Algorithmes pour les polynômes tordus sur les corps finis

Xavier Caruso, Jérémy Le Borgne

30 mai 2013

L'anneau des polynômes tordus

Notations

k	un corps fini
σ	un automorphisme de k (*i.e.* une puissance du Frobenius)
k^σ	les points fixes de σ
r	l'ordre de σ (= le degré de k sur k^σ)

L'anneau des polynômes tordus (ou polynômes de Öre)

C'est l'ensemble $k[X]$ muni de :

- l'addition usuelle
- la multiplication découlant de la règle $X \cdot a = \sigma(a) \cdot X$

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{n} a_j X^j\right) = \sum_{i,j} a_i \sigma^i(a_j) X^{i+j}$$

On le note $k[X, \sigma]$.

Arithmétique élémentaire

Multiplication des polynômes tordus

Soit à calculer PQ (avec $P, Q \in k[X, \sigma]$). On note :

- d le maximum de $\deg(P)$ et $\deg(Q)$
- r l'ordre de σ

Algorithme SchoolBook

Complexité : $\tilde{O}(d^2 r + d r^2)$ opérations dans k^σ

Algorithme de Karatsuba

Si n est un multiple de r, on a :

$$\begin{aligned}&(A + X^n B) \cdot (C + X^n D)\\ = AC + X^n &\left[(A + B)(C + D) - AC - BD\right] + X^{2n} BD\end{aligned}$$

D'où un algorithme à la Karatsuba.

Complexité : $\tilde{O}(d^{1,58} r^{1,42})$ opérations dans k^σ (si $d > r$).

Multiplication des polynômes tordus

Soit à calculer PQ (avec $P, Q \in k[X, \sigma]$). On note :

- d le maximum de $\deg(P)$ et $\deg(Q)$
- r l'ordre de σ

Réduction au cas commutatif

On écrit

$$P = P_0 + P_1 \cdot X + P_2 \cdot X^2 + \cdots + P_{r-1} \cdot X^r$$

avec $P_i \in k[X^r]$. Alors

$$PQ = P_0 Q + P_1 Q^{\sigma} \cdot X + P_2 Q^{\sigma^2} \cdot X^2 + \cdots + P_{r-1} Q^{\sigma^{r-1}} \cdot X^r$$

et les produits $P_i Q^{\sigma^i}$ sont les mêmes qu'on les calcule dans $k[X, \sigma]$ ou dans $k[X]$.

Complexité : $\tilde{O}(dr^2)$ opérations dans k^{σ}

Division des polynômes tordus

Proposition (Division eucldienne à droite)

Étant données $A, B \in k[X, \sigma]$ avec $B \neq 0$, il existe Q et R uniquement déterminés tels que $A = Q \cdot B + R$ et $\deg R < \deg B$.

Algorithme de calcul : réduction au cas de la multiplication

$$\begin{array}{rccc} \tau_n : & k[X,\sigma]_{\leq n} & \longrightarrow & k[X,\sigma^{-1}]_{\leq n} \\ & \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} a_{n-i} X^i \end{array}$$

On pose $n = \deg A$, $m = \deg B$. De $A = QB + R$, on déduit :

$$\tau_n(A) \equiv \tau_{n-m}(Q) \cdot \tau_m(B^{\sigma^{m-n}}) \pmod{X^{n-m+1}}$$

On inverse $\tau_m(B^{\sigma^{m-n}})$ modulo X^{n-m+1} (méthode de Newton).
On en déduit $\tau_{n-m}(Q)$ puis Q, puis R.

Complexité : $\tilde{O}(\mathrm{SM}(d, r))$ opérations dans k^σ

Idéaux (à gauche) de $k[X, \sigma]$

Proposition

Tout idéal à gauche de $k[X, \sigma]$ est de la forme $k[X, \sigma] \cdot P$ pour un certain $P \in k[X, \sigma]$ uniquement determiné modulo multiplication à gauche par une constante.

En particulier :

$$k[X, \sigma] \cdot A + k[X, \sigma] \cdot B = k[X, \sigma] \cdot \mathrm{rgcd}(A, B)$$
$$k[X, \sigma] \cdot A \cap k[X, \sigma] \cdot B = k[X, \sigma] \cdot \mathrm{llcm}(A, B)$$

Algorithmes de calcul

- Algorithme d'Euclide étendu
  Complexité : $\tilde{O}(d^2 r^2)$ opérations dans k^σ
- Adaptation de l'algorithme de Lehmer-Knuth
  Complexité : $\tilde{O}(\mathrm{SM}(d, r))$ opérations dans k^σ

Factorisation des polynômes tordus

Le cas des polynômes séparables

Comparaison avec des algèbres de matrices

Rappel des notations

k^σ les points fixes de σ
r l'ordre de σ (= le degré de k sur k^σ)

Le centre de $k[X, \sigma]$

C'est $k^\sigma[X^r]$. On le note $\mathcal{C}$.

Comparaison avec une algèbre de matrices

On pose $\mathcal{R} = k[X, \sigma]$.
Soit $N \in \mathcal{C}$ irréductible comme élément de $\mathcal{C}$ avec $N \neq X^r$. Alors

$$\mathcal{R}/N\mathcal{R} \simeq M_r(\mathcal{C}/N\mathcal{C}).$$

Démonstration : $\mathcal{R}/N\mathcal{R}$ est une algèbre simple centrale sur le corps fini $\mathcal{C}/N\mathcal{C}$, donc une algèbre de matrices.

Conséquence 1 : Une équivalence de catégories

(R)appel sur l'equivalence de Morita

Soit A un anneau commutatif. Soit $n > 0$ un entier.
On a une équivalence de catégories entre :

- la catégorie des modules à gauche sur $M_n(A)$
- la catégorie des modules sur A

Corollaire

On a une équivalence de catégories entre :

- la catégorie des modules à gauche sur $k[X, \sigma][\frac{1}{X}]$ qui sont de dimension finie comme k-espace vectoriel
- la catégorie des modules sur $k^\sigma[X^r][\frac{1}{X^r}]$ qui sont de dimension finie comme k^σ-espace vectoriel
- la catégorie des k^σ-espaces vectoriels de dimension finie munis d'un automorphisme

Conséquence 2 : La norme réduite

On note encore N un polynôme irréductible de $\mathcal{C}$ avec $N \neq X^r$.

De l'isomorphisme $\mathcal{R}/N\mathcal{R} \simeq M_r(\mathcal{C}/N\mathcal{C})$, on déduit une application « déterminant modulo N »

$$\det_N : \mathcal{R}/N\mathcal{R} \to \mathcal{C}/N\mathcal{C}.$$

Théorème
(conséquence de la théorie des algèbres d'Azumaya)

Il existe une application multiplicative

$$\mathcal{N} : \mathcal{R} = k[X, \sigma] \to \mathcal{C}$$

qui relève les applications $\det_N$ ci-dessus.

On l'appelle la norme réduite sur $k[X, \sigma]$.

Calcul de la norme réduite

Première méthode

On montre que $\mathcal{N}(P)$ est égale au déterminant de la multiplication à droite par P sur l'espace $k[X,\sigma]$ vu comme module (libre) sur $k[X^r]$.

$\Rightarrow$ algorithme de calcul de $\mathcal{N}(P)$

Complexité : $\tilde{O}(d\,\mathrm{MM}(r))$ opérations dans k^σ

Deuxième méthode

On montre $\mathcal{N}(P)$ est égale au polynôme caractéristique (vu comme polynôme en la variable X^r) de la multiplication par X sur le k-espace vectoriel $k[X,\sigma]/k[X,\sigma]\cdot P$

$\Rightarrow$ algorithme de calcul de $\mathcal{N}(P)$

Complexité : $\tilde{O}(dr^2 + r\,\mathrm{MM}(d))$ opérations dans k^σ

Quelques propriétés de la norme réduite

- Si P est central, alors $\mathcal{N}(P) = P^r$

Propriétés de multiplicativité et de divisibilité

- $\mathcal{N}(PQ) = \mathcal{N}(P) \cdot \mathcal{N}(Q)$
- P divise $\mathcal{N}(P)$

Propriétés liées à la factorisation

- P irréductible dans $k[X, \sigma] \Leftrightarrow \mathcal{N}(P)$ irréductible dans $\mathcal{C}$
- Si $P = P_1 \cdots P_n$ avec P_i irréductible,
  alors $\mathcal{N}(P) = \mathcal{N}(P_1) \cdots \mathcal{N}(P_n)$ est la décomposition de $\mathcal{N}(P)$ en produits d'irréductibles
- Si N est un facteur irréductible de $\mathcal{N}(P)$,
  alors il existe $Q \in k[X, \sigma]$ divisant P à droite tel que $\mathcal{N}(Q) = N$

Application à la factorisation

Soit $P \in k[X, \sigma]$. On suppose que $\mathcal{N}(P)$ est séparable :

$$\mathcal{N}(P) = N_1 \cdots N_n$$

où les $N_i \in \mathcal{C}$ sont irréductibles et deux à deux distincts.

Théorème

Pour tout $i \in \{1, \ldots, n\}$, le polynôme $P_i = \mathrm{rgcd}(P, N_i)$ est l'unique facteur irréductible à droite de P tel que $\mathcal{N}(P_i) = N_i$.

Conséquences

- On obtient une factorisation de P en calculant successivement des PGCD par chacun des N_i
  Complexité : $\tilde{O}(dr^3)$ connaissant la factorisation de $\mathcal{N}(P)$
- Sous les mêmes hypothèses, P admet $n!$ factorisations

Factorisation des polynômes tordus

Le cas général

Une première réduction

Soit $P \in k[X, \sigma]$. On écrit :

$$\mathcal{N}(P) = N_1^{\mu_1} \cdots N_n^{\mu_n}$$

avec $\mu_i > 0$ et $N_i \in \mathcal{C}$ irréductible.

Comme précemment, on pose $P_i = \mathrm{rgcd}(P, N_i)$.

Point positif : P_i n'est jamais un polynôme constant.

Point négatif : P_i n'est pas nécessairement irréductible

On est ainsi ramené au problème suivant :

Factoriser $P \in k[X, \sigma]$ sachant qu'il existe N irréductible dans $\mathcal{C}$ tel que P divise N.

On a alors $\mathcal{N}(P) = N^e$ avec $e \in \{1, \ldots, r\}$.

Diviseurs et sous-espaces vectoriels

Notations

- N un polynôme irréductible de $\mathcal{C}$ avec $N \neq X^r$
- P un élément de $k[X, \sigma]$ divisant N
- e l'entier tel que $\mathcal{N}(P) = N^e$

Équivalence de Morita

Il y a une équivalence de catégorie entre :

- la catégorie des espaces vectoriel sur $\mathcal{C}/N\mathcal{C}$
- la catégorie des modules à gauche sur $k[X, \sigma]/k[X, \sigma]N$

Corollaire

Il y a une bijection croissante entre :

- les sous-espaces vectoriels de $(\mathcal{C}/N\mathcal{C})^e$
- les sous-$k[X, \sigma]$-modules à gauche de $k[X, \sigma]/k[X, \sigma]P$
- les diviseurs à droite de P

Anneau des endomorphismes

On pose $D_P = k[X, \sigma]/k[X, \sigma]P$.

Un isomorphisme abstrait

De l'équivalence de Morita, il résulte :

$$\mathrm{End}(D_P) \simeq M_e(\mathcal{C}/N\mathcal{C})$$

Construction explicite d'endomorphismes

Soit Q tel que $PQ = N$.

L'application

$$\begin{array}{rcl} D_P & \to & \mathrm{End}(D_P) \\ R & \mapsto & m_{QR} : x \mapsto xQR \end{array}$$

est bien définie et surjective.

Construction de diviseurs

Un diagramme récapitulatif

$$D_P \twoheadrightarrow \mathrm{End}(D_P) \xrightarrow{\sim} M_e(\mathcal{C}/N\mathcal{C})$$

$$\left\{ \begin{array}{c} \text{diviseurs} \\ \text{de } P \end{array} \right\} \simeq \left\{ \begin{array}{c} \text{sous-mod.} \\ \text{de } D_P \end{array} \right\} \simeq \left\{ \begin{array}{c} \text{sous-e.v.} \\ \text{de } (\mathcal{C}/N\mathcal{C})^e \end{array} \right\}$$

Proposition

Soient $R \in D_P$ et f_R la matrice de $M_e(\mathcal{C}/N\mathcal{C})$ qui lui correspond.

Alors : $\mathrm{rgcd}(R, P)$ est un diviseur non trivial de P

$\Leftrightarrow f_R \neq 0$ et f_R n'est pas bijectif.

Démonstration : $\mathrm{rgcd}(R, P)$ est le diviseur de P correspondant au sous-espace vectoriel de $(\mathcal{C}/N\mathcal{C})^e$ qui est l'image de f_R.

Un algorithme pour calculer un diviseur

Un diagramme récapitulatif

$$D_P \twoheadrightarrow \mathrm{End}(D_P) \xrightarrow{\sim} M_e(\mathcal{C}/N\mathcal{C})$$

$$\left\{ \begin{array}{c} \text{diviseurs} \\ \text{de } P \end{array} \right\} \simeq \left\{ \begin{array}{c} \text{sous-mod.} \\ \text{de } D_P \end{array} \right\} \simeq \left\{ \begin{array}{c} \text{sous-e.v.} \\ \text{de } (\mathcal{C}/N\mathcal{C})^e \end{array} \right\}$$

Algorithme

1. Tirer un élément aléatoire $R \in D_P$
2. Renvoyer $\mathrm{rgcd}(P, (QR)^{\#(\mathcal{C}/N\mathcal{C})-1} - 1)$

Probabilité de succès

C'est la probabilité qu'une matrice aléatoire dans $M_e(\mathcal{C}/N\mathcal{C})$ ait une valeur propre non nulle dans $\mathcal{C}/N\mathcal{C}$. Elle vaut environ 0,3.

Complexité

$$\tilde{O}(dr^3 \log q + d \log^2 q + d^{1+\varepsilon}(\log q)^{1+O(1)}) + F(d,q)$$

opérations binaires, où :

- q est le cardinal de k^σ
- $F(d,q)$ est la complexité de la factorisation d'un polynôme *commutatif* sur le corps de cardinal q

$$F(d,q) = (d^{3/2+o(1)} + d^{1+o(1)} \log q) \cdot (\log q)^{1+o(1)}$$

Remarque

Lorsque $r^3 \ll d$, le terme dominant est $F(d,q)$

Comparaison avec l'algorithme de Giesbrecht

$$\tilde{O}(d^4 r^2 \log q + d^3 r^3 \log q + d \cdot \mathrm{MM}(dr) \log q + d^2 r \log^2 q)$$

Nous sommes meilleurs. 

Implémentation

- Un packetage MAGMA (par Jérémy Le Borgne)
- Un packetage SAGE (par Xavier Caruso)
  qui inclut d'autres fonctionnalités :
  - compter le nombre de factorisations
  - lister toutes les factorisations
  - renvoyer une factorisation aléatoire (équirépartie)

Quelques liens

- Codes source :
  `http://cethop.math.cnrs.fr/prodscient/algos.html`
- Tutorial :
  `https://cethop.math.cnrs.fr:8443/home/pub/2/`
  `https://cethop.math.cnrs.fr:8443/home/pub/1/`
- Utilisation en ligne :
  `https://cethop.math.cnrs.fr:8443/`