# Cryptanalyse

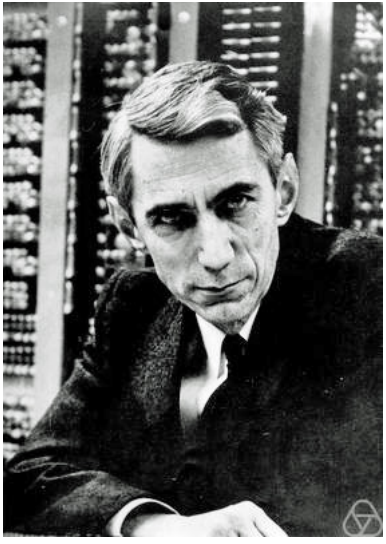
## Cours 8 - Cryptanalyse Algébrique: Introduction

Maxime Bombar

Mardi 22 Octobre

# Introduction

# Observation de Shannon

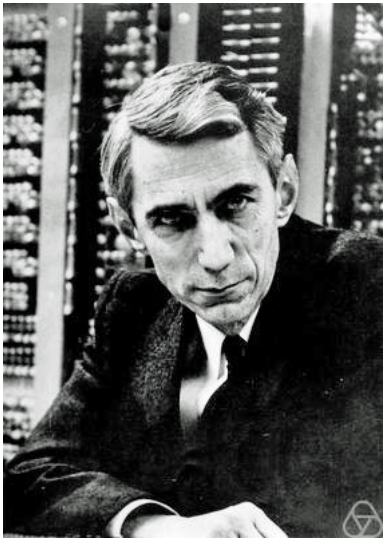


"Thus, if we could show that solving a certain system requires at least as much work as solving a system of simultaneous equations in a large number of unknowns, of a complex type, then we would have a lower bound of sorts for the work characteristic."

*Communication Theory of Secrecy Systems* (1949)

Toute fonction $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ est **polynomiale**.

# Observation de Shannon



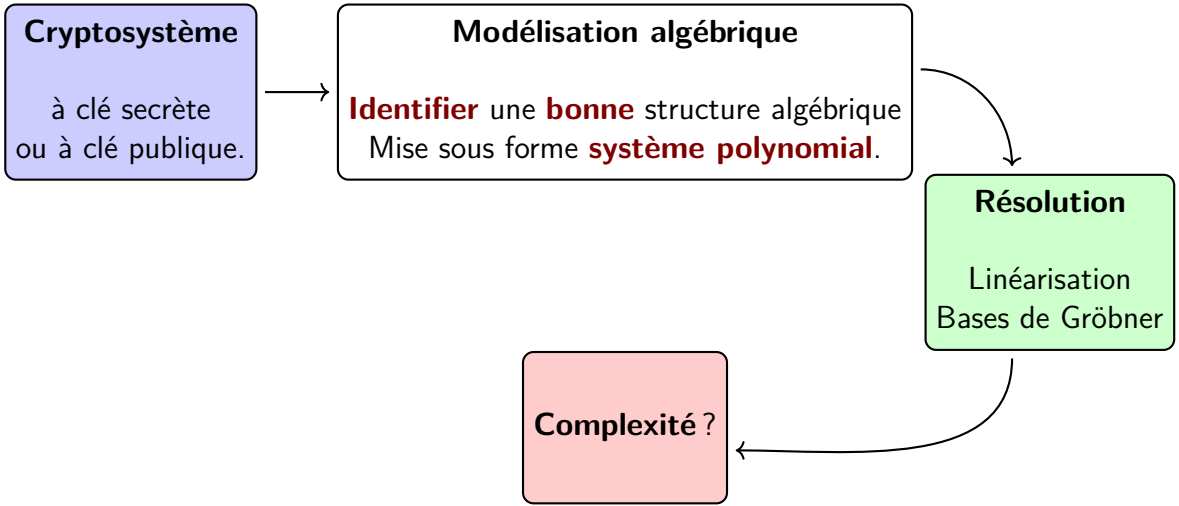
"Thus, if we could show that solving a certain system requires at least as much work as solving a system of simultaneous equations in a large number of unknowns, of a complex type, then we would have a lower bound of sorts for the work characteristic."

*Communication Theory of Secrecy Systems* (1949)

Toute fonction $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ est **polynomiale**.

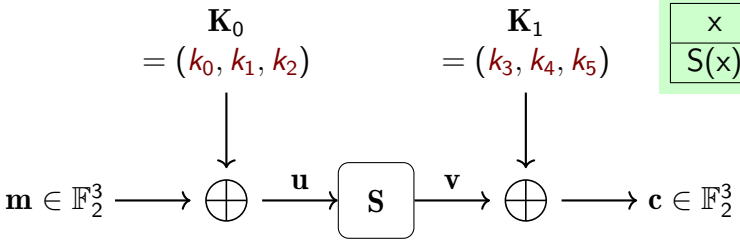
**Chaque couple** (clair-chiffré) définit un **système d'équations polynomiales** d'inconnues les bits de la clé $k$.

# Un Cadre Algébrique Général



# Chiffrement par Blocs

# Exemple : Chiffrement par blocs simple

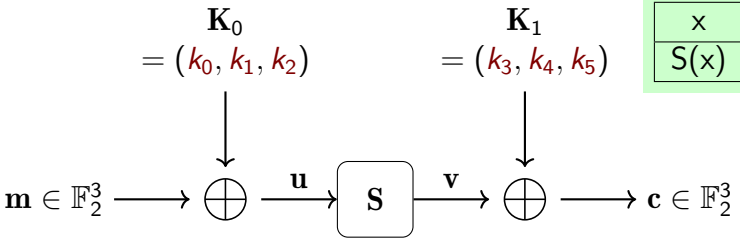



| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| S(x) | 4 | 1 | 3 | 6 | 5 | 7 | 2 | 0 |

On écrit $\mathbf{m} = (m_0, m_1, m_2)$ et $\mathbf{c} = (c_0, c_1, c_2)$

Alors $\mathbf{u} = (m_0 + k_0, m_1 + k_1, m_2 + k_2)$
$\mathbf{v} = (c_0 + k_3, c_1 + k_4, c_2 + k_5)$

# Forme Normale Algébrique de la SBox

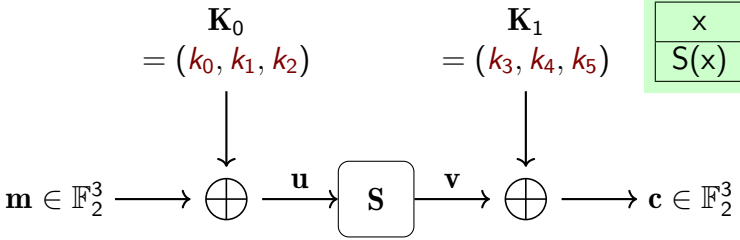



| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| S(x) | 4 | 1 | 3 | 6 | 5 | 7 | 2 | 0 |

On vérifie que $S(\mathbf{x}) = S(x_0, x_1, x_2) = (S_0(\mathbf{x}), S_1(\mathbf{x}), S_2(\mathbf{x}))$ :
(bit de poids fort à gauche : $1 \leftrightarrow (0, 0, 1)$)

$$\begin{cases} S_0 = 1 + x_1 + x_2 + x_0 x_2 \\ S_1 = x_1 + x_0 x_2 \\ S_2 = x_0 + x_1 + x_2 + x_0 x_2 \end{cases}$$

# Mise en Équation




| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| S(x) | 4 | 1 | 3 | 6 | 5 | 7 | 2 | 0 |

$$\begin{cases} c_0 + k_3 = 1 + m_1 + k_1 + m_2 + k_2 + (m_0 + k_0) \cdot (m_2 + k_2) \\ c_1 + k_4 = m_1 + k_1 + (m_0 + k_0) \cdot (m_2 + k_2) \\ c_2 + k_5 = m_0 + k_0 + m_1 + k_1 + m_2 + k_2 + (m_0 + k_0) \cdot (m_2 + k_2) \end{cases}$$

On linéarise en posant $k_6 \stackrel{\text{def}}{=} k_0 k_2$ (seul monôme de degré $>1$).
Chaque couple clair-chiffré donne 3 équations et 7 inconnues !

# Généralisation à plusieurs tours

En général, le degré du système polynomial va grossir comme $\deg(S)^{\#Tours}$. Cela peut vite devenir impossible à résoudre en linéarisant : Pour un système de degré $d$, en $n$ variables, la linéarisation peut donner jusqu'à $\sum_{r=1}^{d} \binom{n}{r}$ inconnues.

# Attention aux relations cachées !

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S(x)$ | 15 | 0 | 6 | 2 | 13 | 9 | 14 | 8 | 7 | 12 | 11 | 4 | 3 | 5 | 1 | 10 |

$$\begin{cases} S_0 = x_0x_2x_3 + x_0 + x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3 + 1 \\ S_1 = x_0x_1x_2 + x_0x_1x_3 + x_0x_1 + x_0x_2x_3 + x_0x_2 + x_0x_3 + x_3 + 1 \\ S_2 = x_0x_1x_3 + x_0x_1 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_1 + x_2x_3 + x_3 + 1 \\ S_3 = x_0x_2x_3 + x_0x_2 + x_1x_2x_3 + x_1x_3 + x_2x_3 + x_2 + x_3 + 1 \end{cases}$$

Système de degré 3

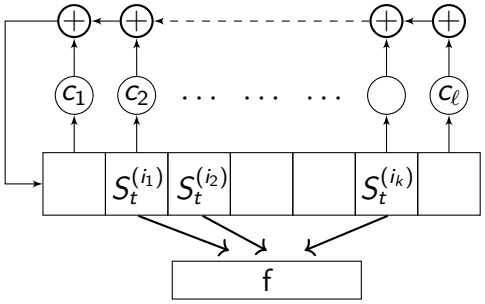
En utilisant $x_i^2 = x_i$ puisqu'on est sur $\mathbb{F}_2$ :

$$x_1x_3 + x_1S_0(x_0, x_1, x_2, x_3) + x_1S_1(x_0, x_1, x_2, x_3) = 0$$

Equation de degré 2

# Cryptanalyse de LFSR filtrés

# Rappel : LFSR filtrés




$f$ de degré $d$.

Revient à combiner $k$ LFSR avec le **même polynôme de rétroaction**

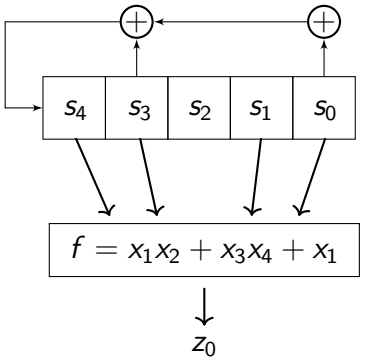
$$P(X) = 1 - \sum_{i=1}^{\ell} c_i X^i$$

mais des états initiaux décalés.

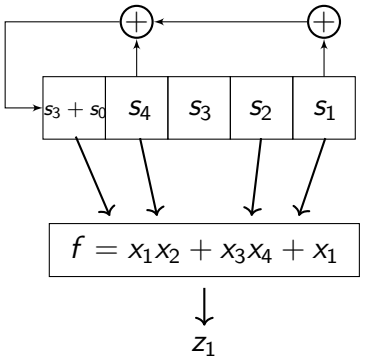
**Complexité linéaire** $\Lambda(s) \approx \sum_{i=1}^{d} \binom{\ell}{i}$

# Exemple de mise en équation

$$z_0 = s_4 s_3 + s_1 s_0 + s_1$$



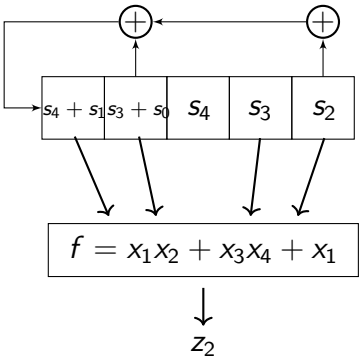
# Exemple de mise en équation




$$z_0 = s_4s_3 + s_1s_0 + s_1$$

$$\begin{aligned} z_1 &= (s_3 + s_0)s_4 + s_2s_1 + (s_3 + s_0) \\ &= s_3s_4 + s_0s_4 + s_2s_1 + s_3 + s_0 \end{aligned}$$

# Exemple de mise en équation

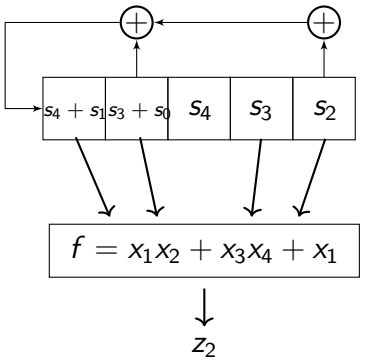



$$z_0 = s_4s_3 + s_1s_0 + s_1$$

$$\begin{aligned} z_1 &= (s_3 + s_0)s_4 + s_2s_1 + (s_3 + s_0) \\ &= s_3s_4 + s_0s_4 + s_2s_1 + s_3 + s_0 \end{aligned}$$

$$z_2 = s_4s_3 + s_4s_0 + s_1s_3 + s_1s_0 + s_3s_2 + s_4 + s_1$$

# Exemple de mise en équation




$$z_0 = s_4s_3 + s_1s_0 + s_1$$

$$\begin{aligned} z_1 &= (s_3 + s_0)s_4 + s_2s_1 + (s_3 + s_0) \\ &= s_3s_4 + s_0s_4 + s_2s_1 + s_3 + s_0 \end{aligned}$$

$$z_2 = s_4s_3 + s_4s_0 + s_1s_3 + s_1s_0 + s_3s_2 + s_4 + s_1$$

Chaque bit de $(z)$ donne une équation quadratique en $s_0, s_1, s_2, s_3, s_4$

Après linéarisation : $\binom{5}{2} + \binom{5}{1} = 15$ variables.

# Le cas général

- On a un LFSR de polynôme de rétroaction $1 \oplus c_1 X \oplus \cdots \oplus c_\ell X^\ell$
- Filtré par une fonction booléenne $f$ de degré $d$.
- Le secret est l'état initial : $S^{(0)} = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{\ell-1} \end{pmatrix}$ et la suite chiffrante est donné par $f(S^{(t)}) = f(A^t S^{(0)})$ avec

$$A \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ c_\ell & c_{\ell-1} & \cdots & c_2 & c_1 \end{pmatrix}$$

# Complexité

- Chaque bit de la suite chiffrante est une équation de degré $d$ en les secrets $s_0, \ldots, s_{\ell-1}$.
- Chaque monôme est de la forme $s_{i_1} \cdots s_{i_k}$ avec $1 \leqslant k \leqslant d$.
- On linéarise avec une variable fraîche pour chaque monôme : Au plus $N = \sum_{i=1}^{d} \binom{\ell}{i}$ variables, et on a besoin de $N$ termes.
- Système linéaire de $N$ équations à $N$ inconnues : $O(N^\omega)$ où $\omega > 2.3$. En pratique, $\omega = \log_2(7) \approx 2.8$ (Strassen).

- Pour $\ell = 256$ et $d = 10$, on a par exemple $\sum_{i=1}^{10} \binom{256}{i} > 2^{58}$.
- Pour cet exemple, cela fait alors au grand minimum $2^{131}$ opérations.

# Le cas de la clé publique

# Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

https://eprint.iacr.org/2022/214.pdf

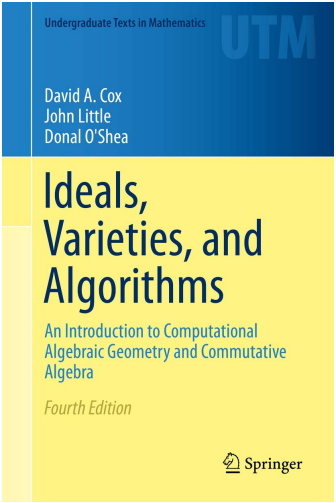
# Cryptanalyse de MinRank

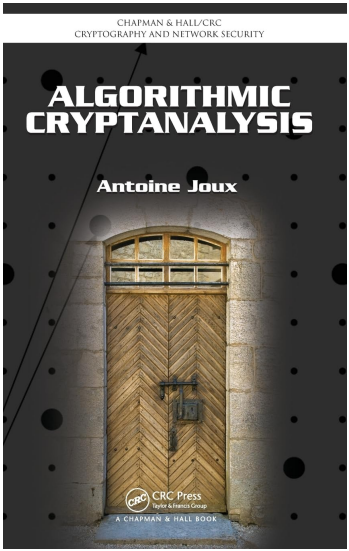
| Cryptosystème | Pré-Algébrique | Algébrique 1 (2019) | Algébrique 2 (2020) |
|---|---|---|---|
| Loidreau | 256 | 98 | 65 |
| ROLLO-128 | 128 | 117 | 71 |
| ROLLO-192 | 192 | 144 | 87 |
| ROLLO-256 | 256 | 197 | 151 |
| RQC-I | 128 | 123 | 77 |
| RQC-II | 192 | 156 | 101 |
| RQC-III | 256 | 214 | 144 |

Bardet *et al.* - *An Algebraic Attack on Rank Metric Code-Based Cryptosystems* - EUROCRYPT 2020
Bardet *et al.* - *Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems* - ASIACRYPT 2020

# Systèmes Polynomiaux, Variétés et Idéaux

# Références


Undergraduate Texts in Mathematics
UTM
David A. Cox
John Little
Donal O'Shea
Ideals, Varieties, and Algorithms
An Introduction to Computational Algebraic Geometry and Commutative Algebra
Fourth Edition
Springer


CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY
ALGORITHMIC CRYPTANALYSIS
Antoine Joux
CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

# Modélisation comme Système polynomial

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

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

- **Propriété :** Les solutions

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

donnent de l'information sur le secret.

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

# Autour de l'ensemble des solutions

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

- **Clôture algébrique :** $\overline{K}$ est infini, même pour $K = \mathbb{F}_2$.
- **Solutions parasites :** Le système peut avoir des solutions qui ne sont pas liées au secret. Dans ce cas, une optimisation consiste à rajouter les **équations de corps** :

  $$x_i^2 - x_i = 0,$$

  pour se forcer à $\mathcal{V}(f_1, \ldots, f_m) \subset \mathbb{F}_2^n$.
- **Relations algébriques :** Si $g_1, \ldots, g_m \in K[x_1, \ldots, x_m]$, et si $\mathbf{x} \stackrel{\text{def}}{=} (x_1, \ldots, x_n) \in \mathcal{V}(f_1, \ldots, f_m)$, alors

  $$\sum_{i=1}^{m} (g_i f_i)(\mathbf{x}) = 0$$

# Idéal et Variété Algébrique

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

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

Étant donné un ensemble $\{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$, l'ensemble

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

ne dépend que de l'idéal $\mathcal{I} = \langle f_i \rangle$. On l'appelle **variété algébrique** associée à $\mathcal{I}$.

# Idéaux de $K[x_1, \ldots, x_n]$

## Polynômes Univariés : $n = 1$

- Lorsque $K$ est un corps, l'anneau $K[x]$ est **principal** : tous les idéaux sont engendrés par un **unique élément**.
- Il est même **Euclidien** : cet élément est le **pgcd** des $f_i$ et on peut le calculer facilement par division euclidienne (algorithme d'Euclide).

## Nombre fini $n > 1$ de variables

- Dans le cas général, $K[x_1, \ldots, x_n]$ n'est **plus principal**.
- Par contre, il est **Noethérien** : Tout idéal $\mathcal{I}$ admet une famille génératrice **finie**.

Parmi toutes les bases de $\mathcal{I}$, il y en a certaines qui sont particulièrement pratiques pour manipuler $\mathcal{I}$ et $\mathcal{V}(\mathcal{I})$. On les appelle **Bases de Gröbner** (ou Groebner) réduites.

# Exemple : Le cas des systèmes linéaires

Pour s'échauffer, considérons ce système linéaire d'équations dans $\mathbb{F}_5[x_1, x_2, x_3]$.

$$\begin{cases} f_1 &= x_1 + 2x_2 + 2x_3 - 2 = 0 \\ f_2 &= 3x_2 + 3x_3 - 1 = 0 \\ f_3 &= 2x_1 + 3x_2 + 4x_3 - 1 = 0 \end{cases} \qquad \left(\begin{array}{ccc|c} 1 & 2 & 2 & 2 \\ 0 & 3 & 3 & 1 \\ 2 & 3 & 4 & 1 \end{array}\right)$$

# Exemple : Le cas des systèmes linéaires

Pour s'échauffer, considérons ce système linéaire d'équations dans $\mathbb{F}_5[x_1, x_2, x_3]$.

$$\begin{cases} f_1 = x_1 + 2x_2 + 2x_3 - 2 = 0 \\ f_2 = 3x_2 + 3x_3 - 1 = 0 \\ f_3 = 2x_1 + 3x_2 + 4x_3 - 1 = 0 \end{cases} \qquad \left(\begin{array}{ccc|c} 1 & 2 & 2 & 2 \\ 0 & 3 & 3 & 1 \\ 2 & 3 & 4 & 1 \end{array}\right)$$

Pivot de Gauss

$$\begin{cases} \tilde{f}_1 = x_1 - 3 = 0 \\ \tilde{f}_2 = x_2 - 3 = 0 \\ \tilde{f}_3 = x_3 - 4 = 0 \end{cases} \qquad \left(\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 4 \end{array}\right)$$

- $x_1 = 3, x_2 = 3$ et $x_3 = 4$ est solution.
- **Remarque :** On a choisit un **ordre** sur les variables : $x_1 > x_2 > x_3 > 1$.

# Systèmes de polynômes univariés

Regardons l'autre extrême

Euclide

$$\begin{cases} f_1 = x^6 + x^5 + x + 1 = 0 \\ f_2 = x^5 + x^2 + x + 1 = 0 \end{cases} \qquad \begin{cases} f_1 = (x^2+1)\cdot(x^4 + x^3 + x^2 + x + 1) \\ f_2 = (x^2+1)\cdot(x^3 + x + 1) \end{cases}$$

$$\delta = x^2 + 1 = (x+1)^2 = 0$$

- 1 est solution dans $\mathbb{F}_2$ avec **multiplicité** 2.
- $x^2 + 1$ est une **base de Gröbner** de $\langle f_1, f_2 \rangle$.
- **Remarque :** $\mathcal{V}(\langle x+1 \rangle) = \mathcal{V}(\langle x^2+1 \rangle) = \{1\}$

# Sur le nombre de solutions

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

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

# Sur le nombre de solutions

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

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

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

# Sur le nombre de solutions

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

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

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

# Résumé et Objectif

- Les solutions (dans $\overline{K}$) d'un système polynomial ne dépendent que de l'**idéal** associé.
- **Objectif :** Trouver une bonne représentation de cet idéal pour déterminer l'ensemble des solutions (et bien plus). C'est exactement le rôle des **bases de Gröbner**. Elles vont dépendre d'un **ordre** sur les monômes.
- **Effectivité :** Il faut aussi des **algorithmes** pour déterminer ces représentations. Plus de détails demain.

# Bases de Gröbner

# Ordre Monomial

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

## Ordre Monomial

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

- $<$ est un **ordre total** (on peut comparer tous les éléments)
- Pour tout triplets de monomes $\mu_1, \mu_2, \mu_3$ alors

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

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

# Exemple : Ordre Lexicographique

## Ordre Lexicographique $x_1 > \cdots > x_n$

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

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

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

Dans $K[x_1, x_2, x_3]$, on a
$x_1^2 x_2 x_3^{15} <_{lex} x_1^2 x_2^2$ car $(2, 1, 15) - (2, 2, 0) = (0, -1, 15)$.
$1 < x_3 < x_3^2 < \cdots < x_2 < x_2 x_3 < x_2 x_3^2 < \cdots < x_2^2 < x_2^2 x_3 < \cdots < x_2^3 < \cdots < x_1 < \cdots$

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

# Base de Gröbner pour l'ordre LEX

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

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

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

# Exemple : Base de Gröbner en Sage

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

# *Graded Reverse Degree Lexicographic* (GREVLEX ou DRL)

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

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

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

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

$x_1^2 x_2 x_3^{15} >_{drl} x_1^2 x_2^2$ car $2 + 1 + 15 = 18 > 4 = 2 + 2$

$1 < \underbrace{x_3 < x_2 < x_1}_{\text{Degré 1}} < \underbrace{x_3^2 < x_3 x_2 < x_2^2 < x_1 x_3 < x_1 x_2 < x_1^2}_{\text{Degré 2}} < x_3^3 < x_2 x_3^2 < x_2^2 x_3 < x_2^3 < \cdots$

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

# Monôme de tête

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

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

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

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

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

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

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

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

# Exemple

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

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

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

# Idéal monomial

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

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

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

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

**Remarquons que** :

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

**donc**

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

# Un critère utile

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

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

**Preuve :** Exercice.

# Base de Gröbner

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

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

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

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

**On verra que** :

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

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

# Base de Gröbner : Existence et Unicité*

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

## Existence (Algorithme de Buchberger)

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

## Base de Gröbner réduite et Unicité

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

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

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

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