On the complexity of computations modulo zero-dimensional triangular sets.

Adrien Poteaux[⋆] [†], Éric Schost[†]

[⋆]: Calcul Formel - LIFL - Université Lille 1

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

GBReLA 2013, Hagenberg, Austria

Thursday, September 5th 2013

On the complexity of computations modulo zero-dimensional triangular sets.

Adrien Poteaux, Éric Schost

- *Modular composition modulo triangular sets and applications*

  Computational Complexity, September 2013, Volume 22, Issue 3, pp 463-516

- *On the complexity of computing with zero-dimensional triangular sets*

  Journal of Symbolic Computation, Volume 50, March 2013, Pages 110-138

Triangular sets

- $\mathbb{K}$ a field.
- $\mathbf{Y} = Y_1, \ldots, Y_s$ variables on $\mathbb{K}$, order $Y_1 < \cdots < Y_s$.
- Triangular set (monic, squarefree, of dimension 0):

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

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

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

One example

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

- Aim: a factor of $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.

One example

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

- Aim: a factor of $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Roots of T_1 invariants by $\alpha \mapsto \frac{1}{\alpha}$

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

One example

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

- Aim: a factor of $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Roots of T_1 invariants by $\alpha \mapsto \frac{1}{\alpha}$

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

- Change of order $Y_2 < Y_1$

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

One example

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

- Aim: a factor of $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Roots of T_1 invariants by $\alpha \mapsto \frac{1}{\alpha}$

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

- Change of order $Y_2 < Y_1$

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

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

One example

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

- Aim: a factor of $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Roots of T_1 invariants by $\alpha \mapsto \frac{1}{\alpha}$

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

- Change of order $Y_2 < Y_1$

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

- $Y_2^3 - 5Y_2^2 + 3Y_2 + 1 = (Y_2^2 - 4Y_2 - 1)(Y_2 - 1)$
- Back to the initial order

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

One example

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

- Aim: a factor of $T_1 = Y^6 - 5Y^5 + 6Y^4 - 9Y^3 + 6Y^2 - 5Y + 1$.
- Roots of T_1 invariants by $\alpha \mapsto \frac{1}{\alpha}$
- Change of order $Y_2 < Y_1$
- $Y_2^3 - 5Y_2^2 + 3Y_2 + 1 = (Y_2^2 - 4Y_2 - 1)(Y_2 - 1)$
- Back to the initial order

$\Longrightarrow$ degree of the polynomial /2

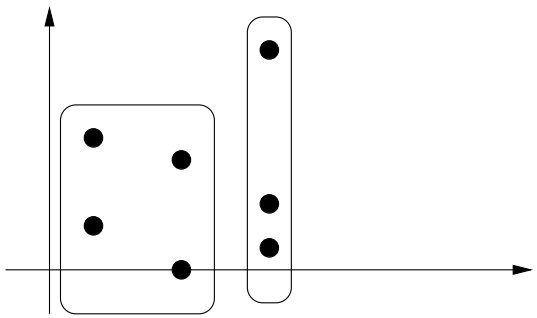
Problems we consider

Multiplication	$\tilde{O}(4^s\delta)$	Li, Moreno Maza & Schost 09
Quasi-inverse	$\tilde{O}(K^s\delta)$	Dahan, Moreno Maza, Schost & Xie 06
Change of order	$\tilde{O}(\delta^{(\omega+1)/2})$	Pascal & Schost 06 ; $s = 2$

Problems we consider

Multiplication	$\tilde{O}(4^s\delta)$	Li, Moreno Maza & Schost 09
Quasi-inverse	$\tilde{O}(K^s\delta)$	Dahan, Moreno Maza, Schost & Xie 06
Change of order	$\tilde{O}(\delta^{(\omega+1)/2})$	Pascal & Schost 06 ; $s = 2$
Equiprojetable dec.	$(s \log d)^{O(1)} d^{s^{O(1)}}$	Szántó 97 ; non radical case, dim ≥ 0

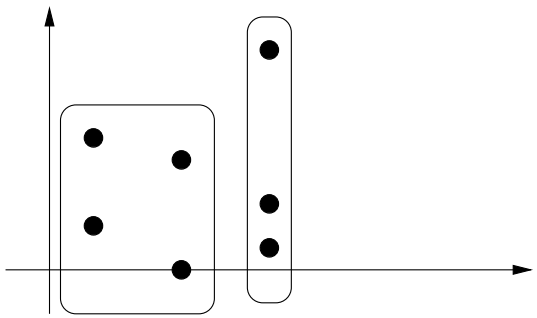
$$I = \langle T_1 \rangle \cup \cdots \cup \langle T_n \rangle$$



Problems we consider

Multiplication	$\tilde{O}(4^s\delta)$	Li, Moreno Maza & Schost 09
Quasi-inverse	$\tilde{O}(K^s\delta)$	Dahan, Moreno Maza, Schost & Xie 06
Change of order	$\tilde{O}(\delta^{(\omega+1)/2})$	Pascal & Schost 06 ; $s = 2$
Equiprojetable dec.	$(s \log d)^{O(1)} d^{s^{O(1)}}$	Szántó 97 ; non radical case, dim ≥ 0

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



We want: quasi-linear algorithms

Idea: univariate representation

- Univariate representation $\mathscr{U} = (P, \mathbf{U}, \mu)$ of an ideal I:

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

Idea: univariate representation

- Univariate representation $\mathscr{U} = (P, \mathbf{U}, \mu)$ of an ideal I:

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

- Finding $\mathscr{U}$? $\to$ s bivariate steps ("mixed" representation)

  $\Longrightarrow$ modular composition and power projection.

Total: $O(s^2 \mathsf{C}(\delta))$

Modular composition

- Univariate case: $F(G) \mod H$.
- Multivariate case: $F(G_1, \cdots, G_m) \in R_{\mathbf{T}}$.
  * $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$; $f_1 \cdots f_m = \delta$
  * $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $F \in \mathbb{K}[X_1, \cdots, X_m]_{\mathbf{f}}$,
- Complexity denoted $\mathsf{C}(\delta)$.

Modular composition

- Univariate case: $F(G) \mod H$.
- Multivariate case: $F(G_1, \cdots, G_m) \in R_{\mathbf{T}}$.
  - $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$; $f_1 \cdots f_m = \delta$
  - $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $F \in \mathbb{K}[X_1, \cdots, X_m]_{\mathbf{f}}$,
- Complexity denoted $\mathsf{C}(\delta)$.
- Matrix representation:

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

Power projection

- Univariate case: $\tau(G^i \bmod H)$ with $i < f$.
- Multivariate case: $\tau(G_1^{a_1} \cdots G_m^{a_m} \mod \langle \mathbf{T} \rangle)$; $0 \leq a_i < f_i$, $i = 1, \ldots, m$.
  - $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$
  - $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $\tau : R_{\mathbf{T}} \to \mathbb{K}$,

Power projection

- Univariate case: $\tau(G^i \bmod H)$ with $i < f$.
- Multivariate case: $\tau(G_1^{a_1} \cdots G_m^{a_m} \mod \langle \mathbf{T} \rangle)$; $0 \leq a_i < f_i$, $i = 1, \ldots, m$.
  - $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{N}^m$
  - $\mathbf{T}$, $G_1, \cdots, G_m \in R_{\mathbf{T}}$, $\tau : R_{\mathbf{T}} \to \mathbb{K}$,
- Transposed of the modular composition:

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

$$\Longrightarrow \text{Complexity } \mathsf{C}(\delta)$$

$C(\delta) = ?$

- Algebraic model:
  - $\rightarrow$ Brent & Kung 1978:
    - $m = s = 1$, $\delta = d$.
    - $C(d) = O(d^{(\omega+1)/2})$
  - $\rightarrow$ Generalisation:
    - $m, s \in \{1, 2\}$.
    - $C(\delta) = O(\delta^{(\omega+1)/2})$

- **Idea:**
  1. "Divide" F as $\delta^{1/2}$ polynomials with degrees $f_1^{1/2} \times f_2^{1/2}$,

     $\Longrightarrow$ compute $G_1^{j_1} G_2^{j_2}$, $j_k < f_k^{1/2}$. $O(4^s \delta^{3/2})$.
  2. Use matrix multiplication for the "small" blocks. $O(\delta^{(\omega+1)/2})$
  3. Get the result via Horner. $O(4^s \delta^{3/2})$

$C(\delta) = ?$

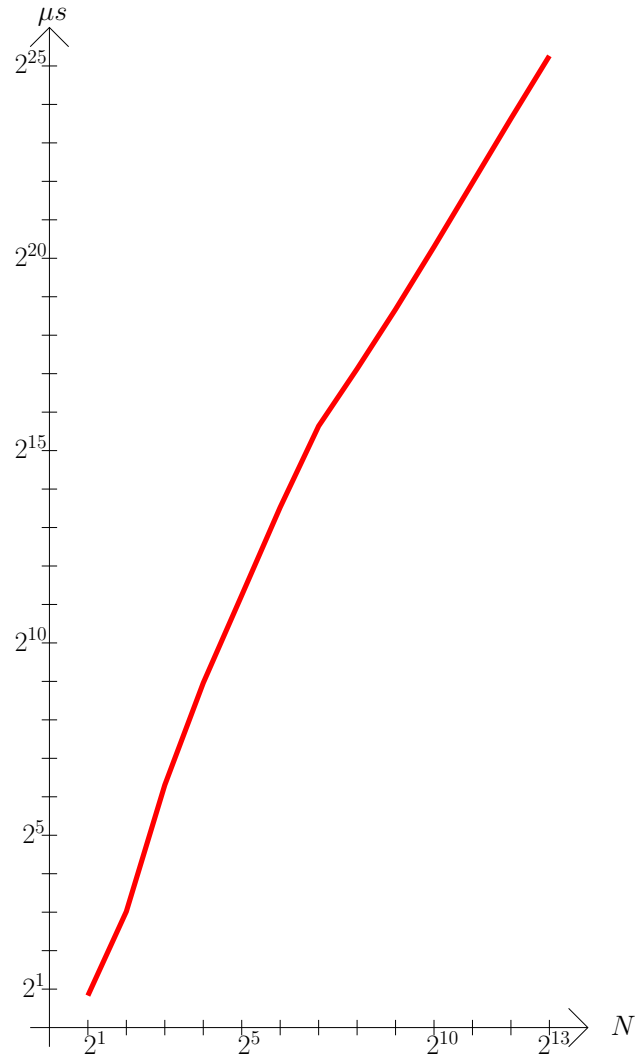
- Boolean model: $\mathbb{K} = \mathbb{F}_q$; binary complexity
  - $\rightarrow$ Kedlaya & Umans 2011:
    - $s = 1$, $\mathbf{f} = (d, \cdots, d)$, $\delta = N$.
    - $C(d^m, N) = (d^m + N)^{1+\varepsilon} \log^{1+o(1)}(q)$
  - $\rightarrow$ Generalisation:
    - $m, s \in \{1, 2\}$.
    - $C(\delta) = \delta^{1+\varepsilon} \log(q) \operatorname{plog}(\log q)$
- **Ideas:**
  - Modular composition $\Longleftrightarrow$ Multivariate Multipoint Evaluation (MME)
    1. Reformat the polynomial (more variables ; smaller degrees)
       $\Longrightarrow$ composition *then* reduction.
    2. Compute the composition via evaluation - interpolation.
       Fast structured evaluation and interpolation + 1 MME
  - Multivariate Multipoint Evaluation:
    1. Data considered in $\mathbb{Z}$ (or $\mathbb{Z}[Z]$) ; successive reductions modulo small p.
    2. $p \simeq m f \Longrightarrow$ evaluation at all points of $\mathbb{F}_p^m$ (FFT) then CRT.

A theoretical algorithm (at least yet)

- R. Basson & G. Lecerf: C++ implementation in Mathemagix

  - $f(g(X)) \mod h(X)$; $\deg_X f, g, h < N$

  - $\mathbb{K} = \mathbb{F}_p$, $p \sim 2^{32}$



Changing representation: $s = 2$

$$\mathbf{T} = (T_1, T_2) \text{ in } \mathbb{K}[Y_1, Y_2] \text{ with degree } \mathbf{d} = (d_1, d_2)$$

$$\text{car}(\mathbb{K}) \geq \delta^2 \text{ or } \text{car}(\mathbb{K}) = 0$$

- $\mathbf{T}$ squarefree ?

  gcd computation

- Yes ? compute a primitive representation $\mathscr{U}$

  trace computations: power projection

- Isomorphisms ?

  modular composition

$$\Longrightarrow \text{Cost: } O(\mathsf{C}(\delta))$$

Changing representation: general case

1. $\mathbf{d} \in \mathbb{N}^s$, $\mathbf{T} = (T_1, \ldots, T_s)$ in $\mathbb{K}[\mathbf{Y}]$, $\mathrm{car}(\mathbb{K}) \geq \delta^2$ or $\mathrm{car}(\mathbb{K}) = 0$

   - $\langle T_1, T_2 \rangle$ radical ideal ? *gcd computation*
   - Yes ? compute a 2-mixed representation $\mathscr{M}$ of $\mathbf{T}$

     trace computations: power projection + modular compositions

     $$\Longrightarrow O(s\,\mathsf{C}(\delta))$$
   - isomorphism computations: *modular compositions*

     $$\Longrightarrow O(\mathsf{C}(\delta))$$

2. "Repeat" $s-1$ times: $O(s^2\,\mathsf{C}(\delta))$

Operations modulo $\langle T \rangle$

1. Case $\mathbb{K} = \mathbb{F}_q$: $q \geq \delta \Rightarrow q' = q$; $q < \delta \Rightarrow$ extension field
2. $\mathscr{U} = (P, \mathbf{U}, \mu)$ primitive representation of $\mathbf{T}$: $O(s^2 \mathsf{C}(\delta))$
3. Operations in $\mathbb{K}[Y]/\langle P \rangle$.
   - Multiplication: $\delta \operatorname{plog}(\delta)$
   - Inversion: *extended gcd* $\delta \operatorname{plog}(\delta)$
   - Norm: *resultant* $\delta \operatorname{plog}(\delta)$
   - Modular composition: $m \leq 2$ $O(\delta^{(\omega+1)/2})$
     $\delta^{1+\varepsilon} \log(q') \operatorname{plog}_\varepsilon(\log(q'))$
   - Power projection: *transposed algorithm* $O(\delta^{(\omega+1)/2})$
     $\delta^{1+\varepsilon} \log(q') \operatorname{plog}_\varepsilon(\log(q'))$

Equiprojetable decomposition / change of order

- Strategy:
  1. Compute a univariate representation $\mathscr{U} = (P, \mathbf{U}, \mu)$
  2. Bivariate case: $O(\mathsf{C}(\delta)\log(\delta))$
     - $\mu' = \mu'_1 Y_1 + \cdots + \mu'_{s-1} Y_{s-1}$ primitive elt ($s-1$ first variables).

       Inverse modular composition (traces ; power projections)
     - Compute its characteristic polynomial: $\chi_{\mu'} = C_1^{r_1} \cdots C_n^{r_n}$

       Trace computations $\rightarrow$ power projection
     - Compute $\gcd(C_i(\mu'_1 U_1 + \cdots + \mu'_{s-1} U_{s-1}), P)$, $1 \leq i \leq n$.

       Recursive computation following the decompotition tree of $\chi_{\mu'}$
  3. "Repeat" s times
- Total cost: $O(s\,\mathsf{C}(\delta)\log(\delta))$
- Remark: we assume $\mathrm{car}(\mathbb{K}) \geq \delta$

Maple bench: us versus RegularChains

d_i	δ	Us	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	Us	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	Us	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	Us	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	Us	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

$s = 6$

Equiprojetable decomposition $\Longrightarrow$ modular composition

- Hyp: $m = 1$ and $s \leq 2$; $\mathbf{T} = (T_1, T_2) \in \mathbb{K}[X_1, X_2]$ radical
- $\mathsf{E}(\mathsf{n}, \delta)$ = complexity of the equiprojetable decomposition
- $G \in R_{\mathbf{T}}$ and $F \in \mathbb{K}[\mathbf{Y}]$ given, $K = F(G) \in R_{\mathbf{T}}$?

$$\Longrightarrow 2\mathsf{E}(4, \delta) + \mathsf{O}\tilde{}(\delta)$$

- s arbitrary can be generalised in $2\mathsf{E}(\mathsf{s}+2, \delta) + \mathsf{O}\tilde{}(\delta)$
- Equiprojetable decomposition $\Longrightarrow$ power projection

Details

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

Details

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

- Let I generated by:

$$\left| \begin{array}{l} Z - F(Y) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

Details

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

- Let I generated by:

$$\left| \begin{array}{l} Z - F(Y) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

- I is actually generated by:

$$\mathbf{T}'' \left| \begin{array}{l} Z - K(X_1, X_2) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  (order $X_1 < X_2 < Y < Z$)

Details

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

$F_i = F \mod R_i$; order $Y < X_1 < X_2 < Z$.

- Let I generated by:

$$\left| \begin{array}{l} Z - F(Y) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

- I is actually generated by:

$$\mathbf{T}'' \left| \begin{array}{l} Z - K(X_1, X_2) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  (order $X_1 < X_2 < Y < Z$)

- But I is the intersection of the

$$\mathbf{V}^{(i)} \left| \begin{array}{l} Z - F_i(Y) \\ U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

Details: complexity

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

E(3, δ)

$F_i = F \mod R_i$; order $Y < X_1 < X_2 < Z$.

- Let I generated by:

$$\left| \begin{array}{l} Z - F(Y) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

- I is actually generated by:

$$\mathbf{T}'' \left| \begin{array}{l} Z - K(X_1, X_2) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

(order $X_1 < X_2 < Y < Z$)

- But I is the intersection of the

$$\mathbf{V}^{(i)} \left| \begin{array}{l} Z - F_i(Y) \\ U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

Details: complexity

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

$\mathsf{E}(3, \delta)$

$O(\mathsf{M}(\delta)\log(\delta))$

$F_i = F \mod R_i$; order $Y < X_1 < X_2 < Z$.

- Let I generated by:

$$\left| \begin{array}{l} Z - F(Y) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

- I is actually generated by:

$$\mathbf{T}'' \left| \begin{array}{l} Z - K(X_1, X_2) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

(order $X_1 < X_2 < Y < Z$)

- But I is the intersection of the

$$\mathbf{V}^{(i)} \left| \begin{array}{l} Z - F_i(Y) \\ U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

Details: complexity

- Let

$$\mathbf{T}' \left| \begin{array}{l} Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  with order $X_1 < X_2 < Y$

- Change of order $Y < X_1 < X_2$:

$$\mathbf{U}^{(i)} \left| \begin{array}{l} U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

$\mathsf{E}(3, \delta)$

$O(\mathsf{M}(\delta)\log(\delta))$

$F_i = F \mod R_i$; order $Y < X_1 < X_2 < Z$.

- Let I generated by:

$$\left| \begin{array}{l} Z - F(Y) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

- I is actually generated by:

$$\mathbf{T}'' \left| \begin{array}{l} Z - K(X_1, X_2) \\ Y - G(X_1, X_2) \\ T_2(X_1, X_2) \\ T_1(X_1) \end{array} \right.$$

  (order $X_1 < X_2 < Y < Z$)

- But I is the intersection of the

$$\mathbf{V}^{(i)} \left| \begin{array}{l} Z - F_i(Y) \\ U_{i,2}(Y, X_1, X_2) \\ U_{i,1}(Y, X_1) \\ R_i(Y) \end{array} \right.$$

$\mathsf{E}(4, \delta)$

Conclusion

- Complexity quasi-linear / sub-quadratic for:
  - multiplication, inversion, norm computation, modular composition and power projection,
  - change of order, equiprojetable decomposition.
- Interesting practical results
- Modular composition, power projection

  $\Updownarrow$

  Equiprojetable decomposition
- Open questions:
  - algebraic case: quasi-linear algorithm ?
  - boolean case: algorithm usable in practice ?
  - non radical ideals ?
  - adaptation to the differentiel case ?