Calcul Formel et Symbolique

Équations algébriques et différentielles, Algèbre linéaire exacte, Cryptanalyse

Jean-Guillaume Dumas, Françoise Jung, Clément Pernet

Université Grenoble Alpes, Laboratoire Jean Kuntzmann, UMR CNRS

Grenoble, 28 novembre 2019

Sommaire

Plan

Équations algébriques et différentielles

Algèbre linéaire exacte
- Multiplication de matrices
- Élimination de Gauss

Cryptanalyse : affiner les paramètres de cryptosystèmes
- Échange de clef secrète dans un groupe (Diffie-Hellman)
- Logarithme discret modulaire par calcul d'index dans une courbe elliptique
- Bases de Gröbner, algorithme de Buchberger et algèbre linéaire
- Challenge de calcul HPAC

Plan

Équations algébriques et différentielles

Algèbre linéaire exacte
- Multiplication de matrices
- Élimination de Gauss

Cryptanalyse : affiner les paramètres de cryptosystèmes
- Échange de clef secrète dans un groupe (Diffie-Hellman)
- Logarithme discret modulaire par calcul d'index dans une courbe elliptique
- Bases de Gröbner, algorithme de Buchberger et algèbre linéaire
- Challenge de calcul HPAC

Algèbre linéaire exacte

Domaine de calcul : $\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}, \mathbb{F}_{p^k}, \mathbb{F}_{p^k}[X]$, etc

Similarité avec l'algèbre linéaire numérique :

- brique de base centrale,
- forte intensité calcul/mémoire,
- algorithmique (relativement) simple et régulière.

Spécificités :

- Déficience de rang,
- Absence de problème de stabilité,
- diversité des arithmétiques (corps finis, multiprécision, etc).

Illustration ici sur

- deux problèmes clés : le produit de matrices et l'élimination de Gauss
- illustrés par les contributions Grenobloises

Algorithmes rapides de produits matriciels

Algorithme de Strassen

$$\begin{array}{ll} \rho_1 \leftarrow (a_{11}+a_{22})(b_{11}+b_{22}), & \rho_4 \leftarrow (a_{11}+a_{12})b_{22}, \\ \rho_2 \leftarrow (a_{12}-a_{22})(b_{21}+b_{22}), & \rho_5 \leftarrow a_{11}(b_{12}-b_{22}), \\ \rho_3 \leftarrow (a_{21}-a_{11})(b_{11}+b_{12}), & \rho_6 \leftarrow a_{22}(b_{21}-b_{11}), \\ & \rho_7 \leftarrow (a_{21}+a_{22})b_{11}, \end{array}$$

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} \rho_1+\rho_2-\rho_4+\rho_6 & \rho_6+\rho_7, \\ \rho_4+\rho_5 & \rho_1+\rho_3+\rho_5-\rho_7 \end{pmatrix}.$$

V. Strassen 1969 : 2×2 en $\mathbf{18}+$ et $\mathbf{7}\times$ ⇨$n \times n$ en $\mathbf{7n^{2.8074}} + \mathbf{o(n^{2.8076})}$

S. Winograd circa 1970 : 2×2 en $\mathbf{15}+$ et $\mathbf{7}\times$ ⇨$n \times n$ en $\mathbf{6n^{2.8074}} + \mathbf{o(n^{2.8074})}$

N. Gastinel 1971 : Interpréte Strassen comme produits de Hadamard.
⇨introduit une paramétrisation

P. Chatelin 1985 : Transformations invariantes d'algorithmes
⇨Dérive Winograd de Strassen

Algorithmes rapides de produits matriciels

Dumas Gautier Pernet 2002 : Mise en oeuvre pour les corps finis : BLAS + Strassen

Boyer Dumas Pernet Zhu 2009 : Empreinte mémoire de Strassen-Winograd

Dumas Pernet Sedoglavitch (en cours) : $A \times A^T$ en 7.5 + et 5 $\times$

⇨généralise les paramétrisations de Chatelin

Autres algorithmes sous-cubiques praticables :

Kaporin'04 : Mise en pratique de [Pan'72]

Boyer Dumas 16 : Adaptation exacte de [Bini & al.' 79] aux corps finis

BLIS'16, Balard'14 : Strassen pour les BLAS numériques

Schwartz & al. 17,19 : Transformations invariantes en pratique

Mise en oeuvre

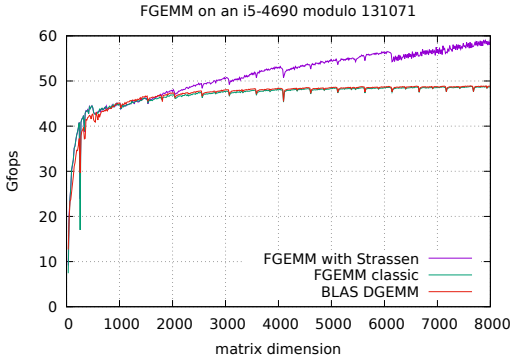
Bibliothèques d'algèbre linéaire exacte : `LinBox`, `fflas-ffpack`

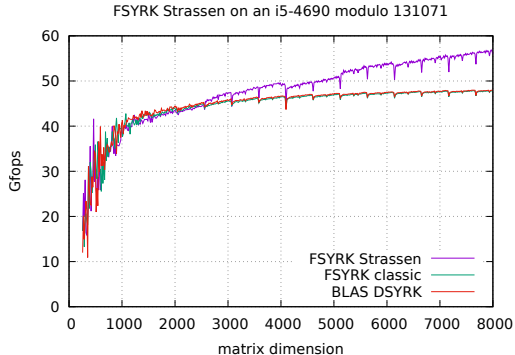
- Open source, paquets : `Debian, arch, fedora`
- Noyaux dans `SageMath, Macaulay2`
- Approche adoptée par `Maple, Mathematica, magma`

Mise en oeuvre

Bibliothèques d'algèbre linéaire exacte : `LinBox`, `fflas-ffpack`

- Open source, paquets : `Debian, arch, fedora`
- Noyaux dans `SageMath, Macaulay2`
- Approche adoptée par `Maple, Mathematica, magma`



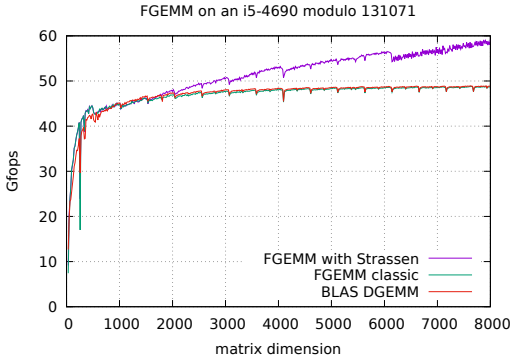


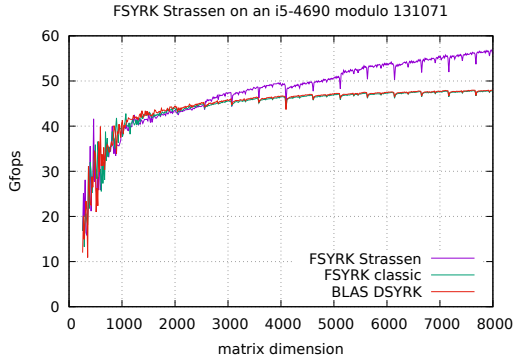
Mise en oeuvre

Bibliothèques d'algèbre linéaire exacte : `LinBox`, `fflas-ffpack`

- Open source, paquets : `Debian, arch, fedora`
- Noyaux dans `SageMath, Macaulay2`
- Approche adoptée par `Maple, Mathematica, magma`

	$A \times B$	$A \times A^T$
$n = 2000$	0.37s	0.19s
$n = 8000$	s 17.3	9.15s





Élimination de Gauss

Algorithmique et implantations haute performance

Villard 88 : Parallélisation sur un hypercube 16 proc.

Dumas Giorgi Pernet 08 : Mise en pratique des réductions au produit de matrice

Dumas Pernet Sultan 16 : Parallélisation multi-coeur

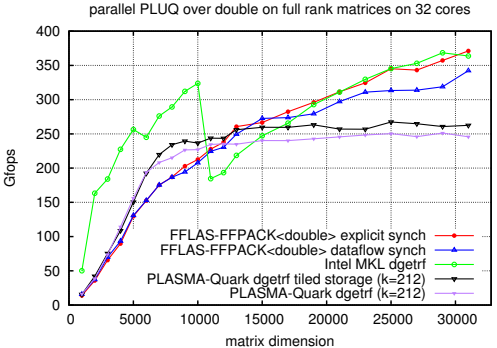
Élimination de Gauss

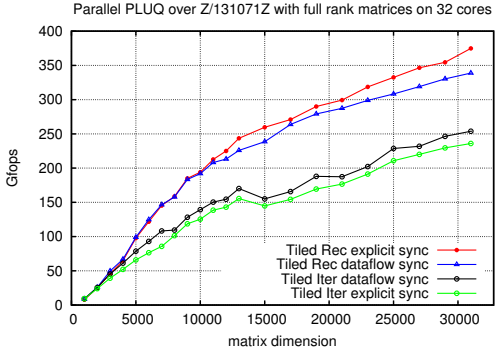
Algorithmique et implantations haute performance

Villard 88 : Parallélisation sur un hypercube 16 proc.

Dumas Giorgi Pernet 08 : Mise en pratique des réductions au produit de matrice

Dumas Pernet Sultan 16 : Parallélisation multi-coeur





Pivotage et profils de rang

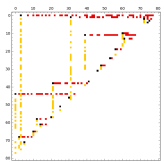
Spécificité du calcul exact :

- Déficience de rang
- Le rang ou le profil de rang sont l'objet du calcul

Dumas Pernet Sultan 15 : *Computing the rank profile matrix*

- Nouvel invariant, résumant toute l'information des profils de rang
- caractérisation des conditions sur le pivotage pour la calculer
- $O(n^\omega)$ par un nouvel algorithme récursif par tuiles.
- Connexion avec la forme généralisée de Bruhat [Della-Dora 73]

Pernet 16 : application à l'algorithmique des matrices quasi-séparables



Plan

Équations algébriques et différentielles

Algèbre linéaire exacte
- Multiplication de matrices
- Élimination de Gauss

Cryptanalyse : affiner les paramètres de cryptosystèmes
- Échange de clef secrète dans un groupe (Diffie-Hellman)
- Logarithme discret modulaire par calcul d'index dans une courbe elliptique
- Bases de Gröbner, algorithme de Buchberger et algèbre linéaire
- Challenge de calcul HPAC

Diffie-Hellman (1976)

● est public

secret ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

secret ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

● & ●

secret ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

● & ●

secret ●

● & ● & ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

● & ●

secret ●

● & ● & ●

● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

● & ●

secret ●

● & ● & ●

● secret

- $g = $ ●
- $a = $ ●
- $b = $ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

g^b

secret ● ● & ● & ● ● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

g^b

secret ● clef : g^{ab} ● secret

- $g = $ ●
- $a = $ ●
- $b = $ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

g^b

secret ● clef : g^{ab} ● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Groupe add. : $[b][a]G = [ab]G = [a][b]G$

Groupe des points d'une courbe elliptique

$$\mathbb{E}(\mathbb{F}_q) = (\{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \oplus)$$

$$[a]P = \underbrace{P \oplus \ldots \oplus P}_{a \text{ fois}}$$

Groupe des points d'une courbe elliptique

$$\mathbb{E}(\mathbb{F}_q) = (\{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \oplus)$$

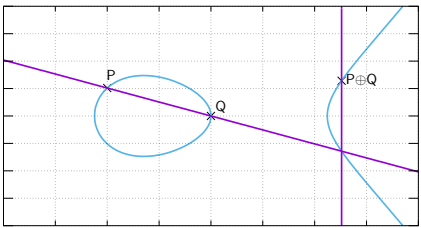
$$[a]P = \underbrace{P \oplus \ldots \oplus P}_{a \text{ fois}}$$

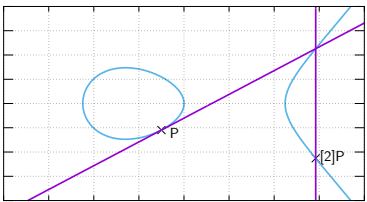
⚠ Le logarithme discret ($a = \log_P(Q)$ pour $Q = [a]P$, connaissant P et Q) doit être difficile pour protéger les clefs

Groupe des points d'une courbe elliptique

$$\mathbb{E}(\mathbb{F}_q) = (\{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \oplus)$$
$$[a]P = \underbrace{P \oplus \ldots \oplus P}_{a \text{ fois}}$$

Loi de groupe :





⚠ Le logarithme discret ($a = \log_P(Q)$ pour $Q = [a]P$, connaissant P et Q) doit être difficile pour protéger les clefs

Calcul d'index sur courbes elliptiques

- *[Gaudry 2005]*
- *[Faugère, Gaudry, Huot, Renault 2013]*
- *[Faugère, Huot, Joux, Renault, Vitse 2014]*

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^{\ell}}\}$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^\ell}\}$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^{\ell}}\}$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^{\ell}}\}$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : sous-ensemble structuré $\#\mathcal{F} \approx 2^{\ell}/4$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : sous-ensemble structuré $\#\mathcal{F} \approx 2^{\ell}/4$

2: Crible : bases de Gröbner Proba. $1/(2^{n-1}n!)$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : sous-ensemble structuré $\#\mathcal{F} \approx 2^{\ell}/4$

2: Crible : bases de Gröbner Proba. $1/(2^{n-1}n!)$

3: LinAlg. : creuse $2^{\ell-2} \times 2^{\ell-2}$, sur $\mathbb{F}_{2^{n\ell}}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

$$\text{PoSSo} : \begin{cases} x_i \in \mathbb{F}_{2^\ell} \\ (x_i, y_i) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) : y_i^2 = x_i^3 + ax_i + b \\ (M_x, M_y) - (x_1, y_1) \oplus (x_2, y_2) \oplus \ldots \oplus (x_k, y_k) = 0 \end{cases}$$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

$$\text{PoSSo} : \begin{cases} x_i \in \mathbb{F}_{2^\ell} \\ (x_i, y_i) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) : y_i^2 = x_i^3 + ax_i + b \\ (M_x, M_y) - (x_1, y_1) \oplus (x_2, y_2) \oplus \ldots \oplus (x_k, y_k) = 0 \end{cases}$$

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right) \in \mathbb{F}_{2^{n\ell}}^2$$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

$$\text{PoSSo} : \begin{cases} x_i \in \mathbb{F}_{2^\ell} \\ (x_i, y_i) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) : y_i^2 = x_i^3 + ax_i + b \\ (M_x, M_y) - (x_1, y_1) \oplus (x_2, y_2) \oplus \ldots \oplus (x_k, y_k) = 0 \end{cases}$$

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right) \in \mathbb{F}_{2^{n\ell}}^2$$

$$x_i, y_i \in \mathbb{F}_{2^{n\ell}} \cong \left(\mathbb{F}[z] \mod z^{n\ell} + \ldots + p_2 z^2 + p_1 z + 1 \mod 2 \right)$$

Bases de Gröbner et systèmes polynomiaux

- base de Gröbner d'un idéal polynomial $\mathcal{I}$  *[Buchberger 1976]*
  - $\prec$ ordre monomial
  - Base de Gröbner G :

$$\forall p \in \mathcal{I}, \exists g \in G, \mathrm{LeadMonom}(g, \prec) \mid \mathrm{LeadMonom}(p, \prec)$$

Bases de Gröbner et systèmes polynomiaux

- base de Gröbner d'un idéal polynomial $\mathcal{I}$  *[Buchberger 1976]*
  - $\prec$ ordre monomial
  - Base de Gröbner G :

$$\forall p \in \mathcal{I}, \exists g \in G, \mathrm{LeadMonom}(g, \prec) \mid \mathrm{LeadMonom}(p, \prec)$$

- Résolution de Systèmes Polynomiaux sur un corps fini
  - PoSSo_q :

$$\begin{cases} p_1(z_1, \ldots, z_m) = 0 \\ \vdots \\ p_n(z_1, \ldots, z_m) = 0 \end{cases}$$

  - NP-dur

Exemple de résolution avec base de Gröbner

$$\begin{cases} 0 = & 2TX - 2YZ + 3Z^2 \\ 0 = & -2TY + 2XZ \\ 0 = & 2TZ - 2XY - 2X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases}$$

Exemple de résolution avec base de Gröbner

$$\begin{cases} 0 = & 2TX - 2YZ + 3Z^2 \\ 0 = & -2TY + 2XZ \\ 0 = & 2TZ - 2XY - 2X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases} \iff \begin{cases} 0 = & 1152X^7 - 1763X^5 + 655X^3 - 44X \\ 0 = & -1152X^6 + 118TX^3 + 1605X^4 - 118TX - 453X^2 \\ 0 = & -1152X^5 + 3835TX^2 - 1404X^3 + 3835XZ + 2556X \\ 0 = & -335232X^6 + 477321X^4 - 11505TX - 134419X^2 + 7670Y - 1150 \\ 0 = & -6912X^5 + 3835T^2X + 10751X^3 - 3839X \\ 0 = & -19584X^5 + 25987X^3 + 3835TZ - 6403X \\ 0 = & -9216X^5 + 3835T^3 + 3835TX^2 + 11778X^3 - 3835T - 2562X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases}$$

Exemple de résolution avec base de Gröbner

$$\begin{cases} 0 = & 2TX - 2YZ + 3Z^2 \\ 0 = & -2TY + 2XZ \\ 0 = & 2TZ - 2XY - 2X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases} \iff \begin{cases} 0 = & 1152X^7 - 1763X^5 + 655X^3 - 44X \\ 0 = & -1152X^6 + 118TX^3 + 1605X^4 - 118TX - 453X^2 \\ 0 = & -1152X^5 + 3835TX^2 - 1404X^3 + 3835XZ + 2556X \\ 0 = & -335232X^6 + 477321X^4 - 11505TX - 134419X^2 + 7670Y - 1150 \\ 0 = & -6912X^5 + 3835T^2X + 10751X^3 - 3839X \\ 0 = & -19584X^5 + 25987X^3 + 3835TZ - 6403X \\ 0 = & -9216X^5 + 3835T^3 + 3835TX^2 + 11778X^3 - 3835T - 2562X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases}$$

- Buchberger 1976 : $\mathcal{O}\left(d^{2^{n+o(1)}}\right)$
- Aujourd'hui : algorithmes F4, F5, systèmes creux, invariants, FGLM, ...

⇨ plusieurs centaines de polynômes, chacun avec plusieurs centaines de termes et coefficients de plusieurs centaines de chiffres.

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

1. Crible :
   - 536 870 912 relations creuses
   - Une semaine sur plus de 1000 ordinateurs personnels de Paris 6

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

1. Crible :
   - 536 870 912 relations creuses
   - Une semaine sur plus de 1000 ordinateurs personnels de Paris 6
2. Algèbre linéaire :
   - Filtrage : 7 196 707 équations et inconnues, 11Go de coefficients
   - Solution : Un serveur 32 cœurs à Grenoble
     - 2.1 Séquence (itérations) : 57 jours
     - 2.2 Polynôme minimal : 54 heures avec 561 Go de RAM/Swap
     - 2.3 Évaluation : 19 jours

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

1. Crible :
   - 536 870 912 relations creuses
   - Une semaine sur plus de 1000 ordinateurs personnels de Paris 6
2. Algèbre linéaire :
   - Filtrage : 7 196 707 équations et inconnues, 11Go de coefficients
   - Solution : Un serveur 32 cœurs à Grenoble
     - 2.1 Séquence (itérations) : 57 jours
     - 2.2 Polynôme minimal : 54 heures avec 561 Go de RAM/Swap
     - 2.3 Évaluation : 19 jours

⇨Courbe IPSEc, $\approx 2^{151}$ points dans $\mathbb{F}_{2^{155}}^2 = \mathbb{F}_{2^{5\times 31}}^2$: Crible $\times$ 300, LinAlg $\times$ 22 ...