères de F_5 il va se réduire à 0.
- $x_1^2 F_3$ mais par les critères de F_5 il va se réduire à 0.

Degré maximal : 4.

Complexité de l'algorithme F_5

Théorème (Bardet, Faugère, Salvy) (homogène, grevlex)

Notons G_i une base de Gröbner réduite de $f_1, \ldots, f_i$.
Le nombre de polynômes de degré d dans G_i dont le terme de tête n'est pas dans $\mathrm{LT}(G_{i-1})$ est majoré par $b_d^{(i)}$, où

$$B_i(z) = \sum_{d=0}^{\infty} b_d^{(i)} z^d = z^{d_i} \prod_{k=1}^{i-1} \frac{1-z^{d_k}}{1-z}. \qquad (2)$$

Corollaire

Le nombre d'opérations dans $\mathbb{K}$ de l'algorithme F_5 matriciel est majoré par

$$N_{F_5} = \sum_{i=1}^{m} \sum_{d=\delta}^{D} b_d^{(i)} \binom{i+d-1}{d} \binom{n+d-1}{d}.$$

Complexité de l'algorithme F_5

Théorème (Bardet, Faugère, Salvy 2004-2014-)

$(f_1,\dots,f_n)\in\mathbb{K}[x_1,\dots,x_n]$ homogènes, $\deg(f_i)=\delta\geq 2$, tels que $(x_1,\dots,x_n)$ soit en position de Noether simultanée par rapport aux f_i. Alors le nombre d'opérations arithmétiques dans $\mathbb{K}$ nécessaires pour calculer une base de Gröbner de I par l'algorithme F_5 pour l'ordre grevlex est majoré par

$$B(\delta)^n n(A(\delta)+O(1/n)),\quad n\to\infty, \tag{3}$$

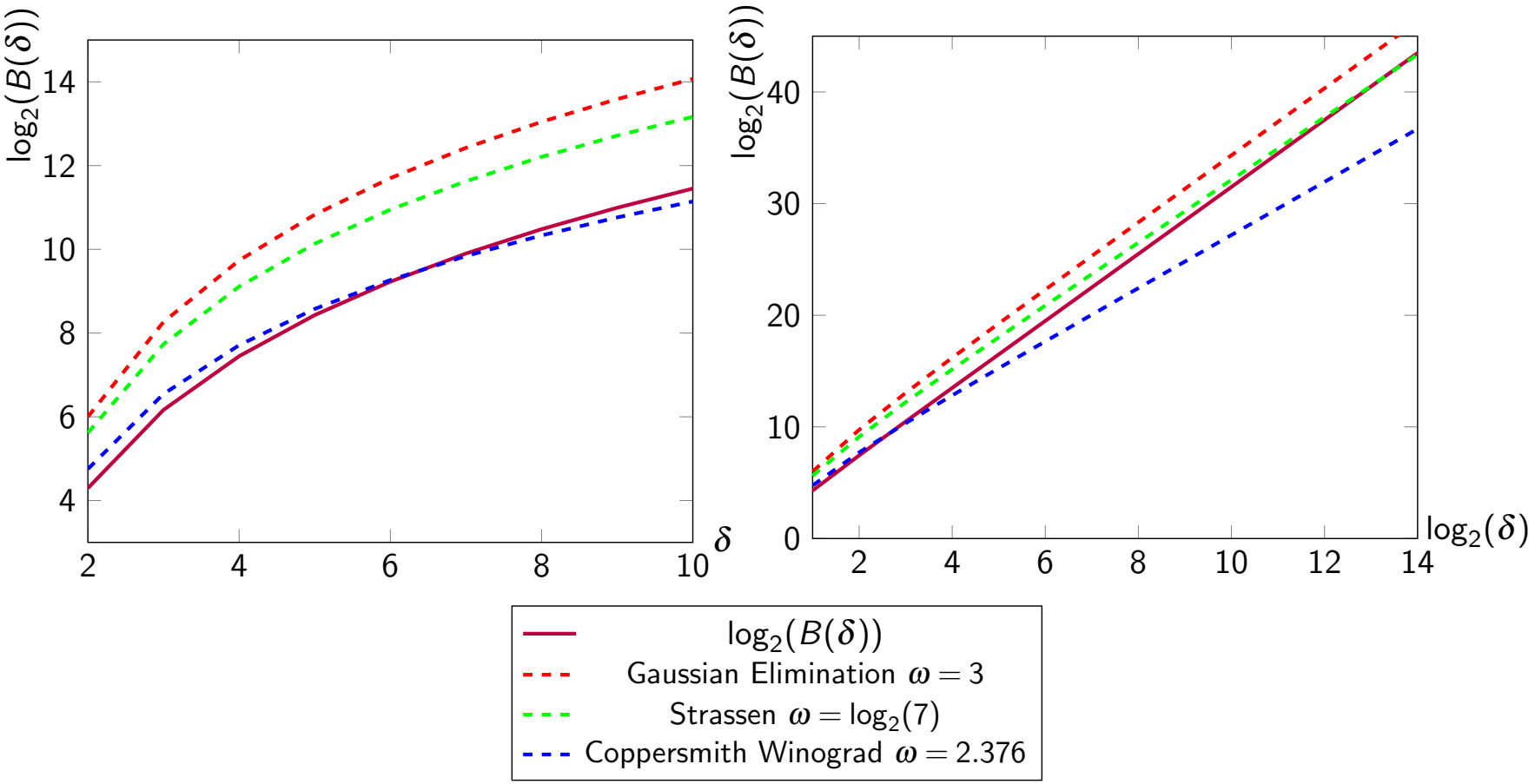
où $\lambda_0\in[\frac{\delta-1}{2},\delta-1]$ unique racine >0 de $\left(\frac{\lambda+1}{\lambda}\right)^{2\delta}=\frac{1}{1-\delta\frac{(\lambda+1)^2-\lambda^2}{(\lambda+1)^3-\lambda^3}}$

$$B(\delta)=\frac{\left(\frac{\lambda_0+1}{\lambda_0}\right)^{2\delta}-1}{\frac{1}{\lambda_0^2}-\frac{1}{(\lambda_0+1)^2}}\geq\delta^3\quad\text{et}\quad A(\delta)=\frac{1-\delta^{-1}}{2\pi}\cdot\frac{\left(1+\lambda_0^{-1}\right)^3-1}{1+\lambda_0}$$

Complexité de l'algorithme F_5 vs borne de Bezout

δ	2	3	4	5	6	7	8
$B(\delta)^n$	$2^{4.29\,n}$	$2^{6.16\,n}$	$2^{7.44\,n}$	$2^{8.43\,n}$	$2^{9.23\,n}$	$2^{9.90\,n}$	$2^{10.5\,n}$
$=$	$(2^n)^{4.3}$	$(3^n)^{3.9}$	$(4^n)^{3.7}$	$(5^n)^{3.6}$	$(6^n)^{3.6}$	$(7^n)^{3.5}$	$(8^n)^{3.5}$

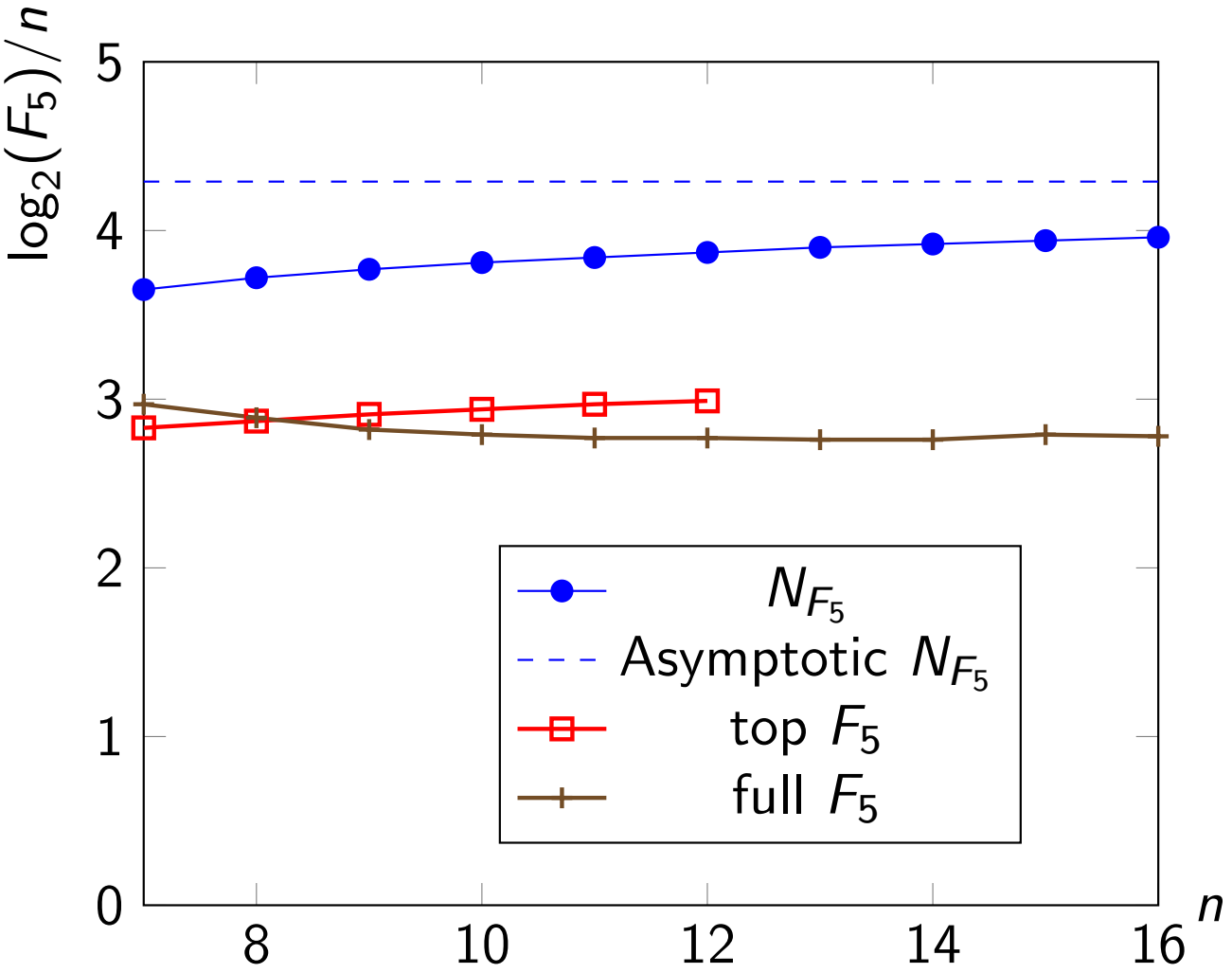
Complexité de l'algorithme F_5 vs algèbre lineaire



Intersections : $\delta = 7$

$\delta = 9911$.

Précision de la borne



Plan

Application en cryptographie

- Les systèmes cryptographiques sont sur-déterminés !
- Les systèmes réguliers sont sous-déterminés !
- La borne précédente peut quand même s'appliquer, mais est très surestimée pour des systèmes surdéterminés,
- Importance du cas booléen $x_i^2 - x_i$,
- Importance des systèmes "aléatoires".

Systèmes surdéterminés

On considère des systèmes :

- homogènes ;
- avec plus d'équations que d'inconnues ;
- avec un nombre fini de solutions ;
- pour l'ordre grevlex.

Systèmes surdéterminés

On considère des systèmes :

- homogènes ;
- avec plus d'équations que d'inconnues ;
- avec un nombre fini de solutions ;
- pour l'ordre grevlex.

Alors le degré de régularité = indice de régularité -1= degré de la série de Hilbert (qui est un polynôme).

Des systèmes réguliers aux semi-réguliers

Définition des systèmes réguliers

- Soit $(f_1, \ldots, f_m)$ un système homogène $(m \leq n)$

  La suite $(f_1, \ldots, f_m)$ est *régulière* si, pour tout $i = 1, \ldots, m$, s'il existe g tel que

  $$g f_i \in \langle f_1, \ldots, f_{i-1} \rangle$$

  alors g appartient à $\langle f_1, \ldots, f_{i-1} \rangle$.

Des systèmes réguliers aux semi-réguliers

Définition des systèmes semi-réguliers

- Soit $(f_1, \ldots, f_m)$ un système homogène $(m \geq n)$, et d_{reg} son indice de régularité.
  La suite $(f_1, \ldots, f_m)$ est *semi-régulière* si, pour tout $i = 1, \ldots, m$, s'il existe g tel que

$$gf_i \in \langle f_1, \ldots, f_{i-1} \rangle \quad \text{et} \quad \deg(gf_i) < d_{\text{reg}}$$

  alors g appartient à $\langle f_1, \ldots, f_{i-1} \rangle$.

Des systèmes réguliers aux semi-réguliers

Propriété des systèmes réguliers

Le système homogène $(f_1, \ldots, f_m)$ est régulier ssi sa série de Hilbert est

$$H_I(z) = \frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^n} \quad . \tag{4}$$

Des systèmes réguliers aux semi-réguliers

Propriété des systèmes semi-réguliers

Le système homogène $(f_1, \ldots, f_m)$ est semi-régulier ssi sa série de Hilbert est

$$H_I(z) = \left[\frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^n} \right]. \quad (4)$$

$[\sum_{n\geq 0} a_n z^n] = \sum_{n\geq 0} b_n z^n$ avec $b_n = a_n$ si $a_i \geq 0 \forall i \leq n$ et 0 sinon.

Des systèmes réguliers aux semi-réguliers

Propriété des systèmes semi-réguliers

Le système homogène $(f_1, \ldots, f_m)$ est semi-régulier ssi sa série de Hilbert est

$$H_I(z) = \left[\frac{\Pi_{j=1}^{m}(1-z^{d_j})}{(1-z)^n} \right]. \quad (4)$$

$[\sum_{n\geq 0} a_n z^n] = \sum_{n\geq 0} b_n z^n$ avec $b_n = a_n$ si $a_i \geq 0 \forall i \leq n$ et 0 sinon.

Complexité

La complexité dans $\mathbb{K}$ du calcul de la base de Gröbner est donnée par

$$O\left(mD \binom{n+D-1}{D}^{\omega} \right), \text{ quand } D \to \infty$$

où $D = \deg(H_I(z))$.

Généricité

Cas de $m = n+1$ équations à n inconnues

- La suite $\{x_1^{d_1}, \ldots, x_n^{d_n}, \sum_{\deg(m)=d_{n+1}} m\}$ est semi-régulière sur $\mathbb{Q}$.
- cas général : $H(I) \leq \left(\sum_{i=1}^{n+1}(d_i - 1) + 1\right)/2$.

$$\frac{(1-z^2)(1-z^5)}{1-z} = 1 + z - z^5 - z^6,$$

donc

$$d_{\text{reg}} = 2 < \frac{(2-1)+(5-1)+1}{2} = 3.$$

Généricité

Cas $m > n+1$: conjecture de Fröberg

- La généricité des suites semi-régulières est conjecturée si k est algébriquement clos et $m > n+1$
- Lorsque k est fini, on conjecture que "presque tout" système est semi-régulier... lorsque n est "assez grand" ! !

Généricité

Cas $m > n+1$: conjecture de Fröberg

- La généricité des suites semi-régulières est conjecturée si k est algébriquement clos et $m > n+1$
- Lorsque k est fini, on conjecture que "presque tout" système est semi-régulier... lorsque n est "assez grand" ! !

Mais. . .

- Pour m, n et les d_i fixés, on peut prouver la généricité en tirant un système au hasard (k algébriquement clos),

Analyse asymptotique : méthode

Analyse complexe

- Écrire le d-ème coefficient de la série de Hilbert $\mathrm{HF}_I(d)$ sous forme d'une intégrale de Cauchy :

$$\mathrm{HF}_I(d) = [z^d]\,\mathrm{HS}_I(z) = \frac{1}{2i\pi}\oint \frac{\prod_{i=1}^{m} 1 - z^{d_i}}{(1-z)^n}\,\frac{1}{z^{d+1}}\,dz$$

- Calcul du développement asymptotique ($n \to \infty$) par des méthodes de calcul de points cols.
- Annulation du développement asymptotique donne un développement asymptotique de d_{reg} ($n \to \infty$).

Analyse asymptotique de l'indice de régularité

Rappel : cas $m = n$, $d_i = D$

$$d_{\text{reg}} = n(D-1)+1$$

Analyse asymptotique de l'indice de régularité

Rappel : cas $m = n$, $d_i = D$

$$d_{\text{reg}} = n(D-1)+1$$

Théorème BFS : cas $m = n+c$, $d_i = D$

L'indice de régularité d'un système semi-régulier de $m = n+c$ polynômes homogènes de degré D se comporte asymptotiquement comme

$$d_{\text{reg}} = n\frac{D-1}{2} - \alpha_c\sqrt{n\frac{D^2-1}{6}} + o(\sqrt{n}) \text{ lorsque } n \to \infty. \quad (5)$$

où α_c est le plus grand zéro du $c$ème polynôme de Hermite ($\alpha_1 = 0$).

Polynômes de Hermite

$$H_c(x) = \frac{2^c}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-u^2} (x + iu)^c \, du.$$

Valeur de la plus grande racine α_c du $c^{\text{ème}}$ polynôme de Hermite :				
c	1	2	3	4
α_c	0	$\frac{1}{\sqrt{2}} \simeq 0.707$	$\sqrt{\frac{3}{2}} \simeq 1.22$	$\left(\frac{3}{2} + \sqrt{\frac{3}{2}}\right)^{\frac{1}{2}} \simeq 1.65$
c	5			
α_c	$\alpha_5 = \left(\frac{5}{2} + \sqrt{\frac{5}{2}}\right)^{\frac{1}{2}} \simeq 2.02$			

Analyse asymptotique de l'indice de régularité

Théorème BFS : cas $m = n + k$, d_i

L'indice de régularité d'un système semi-régulier de $m = n + c$ polynômes homogènes de degré $d_1, \ldots, d_m$ en n variables en caractéristique 0, où c entier positif fixé, se comporte asymptotiquement comme

$$\sum_{i=1}^{m} \frac{d_i - 1}{2} - \alpha_c \sqrt{\sum_{i=1}^{m} \frac{d_i^2 - 1}{6}} + \frac{c}{2} + o(1), \qquad n \to \infty,$$

Analyse asymptotique de l'indice de régularité

Théorème BFS : cas $m = [\alpha n]$, $d_i = 2$

$$d_{\text{reg}} = (\alpha - 1/2 - \sqrt{\alpha(\alpha-1)})n + \frac{-a_1}{2(\alpha(\alpha-1))^{\frac{1}{6}}} n^{\frac{1}{3}} + O(1)$$

Analyse asymptotique de l'indice de régularité

Théorème BFS

L'indice de régularité d'un système semi-régulier de $m = [\alpha n]$ polynômes homogènes de degré $d_1, \ldots, d_m$ en n variables en caractéristique 0, où $\alpha > 1$ réel fixé, se comporte asymptotiquement comme

$$\phi(\rho)n - a_1 \left(\frac{-\rho^2}{2}\phi''(\rho)\right)^{\frac{1}{3}} n^{\frac{1}{3}} + \left(-\frac{1}{2} - \frac{1}{6}\frac{\phi^{(3)}(\rho)}{\phi''(\rho)}\rho\right) + o\left(\frac{1}{n^{\frac{1}{3}}}\right),$$

quand $n \to \infty$, avec $\phi(z) = \frac{z}{1-z} - \frac{1}{n}\sum_{i=1}^{m} \frac{d_i z^{d_i}}{1-z^{d_i}}$, ρ est la racine positive de $\phi'(z)$, et a_1 la plus grande racine de la fonction d'Airy Ai.

Analyse asymptotique de l'indice de régularité

Cas particuliers $d_i = 2$, $m = \alpha n$

α	développement asymptotique de d_{reg}, en $O(\frac{1}{n^{2/3}})$
2	$d_{\text{reg}} = 0.085786\, n + 1.0415\, n^{1/3} - 1.4697 + 1.7130\, \frac{1}{n^{1/3}}$
3	$d_{\text{reg}} = 0.050510\, n + 0.86725\, n^{1/3} - 1.4897 + 1.9958\, \frac{1}{n^{1/3}}$
4	$d_{\text{reg}} = 0.035898\, n + 0.77263\, n^{1/3} - 1.4948 + 2.2230\, \frac{1}{n^{1/3}}$
5	$d_{\text{reg}} = 0.027864\, n + 0.70957\, n^{1/3} - 1.4969 + 2.4131\, \frac{1}{n^{1/3}}$

Semi-régularité sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2-x_1,\ldots,x_n^2-x_n\rangle$

Syzygies

Les syzygies triviales sont les $f_i f_j - f_j f_i = 0$ et les $f_i f_i - f_i = 0$.

Semi-régularité sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2-x_1,\ldots,x_n^2-x_n\rangle$

Syzygies

Les syzygies triviales sont les $f_i f_j - f_j f_i = 0$ et les $f_i f_i - f_i = 0$.

Définition des systèmes semi-réguliers sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2,\ldots,x_n^2\rangle$

- Soit $(f_1,\ldots,f_m)$ un système homogène de dimension 0, et d_{reg} son indice de régularité.
  La suite $(f_1,\ldots,f_m)$ est *semi-régulière* si, pour tout $i=1,\ldots,m$, il existe g tel que, si

$$gf_i \in \langle f_1,\ldots,f_{i-1}\rangle \quad \text{et} \quad \deg(gf_i) < d_{\text{reg}}$$

  alors g appartient à $\langle f_1,\ldots,f_i\rangle$.

Semi-régularité sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2-x_1,\ldots,x_n^2-x_n\rangle$

Définition des systèmes semi-réguliers sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2-x_1,\ldots,x_n^2-x_n\rangle$

$(f_1,\ldots,f_m)$ est semi-régulière si $(f_1^h,\ldots,f_m^h)$ l'est sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2,\ldots,x_n^2\rangle$, où f_i^h est la partie homogène de plus haut degré de f_i.

Caractérisation

La série de Hilbert de ces suites vaut

$$H_m(z)=\left[\frac{(1+z)^n}{\prod_{i=1}^m(1+z^{d_i})}\right].$$

Semi-régularité sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2-x_1,\ldots,x_n^2-x_n\rangle$

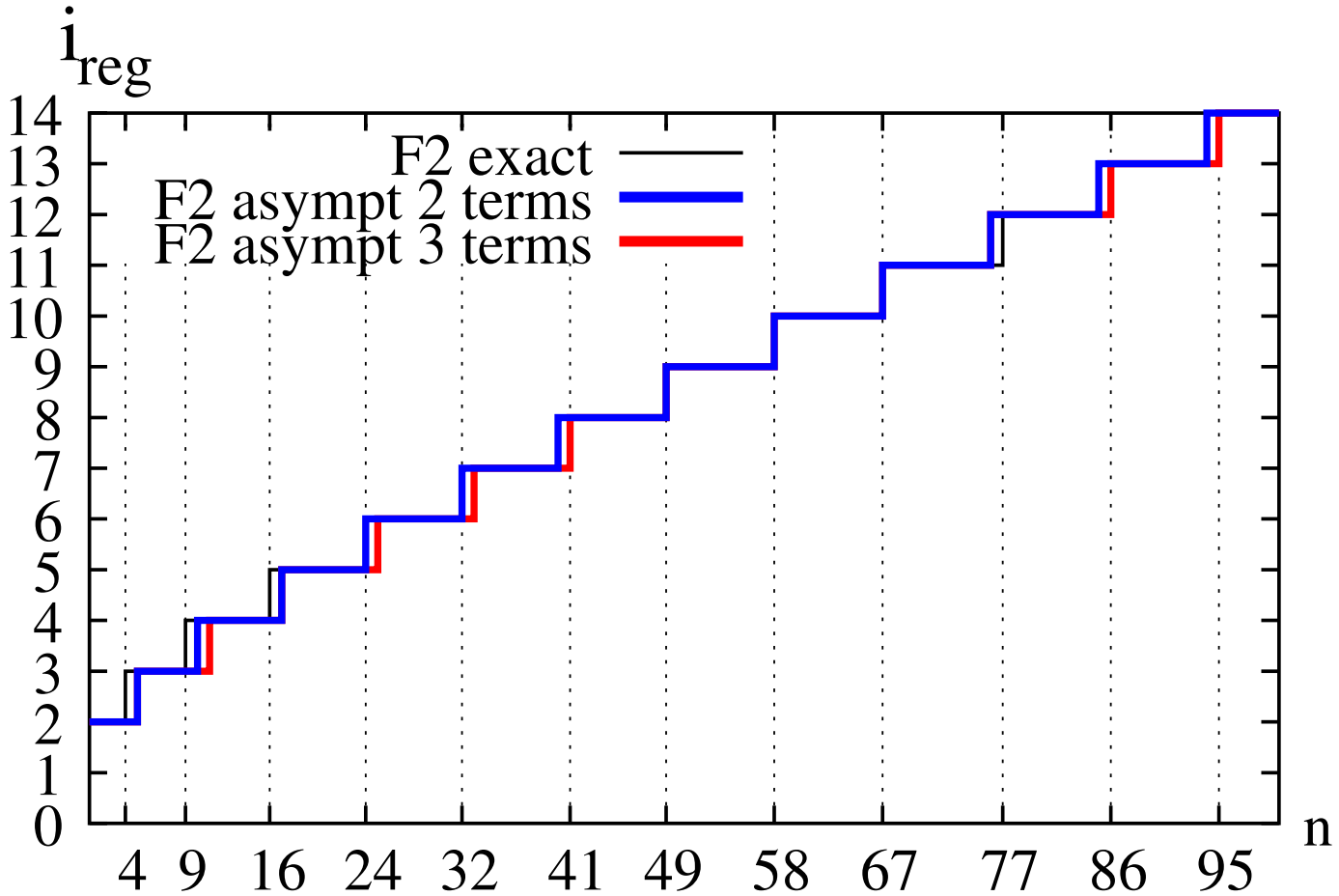
$m=n$, équations quadratiques $d_i=2$, $a_1\simeq -2,338$

$$d_{\text{reg}} = \frac{1}{\lambda_0}n - a_1\left(\frac{3}{2}\right)^{\frac{1}{2}}\left(\frac{13}{3\sqrt{3}}-\frac{5}{2}\right)^{\frac{1}{6}} n^{\frac{1}{3}} - 1 - \left(\frac{265}{648}-\frac{85}{36}\lambda_0-\frac{16}{27}\lambda_0^2-\frac{38}{81}\lambda_0^3\right)^{\frac{1}{3}}$$
$$+\left(\left(\frac{31}{108}+\frac{71}{216}\lambda_0+\frac{1}{18}\lambda_0^3+\frac{13}{108}\lambda_0^2\right)^{\frac{1}{3}} -$$
$$\left(\frac{152231}{2187000}+\frac{1159}{16200}\lambda_0+\frac{2386}{91125}\lambda_0^2+\frac{3062}{273375}\lambda_0^3\right)^{\frac{1}{3}}\right)\frac{a_1^2}{n^{\frac{1}{3}}}+o\left(\frac{1}{n^{\frac{1}{3}}}\right)$$

où $\lambda_0 = -1/2+3/2\sqrt{2/\sqrt{3}-1}\simeq 11.114$

$$d_{\text{reg}} = 0.0900\,n + 1.00\,n^{\frac{1}{3}} - 1.58 + \frac{1.41}{n^{\frac{1}{3}}} + o\left(\frac{1}{n^{\frac{1}{3}}}\right)$$

Cas booléen ($d_i = 2$), $m = n$ équations



Semi-régularité sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle x_1^2-x_1,\ldots,x_n^2-x_n\rangle$

Théorème

L'indice de régularité d'un système semi-régulier de $m=[\alpha n]$ polynômes de degré $d_1,\ldots,d_m$ sur $\mathbb{F}_2[x_1,\ldots,x_n]/\langle (x_i^2-x_i)_{i=1\ldots n}\rangle$, où $\alpha>1$ réel fixé, se comporte asymptotiquement comme

$$\phi(\rho)n - a_1\left(\frac{-\rho^2}{2}\phi''(\rho)\right)^{\frac{1}{3}} n^{\frac{1}{3}} + \left(-\frac{1}{2}-\frac{1}{6}\frac{\phi^{(3)}(\rho)}{\phi''(\rho)}\rho\right) + o\left(\frac{1}{n^{\frac{1}{3}}}\right),$$

$n\to\infty$, $\phi(z)=\frac{z}{1+z}-\frac{1}{n}\sum_{i=1}^{\alpha n}\frac{d_i z^{d_i}}{1+z^{d_i}}$, $\rho>0$ est la racine de $\phi'(z)$.

Analyse asymptotique

Cas de $m = n$ équations de degré $d_i = D$ sur $\mathbb{F}_2$

D	développement asymptotique de d_{reg}, en $O(\frac{1}{n^{1/3}})$
2	$d_{\text{reg}} = 0.09n + 1.00n^{\frac{1}{3}} - 1.58$
3	$d_{\text{reg}} = 0.15n + 1.35n^{\frac{1}{3}} - 1.42$
4	$d_{\text{reg}} = 0.20n + 1.60n^{\frac{1}{3}} - 1.27$
5	$d_{\text{reg}} = 0.24n + 1.79n^{\frac{1}{3}} - 1.11$
6	$d_{\text{reg}} = 0.26n + 1.95n^{\frac{1}{3}} - 0.94$
7	$d_{\text{reg}} = 0.28n + 2.09n^{\frac{1}{3}} - 0.78$

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : 10 équations, 10 variables, degré 2, degré secret 3.

$$\begin{cases}
x_1x_2+x_1x_3+x_1x_5+x_1x_6+x_1x_8+x_2x_3+x_2x_6+x_3x_5+x_3x_7+x_3x_8+x_3x_{10}+x_3+x_4x_7+x_4\\
x_1x_3+x_1x_5+x_1x_7+x_1x_8+x_1x_9+x_2x_5+x_2x_9+x_2x_{10}+x_2+x_3x_4+x_3x_5+x_3x_6+x_3x_7+x_3\\
x_1x_2+x_1x_4+x_1x_5+x_1x_6+x_1x_7+x_1x_8+x_1x_9+x_2x_5+x_2x_6+x_2x_8+x_2x_9+x_2x_{10}+x_2+x_3\\
x_1x_3+x_1x_4+x_1x_6+x_1x_9+x_1x_{10}+x_2x_4+x_2x_6+x_2x_8+x_2x_{10}+x_3x_5+x_3x_6+x_3x_8+x_3x_{10}\\
x_1x_2+x_1x_4+x_1x_6+x_1x_8+x_1x_9+x_2x_3+x_2x_4+x_2x_9+x_2+x_3x_5+x_3x_6+x_3x_7+x_3x_8+x_3\\
x_1x_2+x_1x_4+x_1x_5+x_1x_8+x_1x_9+x_2x_3+x_2x_4+x_2x_9+x_2+x_3x_4+x_3x_5+x_3x_6+x_3x_7+x_3\\
x_1x_3+x_1x_5+x_1x_6+x_1x_{10}+x_2x_4+x_2x_8+x_2x_9+x_3x_6+x_3x_8+x_4x_5+x_4x_7+x_4x_9+x_5x_8+\\
x_1x_2+x_1x_4+x_1x_5+x_1+x_2x_7+x_2x_8+x_2x_9+x_2x_{10}+x_3x_8+x_3x_{10}+x_4x_5+x_4x_6+x_4x_7+x_4\\
x_1x_2+x_1x_4+x_1x_5+x_1x_6+x_1x_7+x_1x_8+x_1+x_2x_4+x_2x_7+x_2x_8+x_2x_{10}+x_3x_4+x_3x_5+x_3\\
x_1x_2+x_1x_7+x_1x_9+x_1+x_2x_5+x_2x_8+x_2x_9+x_2+x_3x_7+x_3x_8+x_3x_9+x_4x_5+x_4x_6+x_4x_8+
\end{cases}$$

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2
- attaquer : résoudre $c_1 = f_1(\mathbf{x}),\ldots,c_m = f_m(\mathbf{x})$
- clef secrète : un système facile à résoudre et une "transformation".

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2
- attaquer : résoudre $c_1 = f_1(\mathbf{x}),\ldots,c_m = f_m(\mathbf{x})$
- clef secrète : un système facile à résoudre et une "transformation".

Sécurité ?

Cryptographie à clef publique

Cryptosystème type HFE [Patarin 96], TTM [Moh 99]

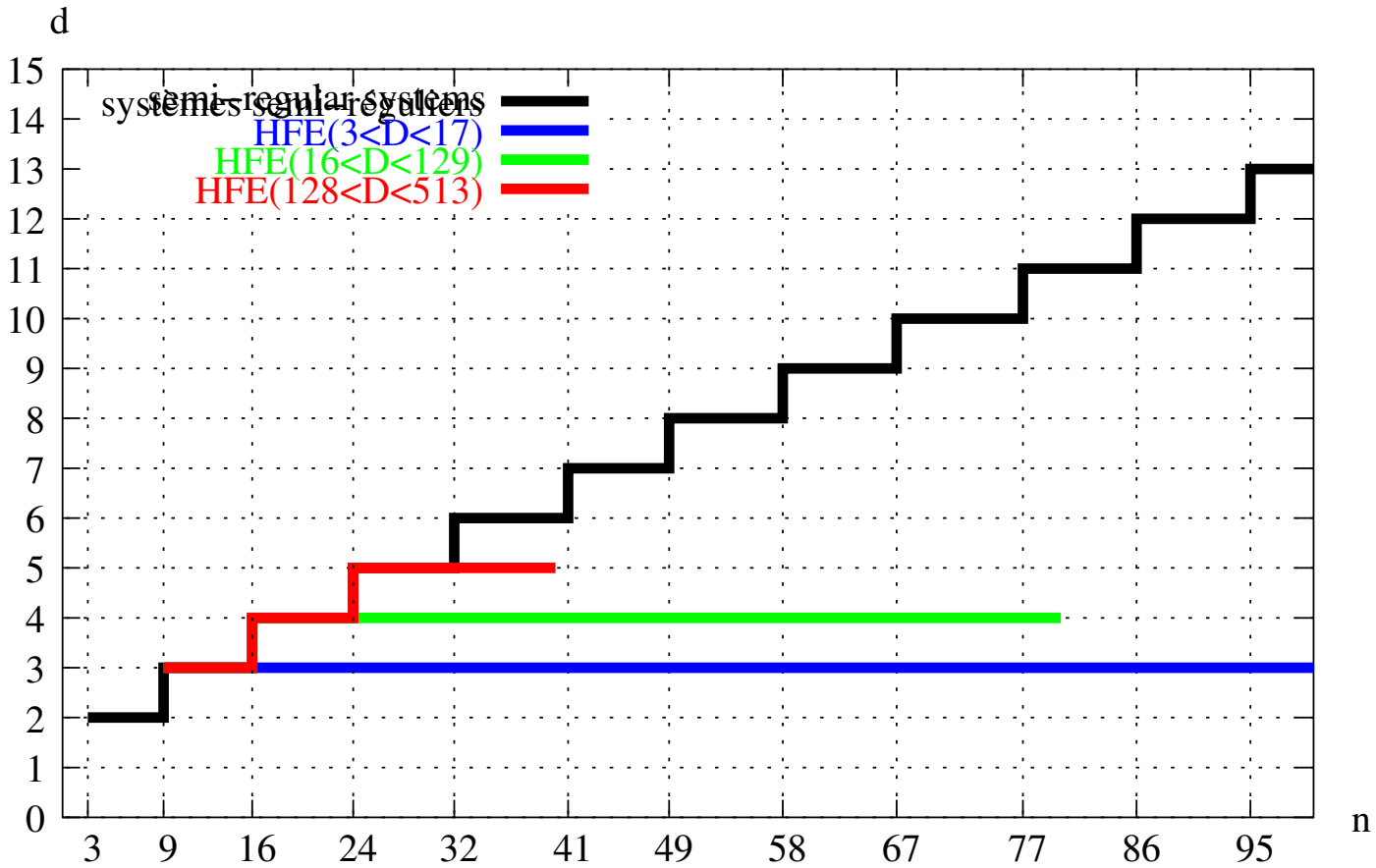
Clef publique : n équations, n variables, degré 2.

$$\begin{cases} f_1(x_1,\ldots,x_n), \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}$$

- message : $\mathbf{a} = (a_1,\ldots,a_n)$, $a_i \in \{0,1\} = \mathbb{F}_2$
- chiffrer : $(c_1,\ldots,c_n) = (f_1(\mathbf{a}),\ldots,f_m(\mathbf{a}))$ mod 2
- attaquer : résoudre $c_1 = f_1(\mathbf{x}),\ldots,c_m = f_m(\mathbf{x})$
- clef secrète : un système facile à résoudre et une "transformation".

Sécurité ? Au moins 80 variables pour une sécurité en 2^{80}

Cryptosystèmes HFE



d-régularité des systèmes HFE [Faugère-Joux, CRYPTO 03]
(D degré du polynôme secret)

Classes de complexité de problèmes algébriques

Problème Boolean Multivariate Quadratic (MQ)

Entrée : $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ polynômes quadratiques (deg 2)
Sortie : une/toutes les solutions booléennes du système

Classes de complexité de problèmes algébriques

Problème Boolean Multivariate Quadratic (MQ)

Entrée : $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ polynômes quadratiques (deg 2)
Sortie : une/toutes les solutions booléennes du système

Rappels

- problème NP-complet (réduction de 3-SAT) (*Fraenkel, Yesha* 1979) ;
- complexité arithmétique de la recherche exhaustive bornée par (pire cas) :

$$4 \cdot 2^n \log_2 n$$

(*Bouillaguet/Chen/Cheng/Chou/Niederhagen/Shamir/Yang* CHES'10).

- de nombreuses applications en cryptographie.

Applications en cryptographie

cf Pierre-Jean Spaenlehauer mercredi 26.

La sécurité de plusieurs cryptosystèmes asymétriques modernes repose directement sur ce problème

- HFE (Patarin, 1996) ;
- UOV (Kipnis, Patarin, Goubin, 1999) ;
- Polly Cracker (Albrecht, Faugère, Farshim, Perret 2011) ;

Applications en cryptographie

cf Pierre-Jean Spaenlehauer mercredi 26.

La sécurité de plusieurs cryptosystèmes asymétriques modernes repose directement sur ce problème

- HFE (Patarin, 1996) ;
- UOV (Kipnis, Patarin, Goubin, 1999) ;
- Polly Cracker (Albrecht, Faugère, Farshim, Perret 2011) ;

Sécurité prouvée

- chiffrement à flux QUAD (Berbain, Gilbert, Patarin 2006, 09) ;

Applications en cryptographie

cf Pierre-Jean Spaenlehauer mercredi 26.

La sécurité de plusieurs cryptosystèmes asymétriques modernes repose directement sur ce problème

- HFE (Patarin, 1996) ;
- UOV (Kipnis, Patarin, Goubin, 1999) ;
- Polly Cracker (Albrecht, Faugère, Farshim, Perret 2011) ;

Sécurité prouvée

- chiffrement à flux QUAD (Berbain, Gilbert, Patarin 2006, 09) ;

Cryptanalyse algébrique

- cryptosystème asymétrique McEliece (Faugère, Otmani, Perret, Tillich, 2010) ;

"On the Complexity of Solving Quadratic Boolean Systems", BFSS 2013

Sous hypothèse algébriques (γ-fortement semi-régulier)

Théorème : La complexité *arithmétique* de résolution d'un système $(f_1, \ldots, f_n)$ de $\mathbb{F}_2[x_1, \ldots, x_n]$ vérifiant l'hypothèse est :

- bornée par $O(2^{0.841n})$ (variante déterministe) ;
- d'espérance bornée par $O(2^{0.792n})$ (variante probabiliste de type *Las Vegas*[a]).

a. Résultat correct, mais la complexité de l'algorithme est une variable aléatoire.

Conjecture

Lorsque $n \to \infty$, la proportion de systèmes γ-fortement semi-réguliers tends vers 1. (expériences positives)

Application en cryptographie

Attaque par recherche exhaustive sur HFE pour une sécurité en 2^{80}

- algorithme en 2^n : il faut au minimum 80 variables ;
- algorithme en $2^{0.841n}$: il faut au minimum 96 variables ;
- algorithme en $2^{0.792n}$: il faut au minimum 101 variables ;

---

sans tenir compte des constantes dans les $O()$...

Application en cryptographie

Attaque par recherche exhaustive sur HFE pour une sécurité en 2^{80}

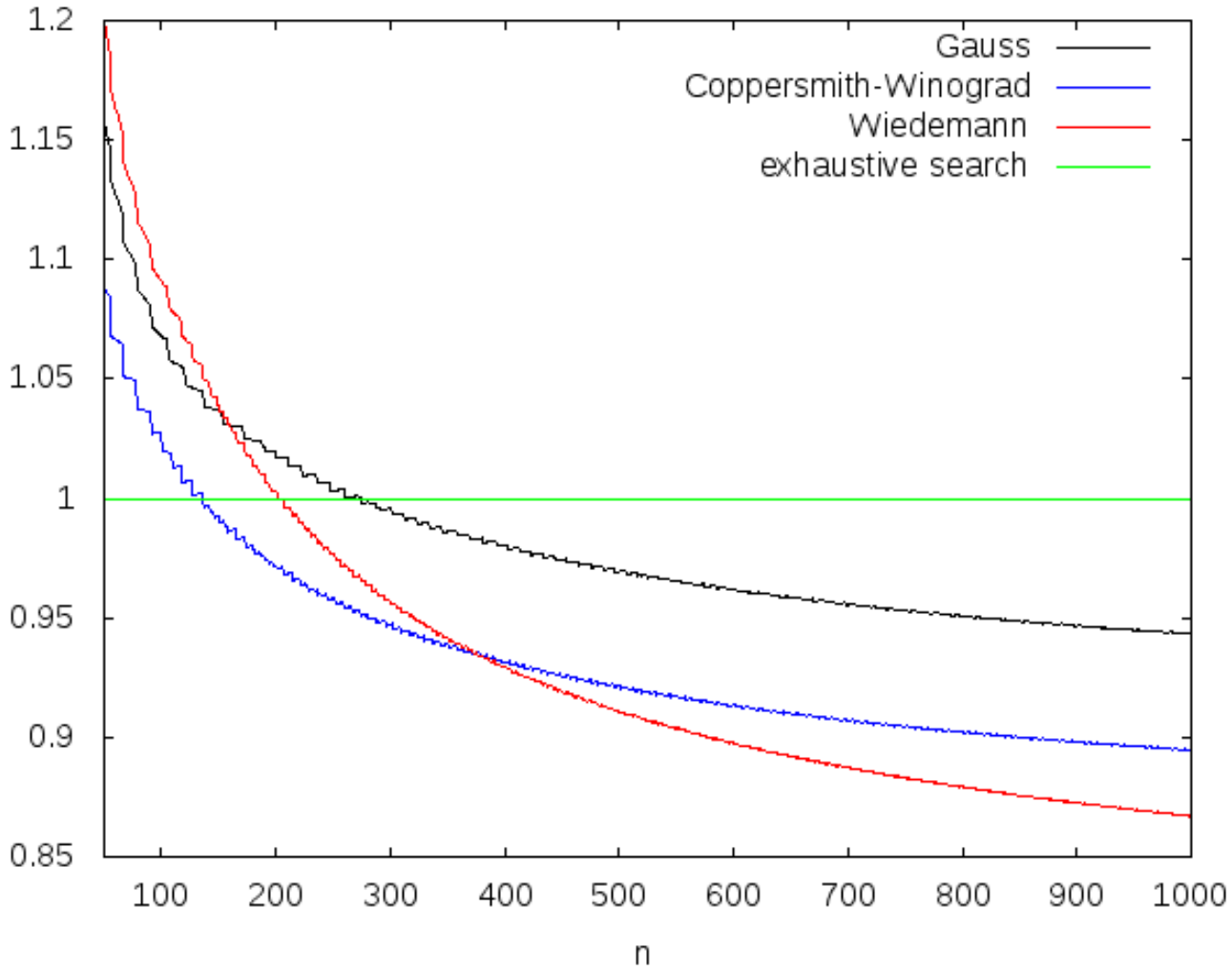
- algorithme en 2^n : il faut au minimum 80 variables ;
- algorithme en $2^{0.841n}$: il faut au minimum 96 variables ;
- algorithme en $2^{0.792n}$: il faut au minimum 101 variables ;

---

sans tenir compte des constantes dans les $O()\ldots$

En fait...

Il existe des attaques bien meilleures, le cryptosystème est cassé !
Faugère, Joux 2003 : résolution d'un système de 80 équations en 80 variables.



Valeurs de $\log_2 N/n$, où N nombre d'opérations pour un système booléen semi-régulier.

Conclusion

- Présentation des bases de Gröbner, lien avec algèbre linéaire.
- Analyse de complexité sous des hypothèses « génériques ».
- Applications en cryptographie nombreuses :
  Frédéric de Portzamparc, Faiblesse structurelle des schémas McEliece avec clefs compactes, mardi 25 mars à 11h30
  Pierre-Jean Spaenlehauer, exposé invité, mercredi 26 mars à 9h, Journées C2 2014
  et d'autres !