Sur la complexité du calcul modulo un ensemble triangulaire zéro-dimensionnel.

Adrien Poteaux[⋆] [†] , Éric Schost[†]

[⋆]: UPMC / INRIA Rocquencourt, équipe SALSA

[†]: Computer Science Department, The University of Western Ontario, London, ON, Canada

Séminaire BIPOP - CASYS

Institut de Mathématiques-Informatique de Grenoble

Jeudi 17 Février 2011

Sur la complexité du calcul modulo un ensemble triangulaire zéro-dimensionnel.

- A. Poteaux & É. Schost, *Modular composition modulo triangular sets and applications* (soumis à publication).

- A. Poteaux & É. Schost, *On the complexity of computing with zero-dimensional triangular sets* (en cours de rédaction).

Ensemble triangulaire

- $\mathbb{K}$ un corps.
- $\mathbf{Y} = Y_1, \ldots, Y_s$ variables sur $\mathbb{K}$, ordre $Y_1 < \cdots < Y_s$.
- Ensemble triangulaire (unitaire, sans facteur carré, en dimension 0) :

$$\mathbf{T} \left| \begin{array}{l} T_s(Y_1, \ldots, Y_s) \\ \vdots \\ T_1(Y_1) \end{array} \right.$$

  - $T_i \in \mathbb{K}[Y_1, \cdots, Y_i]$ unitaire en Y_i
  - T_i réduit modulo $\langle T_1, \ldots, T_{i-1} \rangle$.

- Notations :
  - $d_i = \deg_{Y_i}(T_i) \geq 2$; $\mathbf{d} = (d_1, \ldots, d_s)$ *multidegré* de $\mathbf{T}$.
  - $\delta_{\mathbf{T}} = d_1 \cdots d_s$
  - $R_{\mathbf{T}} = \mathbb{K}[\mathbf{Y}]/\langle \mathbf{T} \rangle \simeq \mathbb{K}[\mathbf{Y}]_{\mathbf{d}}$

Un exemple

C. Pascal & É. Schost 2006, *Change of order for bivariate triangular sets*

- But : un facteur de $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.

Un exemple

C. Pascal & É. Schost 2006, *Change of order for bivariate triangular sets*

- But : un facteur de $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Racines de T_1 invariantes par $\alpha \mapsto \frac{1}{\alpha}$

$$\mathbf{T} \left| \begin{array}{l} T_2 = Y_2 - (Y_1 + \frac{1}{Y_1}) \bmod T_1 = Y_2 - (Y_1^5 - 5Y_1^4 + 6Y_1^3 - 9Y_1^2 + 5Y_1 - 5) \\ T_1(Y_1) = Y_1^6 - 5Y_1^5 + 6Y_1^4 - 9Y_1^3 + 6Y_1^2 - 5Y_1 + 1 \end{array} \right.$$

Un exemple

C. Pascal & É. Schost 2006, *Change of order for bivariate triangular sets*

- But : un facteur de $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Racines de T_1 invariantes par $\alpha \mapsto \frac{1}{\alpha}$

$$\mathbf{T} \left| \begin{array}{l} T_2 = Y_2 - (Y_1 + \frac{1}{Y_1}) \bmod T_1 = Y_2 - (Y_1^5 - 5Y_1^4 + 6Y_1^3 - 9Y_1^2 + 5Y_1 - 5) \\ T_1(Y_1) = Y_1^6 - 5Y_1^5 + 6Y_1^4 - 9Y_1^3 + 6Y_1^2 - 5Y_1 + 1 \end{array} \right.$$

- Changement d'ordre $Y_2 < Y_1$

$$\left| \begin{array}{l} Y_1^2 - Y_2 Y_1 + 1 \\ Y_2^3 - 5Y_2^2 + 3Y_2 + 1 \end{array} \right.$$

Un exemple

C. Pascal & É. Schost 2006, *Change of order for bivariate triangular sets*

- But : un facteur de $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Racines de T_1 invariantes par $\alpha \mapsto \frac{1}{\alpha}$

$$\mathbf{T} \left| \begin{array}{l} T_2 = Y_2 - (Y_1 + \frac{1}{Y_1}) \bmod T_1 = Y_2 - (Y_1^5 - 5Y_1^4 + 6Y_1^3 - 9Y_1^2 + 5Y_1 - 5) \\ T_1(Y_1) = Y_1^6 - 5Y_1^5 + 6Y_1^4 - 9Y_1^3 + 6Y_1^2 - 5Y_1 + 1 \end{array} \right.$$

- Changement d'ordre $Y_2 < Y_1$

$$\left| \begin{array}{l} Y_1^2 - Y_2 Y_1 + 1 \\ Y_2^3 - 5Y_2^2 + 3Y_2 + 1 \end{array} \right.$$

- $Y_2^3 - 5Y_2^2 + 3Y_2 + 1 = (Y_2^2 - 4Y_2 - 1)(Y_2 - 1)$

Un exemple

C. Pascal & É. Schost 2006, *Change of order for bivariate triangular sets*

- But : un facteur de $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Racines de T_1 invariantes par $\alpha \mapsto \frac{1}{\alpha}$

$$\mathbf{T} \left| \begin{array}{l} T_2 = Y_2 - (Y_1 + \frac{1}{Y_1}) \bmod T_1 = Y_2 - (Y_1^5 - 5Y_1^4 + 6Y_1^3 - 9Y_1^2 + 5Y_1 - 5) \\ T_1(Y_1) = Y_1^6 - 5Y_1^5 + 6Y_1^4 - 9Y_1^3 + 6Y_1^2 - 5Y_1 + 1 \end{array} \right.$$

- Changement d'ordre $Y_2 < Y_1$

$$\left| \begin{array}{l} Y_1^2 - Y_2 Y_1 + 1 \\ Y_2^3 - 5Y_2^2 + 3Y_2 + 1 \end{array} \right.$$

- $Y_2^3 - 5Y_2^2 + 3Y_2 + 1 = (Y_2^2 - 4Y_2 - 1)(Y_2 - 1)$
- Restauration de l'ordre

$$\left| \begin{array}{l} Y_1^2 - Y_2 Y_1 + 1 \\ Y_2^2 - 4Y_2 - 1 \end{array} \right. \Longrightarrow \left| \begin{array}{l} Y_2 + Y_1^3 - 4Y_1^2 - 4 \\ Y_1^4 - 4Y_1^3 + Y_1^2 - 4Y_1 + 1 \end{array} \right.$$

Un exemple

C. Pascal & É. Schost 2006, *Change of order for bivariate triangular sets*

- But : un facteur de $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Racines de T_1 invariantes par $\alpha \mapsto \frac{1}{\alpha}$
- Changement d'ordre $Y_2 < Y_1$
- $Y_2^3 - 5Y_2^2 + 3Y_2 + 1 = (Y_2^2 - 4Y_2 - 1)(Y_2 - 1)$
- Restauration de l'ordre

$\Longrightarrow$ degré du polynôme à factoriser /2

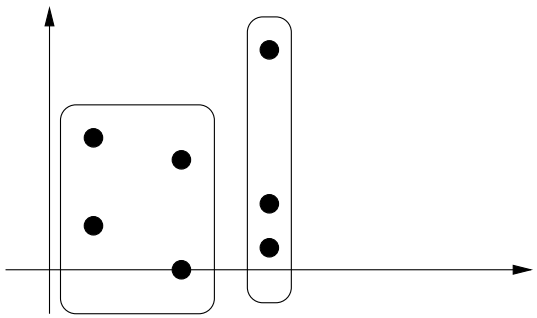
Problèmes considérés

Multiplication	$O^{\sim}(4^s \delta_{\mathbf{T}})$	Li, Moreno Maza & Schost 09
Quasi-inverse	$O^{\sim}(K^s \delta_{\mathbf{T}})$	Dahan, Moreno Maza, Schost & Xie 06
Changement d'ordre	$O^{\sim}(\delta_{\mathbf{d}}^{(\omega+1)/2})$	Pascal & Schost 06 ; $s = 2$

Problèmes considérés

Multiplication	$O^{\sim}(4^s \delta_{\mathbf{T}})$	Li, Moreno Maza & Schost 09
Quasi-inverse	$O^{\sim}(K^s \delta_{\mathbf{T}})$	Dahan, Moreno Maza, Schost & Xie 06
Changement d'ordre	$O^{\sim}(\delta_{\mathbf{d}}^{(\omega+1)/2})$	Pascal & Schost 06 ; $s = 2$
Déc. équiprojetable	$(n \log d)^{O(1)} d^{n^{\mathbf{O(1)}}}$	Szántó 97 ; cas non radical, dim. qcq

$$I = \langle T_1 \rangle \cup \cdots \cup \langle T_n \rangle$$



Objectif : algorithmes quasi-linéaires

Idée : représentation univariée

- Représentation univariée $\mathscr{U} = (P, \mathbf{U}, \mu)$ d'un idéal I :

$$\begin{array}{rccc} \psi_{\mathscr{U}} : & \mathbb{K}[\mathbf{X}]/I & \to & \mathbb{K}[Z]/\langle P \rangle \\ & X_1, \ldots, X_s & \mapsto & U_1, \ldots, U_s \\ & \mu_1 X_1 + \cdots + \mu_s X_s & \leftarrow\!\shortmid & Z \end{array} .$$

Idée : représentation univariée

- Représentation univariée $\mathscr{U} = (P, \mathbf{U}, \mu)$ d'un idéal I :

$$\begin{array}{rccc} \psi_{\mathscr{U}} : & \mathbb{K}[\mathbf{X}]/I & \to & \mathbb{K}[Z]/\langle P \rangle \\ & X_1, \ldots, X_s & \mapsto & U_1, \ldots, U_s \ . \\ & \mu_1 X_1 + \cdots + \mu_s X_s & \leftarrow\!\shortmid & Z \end{array}$$

- Trouver $\mathscr{U}$? $\to$ s étapes bivariées (représentation « mixte »)

$\Longrightarrow$ composition modulaire et projection des puissances.

Total : $O(s^2 \mathsf{C}(\delta_{\mathbf{T}}))$

Composition modulaire

- Cas univarié : calculer $F(G) \mod H$.
- Cas multivarié :
  * $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$; $\delta_{\mathbf{f}} = f_1 \cdots f_m$
  * $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $F \in \mathbb{K}[X_1, \cdots, X_m]_{\mathbf{f}}$,
  * Calculer $F(G_1, \cdots, G_m) \in R_{\mathbf{T}}$.
- Complexité $\mathsf{C}(\delta_{\mathbf{f}}, \delta_{\mathbf{T}})$; $\mathsf{C}(\delta_{\mathbf{T}}, \delta_{\mathbf{T}})$ noté $\mathsf{C}(\delta_{\mathbf{T}})$.

Composition modulaire

- Cas univarié : calculer $F(G) \mod H$.
- Cas multivarié :
  * $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$; $\delta_{\mathbf{f}} = f_1 \cdots f_m$
  * $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $F \in \mathbb{K}[X_1, \cdots, X_m]_{\mathbf{f}}$,
  * Calculer $F(G_1, \cdots, G_m) \in R_{\mathbf{T}}$.
- Complexité $\mathsf{C}(\delta_{\mathbf{f}}, \delta_{\mathbf{T}})$; $\mathsf{C}(\delta_{\mathbf{T}}, \delta_{\mathbf{T}})$ noté $\mathsf{C}(\delta_{\mathbf{T}})$.
- Représentation matricielle :

$$\begin{pmatrix} \vdots & & \vdots \\ G_1^0 \cdots G_m^0 \mod \langle \mathbf{T} \rangle & \cdots & G_1^{f_1-1} \cdots G_m^{f_m-1} \mod \langle \mathbf{T} \rangle \\ \vdots & & \vdots \end{pmatrix}_{\delta_{\mathbf{T}} \times \delta_{\mathbf{f}}} * \begin{pmatrix} \vdots \\ F \\ \vdots \end{pmatrix}_{\delta_{\mathbf{f}} \times 1}$$

Projection des puissances

- Cas univarié calculer $\tau(G^i \bmod H)$ pour $i < f$.
- Cas multivarié $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$
  - $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $\tau : R_{\mathbf{T}} \to \mathbb{K}$,
  - Calculer $\tau(G_1^{a_1} \cdots G_m^{a_m} \bmod \langle \mathbf{T} \rangle)$, pour $0 \leq a_i < f_i$, $i = 1, \ldots, m$.

Projection des puissances

- Cas univarié calculer $\tau(G^i \bmod H)$ pour $i < f$.
- Cas multivarié $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$
  - $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $\tau : R_{\mathbf{T}} \to \mathbb{K}$,
  - Calculer $\tau(G_1^{a_1} \cdots G_m^{a_m} \bmod \langle \mathbf{T} \rangle)$, pour $0 \leq a_i < f_i$, $i = 1, \ldots, m$.
- Problème transposé de la composition modulaire :

$$\begin{pmatrix} \cdots & \ell & \cdots \end{pmatrix}_{1 \times \delta_{\mathbf{T}}} * \begin{pmatrix} \vdots & & \vdots \\ G_1^0 \cdots G_m^0 \bmod \langle \mathbf{T} \rangle & \cdots & G_1^{f_1-1} \cdots G_m^{f_m-1} \bmod \langle \mathbf{T} \rangle \\ \vdots & & \vdots \end{pmatrix}_{\delta_{\mathbf{T}} \times \delta_{\mathbf{f}}}$$

$$\Longrightarrow \text{complexité } C(\delta_{\mathbf{f}}, \delta_{\mathbf{T}})$$

$C(\delta_f, \delta_T) = ?$

- Modèle algébrique :

  → Brent & Kung 78

  - Cas $m = s = 1$, $\delta_f = \delta_T = d$.
  - $C(d) = O(d^{(\omega+1)/2})$

  → Généralisation :

  - Cas $m, s \in \{1, 2\}$, $\delta_f = O(\delta_T)$.
  - $C(\delta_T) = O(\delta_T^{(\omega+1)/2})$

Idée :

1. « Découper » F avec $\delta_f^{1/2}$ polynômes de degré $f_1^{1/2} \times f_2^{1/2}$,

   $\Longrightarrow$ calcul de $G_1^{j_1} G_2^{j_2}$, $j_k < f_k^{1/2}$. $O(\delta_f^{1/2} 4^s \delta_T)$.

2. Faire le calcul matriciel pour chaque « petit » polynôme. $O(\delta_T^{(\omega+1)/2})$
3. Trouver le résultat avec un schéma de Horner. $O(\delta_f^{1/2} 4^s \delta_T)$

$C(\delta_f, \delta_T) = ?$

- Modèle algébrique :
  - $\rightarrow$ Brent & Kung 78
    - Cas $m = s = 1$, $\delta_f = \delta_T = d$.
    - $C(d) = O(d^{(\omega+1)/2})$
  - $\rightarrow$ Généralisation :
    - Cas $m, s \in \{1, 2\}$, $\delta_f = O(\delta_T)$.
    - $C(\delta_T) = O(\delta_T^{(\omega+1)/2})$
- Modèle booléen : $\mathbb{K} = \mathbb{F}_q$; complexité binaire
  - $\rightarrow$ Kedlaya & Umans (à paraître) :
    - Cas $s = 1$, $\mathbf{f} = (d, \cdots, d)$, $\delta_T = N$.
    - $C(d^m, N) = (d^m + N)^{1+\varepsilon} \log^{1+o(1)}(q)$
  - $\rightarrow$ Généralisation :
    - Cas $m, s \in \{1, 2\}$.
    - $C(\delta_f, \delta_T) = (\delta_f + \delta_T)^{1+\varepsilon} \log(q) \operatorname{plog}(\log q)$

Composition modulaire sur les corps finis

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

1. Si nécessaire, plongement $\mathbb{F}_q \to \mathbb{F}_{q'}$, $q' = q^t$

   $\Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{e}})\,\mathrm{plog}_{\varepsilon,s,m}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})$ op. dans $\mathbb{F}_{q'}$
2. Reformater F

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

1. Si nécessaire, plongement $\mathbb{F}_q \to \mathbb{F}_{q'}$, $q' = q^t$

   $\Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{e}})\,\mathrm{plog}_{\varepsilon,s,m}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})$ op. dans $\mathbb{F}_{q'}$

2. Reformater F

$$\Lambda_{\mathbf{f},\mathbf{f}'} : \quad \mathbb{F}_{q'}[X_1, \ldots, X_m]_{\mathbf{f}} \quad \to \quad \mathbb{F}'_q[X_{1,0}, \ldots, X_{m,\ell_m-1}]_{\mathbf{f}'}$$

- $\mathbf{f} = (f_1, \cdots, f_m) \to \mathbf{f}' = (\underbrace{f'_1, \cdots, f'_1}_{\ell_1 \text{ fois}}, \cdots, \underbrace{f'_m, \cdots, f'_m}_{\ell_m \text{ fois}})$
- # variables : $m \to m' = \ell_1 + \cdots + \ell_m$
- degrés : $f_i \to f'_i = \left\lceil f_i^{1/\ell_i} \right\rceil$

$$\Lambda^{\star}_{\mathbf{f},\mathbf{f}'} : \quad R_{\mathbf{T}}^{m} \quad \to \quad R_{\mathbf{T}}^{m'}$$

$$G_i \quad \mapsto \quad G_i, G_i^{f'_i}, \ldots, G_i^{f_i'^{\ell_i-1}}$$

- Égalité fondamentale : $F(G) = \Lambda_{\mathbf{f},\mathbf{f}'}(F)\big(\Lambda^{\star}_{\mathbf{f},\mathbf{f}'}(G)\big)$
- Coût : $F = O(\delta_{\mathbf{f}'})$ op. dans $\mathbb{F}_{q'}$; $G = O(\log(\delta_{\mathbf{f}'}))$ mult. dans $R_{\mathbf{T}}$.

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

1. Si nécessaire, plongement $\mathbb{F}_q \to \mathbb{F}_{q'}$, $q' = q^t$

   $\Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{e}})\,\mathrm{plog}_{\varepsilon,s,m}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})$ op. dans $\mathbb{F}_{q'}$

2. Reformater F

   $\Longrightarrow (4^s\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})\,\mathrm{plog}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})$ op. dans $\mathbb{F}_{q'}$

3. Évaluation multipoint « structurée » : B_i t.q. $\#B_i = d_i' = m'f'd_i$
   $g_b' := (G_1'(b), \ldots, G_{m'}'(b)) \in \mathbb{F}_{q'}^{m'}$, $b \in B_1 \times \cdots \times B_s$

   $\Longrightarrow m'\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

1. Si nécessaire, plongement $\mathbb{F}_q \to \mathbb{F}_{q'}$, $q' = q^t$

   $\Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{e}})\,\mathrm{plog}_{\varepsilon,s,m}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})$ op. dans $\mathbb{F}_{q'}$

2. Reformater F

   $\Longrightarrow (4^s\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})\,\mathrm{plog}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})$ op. dans $\mathbb{F}_{q'}$

3. Évaluation multipoint « structurée » : B_i t.q. $\#B_i = d_i' = m'f'd_i$
   $g_b' := (G_1'(b), \ldots, G_{m'}'(b)) \in \mathbb{F}_{q'}^{m'}$, $b \in B_1 \times \cdots \times B_s$

   $\Longrightarrow m'\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

4. Evaluation multipoint multivariée : $f_b' = F'(g_b')$

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

4. Evaluation multipoint multivariée : $f'_b = F'(g'_b)$

$$\begin{array}{rccc} \text{Eval}_B : & \mathbb{F}_q[\mathbf{X}]_{\mathbf{f}} & \to & \mathbb{F}_q^N \\ & F & \mapsto & [F(b) \mid b \in B] \end{array} \quad \text{et } \text{Eval}_B^t : \mathbb{F}_q^N \to \mathbb{F}_q[\mathbf{X}]_{\mathbf{f}}^*$$

$$\Longrightarrow \text{Kedlaya \& Umans : } (\delta_{\mathbf{f}} + N)^{1+\varepsilon} \log(q) \operatorname{plog}_{\varepsilon,m}(\log(q))$$

Idées :

1. On considère les données dans $\mathbb{Z}$ (ou $\mathbb{Z}[Z]$).
2. Réductions succesives modulo des petits p.
3. $p \simeq f_1 + \cdots + f_m \Longrightarrow$ évaluation en tous les points de $\mathbb{F}_p^m$ (FFT).
4. Théorème des Restes Chinois.

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

1. Si nécessaire, plongement $\mathbb{F}_q \to \mathbb{F}_{q'}$, $q' = q^t$

   $\Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{e}})\,\mathrm{plog}_{\varepsilon,s,m}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})$ op. dans $\mathbb{F}_{q'}$

2. Reformater F

   $\Longrightarrow (4^s\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})\,\mathrm{plog}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})$ op. dans $\mathbb{F}_{q'}$

3. Évaluation multipoint « structurée » : B_i t.q. $\#B_i = d_i' = m'f'd_i$
   $g_b' := (G_1'(b), \ldots, G_{m'}'(b)) \in \mathbb{F}_{q'}^{m'}$, $b \in B_1 \times \cdots \times B_s$

   $\Longrightarrow m'\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

4. Evaluation multipoint multivariée : $f_b' = F'(g_b')$

   $\Longrightarrow (\delta_{\mathbf{d}'} + \delta_{\mathbf{f}'})^{1+\varepsilon}\log(q')\,\mathrm{plog}_{\varepsilon,s,m}(\log(q'))$

5. Interpolation : $\varphi = F'(G_1', \ldots, G_{m'}')$.

   $\Longrightarrow m'\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

6. Retourner $\varphi \mod \langle T \rangle$.

   $\Longrightarrow 4^s\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f, \cdots, f)$, m=cte et $s \leq 2$

1. Si nécessaire, plongement $\mathbb{F}_q \to \mathbb{F}_{q'}$, $q' = q^t$

   $\Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{e}})\,\mathrm{plog}_{\varepsilon,s,m}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})$ op. dans $\mathbb{F}_{q'}$

2. Reformater F

   $\Longrightarrow (4^s\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})\,\mathrm{plog}(\delta_{\mathbf{T}} + \delta_{\mathbf{f}'})$ op. dans $\mathbb{F}_{q'}$

3. Évaluation multipoint « structurée » : B_i t.q. $\#B_i = d_i' = m'f'd_i$
   $g_b' := (G_1'(b), \ldots, G_{m'}'(b)) \in \mathbb{F}_{q'}^{m'}$, $b \in B_1 \times \cdots \times B_s$

   $\Longrightarrow m'\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

4. Evaluation multipoint multivariée : $f_b' = F'(g_b')$

   $\Longrightarrow (\delta_{\mathbf{d}'} + \delta_{\mathbf{f}'})^{1+\varepsilon}\log(q')\,\mathrm{plog}_{\varepsilon,s,m}(\log(q'))$

5. Interpolation : $\varphi = F'(G_1', \ldots, G_{m'}')$.

   $\Longrightarrow m'\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

6. Retourner $\varphi \mod \langle T \rangle$.

   $\Longrightarrow 4^s\delta_{\mathbf{d}'}\,\mathrm{plog}(\delta_{\mathbf{d}'})$ op. dans $\mathbb{F}_{q'}$

Total : $(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})^{1+\varepsilon}\log(q)\,\mathrm{plog}_{\varepsilon,s,m}(\log(q))$

Cas $\mathbb{K} = \mathbb{F}_q$, $\mathbf{f} = (f_1, f_2)$ et $s \leq 2$

Hyp : $\varepsilon \leq 1$ et $f_1 \leq f_2$

$\rightarrow$ $f_2 \leq f_1^{\frac{1}{\varepsilon}}$: cas équilibré

1. $\ell_1 = \lceil \frac{1}{\varepsilon} \rceil$, $\ell_2 = \lceil \frac{1}{\varepsilon} \log_{f_1}(f_2) \rceil$ et $f = \lceil f_1^{\varepsilon} \rceil$; $\mathbf{f}' = (f, \ldots, f) \in \mathbb{N}^{\ell_1 + \ell_2}$
2. Composition modulaire, paramètre $\mathbf{f}'$

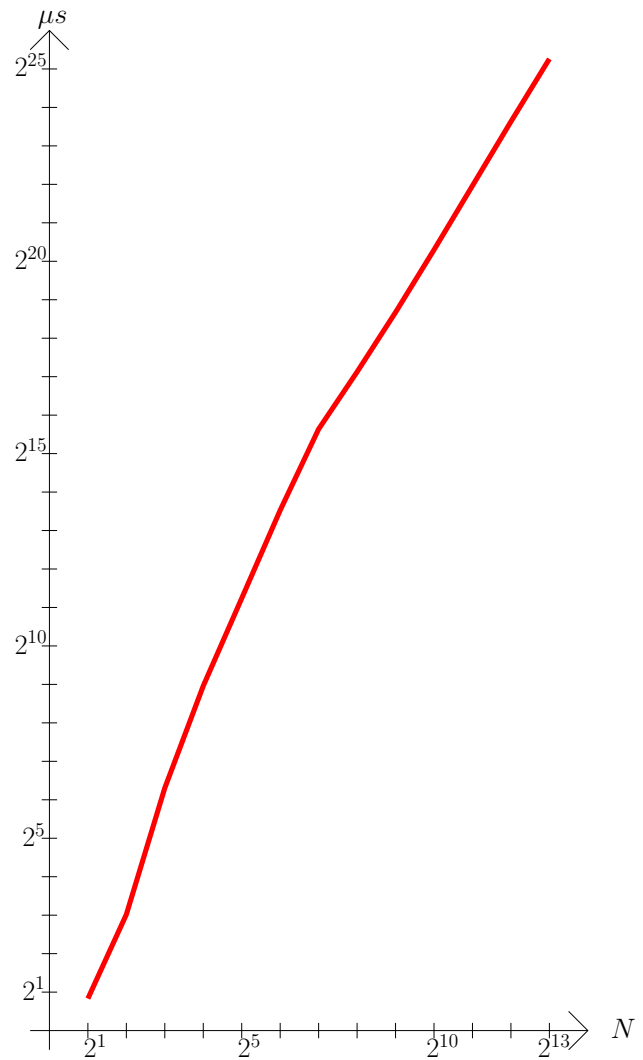
Coût : $\delta_{\mathbf{f}'} \leq 2^{\frac{1}{\varepsilon} + \frac{1}{\varepsilon^2} + 2} \delta_{\mathbf{f}}^{1+\varepsilon} \Longrightarrow (\delta_{\mathbf{T}} + \delta_{\mathbf{f}})^{1+3\varepsilon} \log(q) \operatorname{plog}_{\varepsilon,s}(\log(q))$

$\rightarrow$ $f_2 \geq f_1^{\frac{1}{\varepsilon}} \Rightarrow f_1 \leq \delta_{\mathbf{f}}^{\varepsilon}$: f_1 compositions modulaires univariées + Horner.

Coût : $(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})^{1+2\varepsilon} \log(q) \operatorname{plog}_{\varepsilon,s}(\log(q))$

Remarque : un algorithme (pour l'instant) théorique

- R. Basson & G. Lecerf : implémentation C++ pour Mathémagix
  - $f(g(X)) \mod h(X)$; $\deg_X f, g, h < N$
  - $\mathbb{K} = \mathbb{F}_p$, $p \sim 2^{32}$



Changement de représentation

Idée générale

- I idéal de $\mathbb{K}[\mathbf{Y}]$, $R = \mathbb{K}[\mathbf{Y}]/I$ et $\delta = [R : \mathbb{K}[\mathbf{Y}]]$.
- Représentation primitive $\mathscr{U}$ de I : élément primitif + isomorphismes
- Représentation j-mixte $\mathscr{M} = (\mathbf{P}, \mathbf{M}, \mu)$ de I :

  ensemble triangulaire de $\mathbb{K}[Y, Y_{j+1}, \ldots, Y_s]$ + isomorphismes

$$\begin{array}{rccc} \Psi_{\mathscr{M}} : & \mathbb{K}[\mathbf{Y}]/I & \to & \mathbb{K}[Y, Y_{j+1}, \ldots, Y_s]/\langle \mathbf{P} \rangle \\ & Y_1, \ldots, Y_j & \mapsto & M_1, \ldots, M_j \\ & Y_{j+1}, \ldots, Y_s & \mapsto & Y_{j+1}, \ldots, Y_s \\ & \sum_{k \leq j} \mu_k Y_k & \leftarrow\!\shortmid & Y \end{array}$$

Utilisation des formules de trace

1. I idéal radical, $A, B \in R = \mathbb{K}[\mathbf{Y}]/I$.
   - $(\mathrm{tr}(A^j))_{j<2\delta}$ donné.
     - A élément primitif ?
     - oui $\rightarrow$ polynôme minimal P
   - P et $(\mathrm{tr}(BA^j))_{j<\delta}$ donnés.
     - $V \in \mathbb{K}[Y]$ de degré $< \delta$, tel que $B = V(A) \in R$ (si possible).

2. $I \subset \mathbb{K}[Y_1, Y_2]$ idéal radical ; hypothèse : $\mathrm{car}(\mathbb{K}) > \delta$
   - $(\mathrm{tr}(Y_1^j))_{j<\delta}$ donné.
     - I engendré par $(T_1(Y_1), T_2(Y_1, Y_2))$?
     - oui $\rightarrow$ calculer T_1
   - T_1 et $(\mathrm{tr}(Y_1^i Y_2^j))_{i<d_1, j<d_2}$, avec $d_1 = \deg(T_1)$ et $d_2 = \delta/d_1$ donnés
     - calculer T_2.

$$\Longrightarrow \delta\mathrm{plog}(\delta) \text{ op. dans } \mathbb{K}$$

Changement de représentation : cas $s = 2$

$\mathbb{K} = \mathbb{F}_q$, $\mathbf{T} = (T_1, T_2)$ dans $\mathbb{F}_q[Y_1, Y_2]$, degré $\mathbf{d} = (d_1, d_2)$; $q \geq \delta_{\mathbf{T}}^2$

- $\mathbf{T}$ sans facteur carré ?

  calcul de pgcd

- Oui ? calcul d'une représentation primitive $\mathscr{U}$

  calcul de traces : projection des puissances

- $\mathscr{U}$ et $B \in R_{\mathbf{T}}$ donnés, calculer $\psi_{\mathscr{U}}(B) \in \mathbb{F}_q[Y]/P$

  composition modulaire

- $\mathscr{U}$ et $B \in \mathbb{F}_q[Y]/P$ donnés, calculer $\varphi_{\mathscr{U}}(B) \in R_{\mathbf{T}}$

  composition modulaire

$$\Longrightarrow \text{Coût : } O(\mathsf{C}(\delta_{\mathbf{T}}))$$

Changement de représentation : cas général

1. $\mathbf{d} \in \mathbb{N}^s$, $\mathbf{T} = (T_1, \ldots, T_s)$ dans $\mathbb{F}_q[\mathbf{Y}]$, $q \geq \delta_{\mathbf{T}}^2$

   - $\langle T_1, T_2 \rangle$ idéal radical ? *calcul de pgcd*
   - Oui ? calcul d'une représentation 2-mixte $\mathscr{M}$ de $\mathbf{T}$

     calcul de traces : projection des puissances + compositions modulaires

     $$\Longrightarrow O(s\,\mathsf{C}(\delta_{\mathbf{T}}))$$
   - Calcul des isomorphismes : *compositions modulaires*

     $$\Longrightarrow O(\mathsf{C}(\delta_{\mathbf{T}}))$$

2. « Répétition » s fois : $O(s^2\,\mathsf{C}(\delta_{\mathbf{T}}))$

Résultats

Opérations modulo $\langle T \rangle$

1. Cas $\mathbb{K} = \mathbb{F}_q$: $q \geq \delta_{\mathbf{T}} \Rightarrow q' = q$; $q < \delta_{\mathbf{T}} \Rightarrow$ extension
2. $\mathscr{U} = (P, \mathbf{U}, \mu)$ représentation primitive de $\mathbf{T}$: $O(s^2 \mathsf{C}(\delta_{\mathbf{T}}))$
3. Opérations dans $\mathbb{K}[Y]/\langle P \rangle$.
   - Multiplication : $\delta_{\mathbf{T}} \operatorname{plog}(\delta_{\mathbf{T}})$
   - Inversion : *pgcd étendu* $\delta_{\mathbf{T}} \operatorname{plog}(\delta_{\mathbf{T}})$
   - Norme : *résultant* $\delta_{\mathbf{T}} \operatorname{plog}(\delta_{\mathbf{T}})$
   - Composition modulaire : $m \leq 2$ $O(\delta_{\mathbf{T}}^{(\omega+1)/2})$
     $(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})^{1+\varepsilon} \log(q') \operatorname{plog}_{\varepsilon}(\log(q'))$
   - Projection des puissances : *algorithme transposé*
     $O(\delta_{\mathbf{T}}^{(\omega+1)/2})$
     $(\delta_{\mathbf{T}} + \delta_{\mathbf{f}})^{1+\varepsilon} \log(q') \operatorname{plog}_{\varepsilon}(\log(q'))$

Décomposition équiprojetable / changement d'ordre

- Stratégie :

  1. Calcul d'une représentation univariée $\mathscr{U} = (P, \mathbf{U}, \mu)$
  2. Cas bivarié : $O(\mathsf{C}(\delta_{\mathbf{T}}) \log(\delta_{\mathbf{T}}))$
     - $\mu' = \mu'_1 Y_1 + \cdots + \mu'_{s-1} Y_{s-1}$ élt primitif ($s-1$ premières variables).

       Composition modulaire inverse (traces ; proj. puissances)
     - Calcul de son polynôme caractéristique : $\chi_{\mu'} = C_1^{r_1} \cdots C_n^{r_n}$

       Calcul de traces $\rightarrow$ projection des puissances
     - Calculer $\gcd(C_i(\mu'_1 U_1 + \cdots + \mu'_{s-1} U_{s-1}), P)$, $1 \leq i \leq n$.

       Calcul récursif suivant l'arbre de décomposition de $\chi_{\mu'}$
  3. « Répétition » s fois

- Coût total : $O(s\, \mathsf{C}(\delta_{\mathbf{T}}) \log(\delta_{\mathbf{T}}))$

- Remarque : on suppose $\mathrm{car}(\mathbb{K}) \geq \delta_{\mathbf{T}}$

Bench en Maple : comparaison avec RegularChains

d_i	δ_T	Nous	Maple
2	3	.30e-1	.119
3	6	.41e-1	.40e-1
4	10	.70e-1	.119
5	15	.81e-1	.269
6	21	.161	.699

$s = 2$

d_i	δ_T	Nous	Maple
2	4	.40e-1	.31e-1
3	10	.81e-1	.140
4	20	.170	.590
5	35	.330	1.740
6	56	.520	4.980

$s = 3$

d_i	δ_T	Nous	Maple
2	5	.80e-1	.50e-1
3	15	.200	.380
4	35	.510	2.280
5	70	1.060	8.800
6	126	2.510	39.450

$s = 4$

d_i	δ_T	Nous	Maple
2	6	.230	.100
3	21	.370	1.000
4	56	1.090	6.660
5	126	3.230	45.220
6	252	12.380	459.130

$s = 5$

d_i	δ_T	Nous	Maple
2	7	.360	.160
3	28	.670	2.170
4	84	2.490	19.640
5	210	10.570	262.100
6	462	62.940	6155.290

$s = 6$

Application

Comptage de points d'une courbe elliptique

- Question : nombre de points de $E : Y^2 = X^3 + AX + B$ sur $\mathbb{F}_p$.
- *Schoof 85* : recherche modulo plusieurs premiers ℓ

  travail modulo le polynôme de division ψ_ℓ, degré $(\ell^2 - 1)/2$.
- *Elkies 92* : travail modulo f_ℓ, facteur de ψ_ℓ de degré $(\ell - 1)/2$.
  1. $\Phi_\ell(J, J')$ ℓ-ième polynôme modulaire ; $\varphi_\ell = \Phi_\ell \mod p$
  2. Calcul de α racine de $\varphi(J, j(E))$; $j(E)$ j-ième invariant de E.
  3. En déduire f_ℓ.

  - Complexité :
    - *Lercier & Sirvent 08* $\rightarrow \tilde{O}(\ell \log^2 p)$
    - taille de $\Phi_\ell \rightarrow \Omega(\ell^3)$

Travaux de Charlap, Coley & Robbins 1991

- Variante de Elkies : approche algébrique pour trouver f_ℓ facteur de ψ_ℓ.
- Soient
  - $g_m = \gamma_m \mod \psi_m$ où $[m](x,y) = (\gamma_m(x), y\eta_m(x))$,
  - $A = \sum_{i=1}^{(\ell-1)/2} g_i$; m_A polynôme minimal de $A \mod \psi_\ell$.
- $\langle \psi_\ell(Y), Z - A(Y) \rangle$ généré par $(m_A(Z), Q(Z,Y))$
- $\deg(m_A) = \ell + 1$ et $\alpha \in \mathbb{F}_p$ racine de $m_A \Longrightarrow Q(\alpha, Y)$ facteur de ψ_ℓ.
- Complexité : *Peters 2006* $\tilde{O}(\ell^4 + \ell \log p)$ op. dans $\mathbb{F}_p$.

Utiliser la composition modulaire

1. Calcul de ψ_ℓ : $\ell^2 \log(p)\,\mathrm{plog}(\ell \log(p))$ op.
2. Calcul de $A = \sum_{i=0}^{(\ell-1)/2-1} g_{\tau^i}$ où $\mathbb{F}_\ell^* = \langle \tau \rangle$. Si $(l-1)/2 = 2^k$,
   - $\{G_i = g_{\tau^{2^i}}\}_{1 \le i \le k}$ via $G_{i+1} = G_i(G_i) \bmod \psi_\ell$
   - $\{A_i = \sum_{j=0}^{2^i-1} g_{\tau^j}\}_{1 \le i \le k}$ via $A_{i+1} = A_i(G_i) \bmod \psi_\ell$

   Coût : $O(\log(\ell))$ comp. modulaires $= \ell^{2+\varepsilon} \log(p)\,\mathrm{plog}_\varepsilon(\log(p))$ op.
3. Changement d'ordre $\ell^{2+\varepsilon} \log(p)\,\mathrm{plog}_\varepsilon(\log(p))$ op.
4. Racine $\alpha \in \mathbb{F}_p$ de m_A $\ell \log(p)^2\,\mathrm{plog}(\ell \log(p))$ op.

Total $\left(\ell^{2+\varepsilon} \log(p) + \ell \log(p)^2\right) \mathrm{plog}_\varepsilon(\ell \log(p))$ op.

Conclusion

- Complexité binaire quasi-linéaire / sous-quadratique pour différentes opérations modulo un ensemble triangulaire :
  - multiplication, inversion et calcul de norme, composition modulaire et projection des puissances,
  - changement d'ordre, décomposition équiprojetable.
  - résultats pratiques intéressants
- Application : problème du comptage de points d'une courbe elliptique,
  - complexité théorique compétitive
  - ne nécessite pas les polynômes modulaires.
- Questions ouvertes :
  - cas algébrique : algorithme quasi-linéaire ?
  - cas booléen : algorithme pratique ? Application viable ?
  - idéaux non radicaux ?