

# Sur la factorisation des polynômes à deux variables

G. Lecerf

LAMA, UMR CNRS 8100

Université de Versailles

travail en commun avec

A. Bostan,    B. Salvy,    É. Schost,    B. Wiebelt  
(LAMA-STIX)    (INRIA)    (STIX)    (STIX)



## **Prologue**

- Décomposition en composantes irréductibles des solutions de systèmes algébriques (Kronecker).
- Factorisation des polynômes à plusieurs variables.

## Factorisation dans $K[x, y]$

Notations :  $K$  est un corps (commutatif).

Si  $F \in K[x, y]$ , on note  $F' = \frac{\partial F}{\partial y}$ .

Entrée :  $F \in K[x, y]$ .

Sortie : Facteurs irréductibles de  $F$ .

Hypothèses : 
$$\begin{cases} (i) \deg_y(F) = \deg(F) = d \\ (ii) \text{Res}_y(F', F)(0) \neq 0 \end{cases}$$

Algorithme : Remontée + Recombinaison

1. Factorisation dans  $K[[x]][y]/(x)$  ;
2. Remontée de la factorisation dans  $K[[x]][y]/(x^\sigma)$  ;
3. Recombinaison des facteurs.

► Si  $\text{Res}_y(F', F) \neq 0$ , ces hypothèses peuvent être satisfaites après un changement de variables linéaire générique.

## Bibliographie

- Complexités exponentielles :
  - Kronecker (1882) : substitution  $x \leftarrow x, y \leftarrow x^{d+1}$ .
  - Zassenhaus (1969), Musser (1973) : Remontée + Recombinaison.
- Complexités polynomiales :
  - Chistov & Grigoriev (1982).
  - Kaltofen (1982) : approximants algébriques,  $\mathcal{O}(d^{12})$ .
  - Lenstra (1982) : réduction de réseaux (LLL),  $\mathcal{O}(d^8)$ .
  - Noro & Yokoyama (2002) : bases de Gröbner,  $\mathcal{O}(d^6)$ .
  - Gao (2002) : recherche de formes différentielles exactes,  $\mathcal{O}(d^5)$ .
  - Belabas, van Hoeij, Klüners & Steel (2004, en préparation) : cadre plus général ( $\mathbb{Z}[x]$ , petite caractéristique...).
  - BOLESaScWi (ISSAC 2004) : dérivée logarithmique,  $\tilde{\mathcal{O}}(d^\omega)$ ,  
 $2 \leq \omega \leq 2,39$ .

## Améliorations de la méthode Remontée + Recombinaison

- ▶ À l'origine, la phase de recombinaison était exponentielle.
- ▶ Préférée en pratique aux méthodes polynomiales.
- **T. Sasaki *et al.* (1991, 1992, 1993)** *heuristiques* : ramènent la recombinaison à de l'algèbre linéaire sur une matrice  $\sigma^2 \times \mathcal{O}(d)$ .  
Conjecture :  $\sigma = d + 1$  suffit "presque tout le temps".
- **Gao & Lauder (2000)** : si  $K$  est fini, la complexité *moyenne* de la recombinaison est polynomiale en  $d$ .
- **Belabas, van Hoeij, Klüners & Steel (2004, en préparation)** :  
 $\sigma = d(d - 1) + 1$  suffit pour faire la recombinaison en temps polynomial.
- **BoLeSaScWi (Issac 2004)** :  $\sigma = 3d - 2$  suffit si la caractéristique de  $K$  est nulle ou au moins  $d(d - 1) + 1$ .

## Plan de l'exposé

$$\underbrace{\mathcal{O}(d^{\mathcal{O}(I)})}_{\text{Recombinaison}} + \underbrace{\mathcal{O}(II)d^2 \log(d)}_{\text{Remontée}}^{\mathcal{O}(1)}$$

**$\sigma = +\infty$  suffit**

**Théorème [Sasaki et al., 1992]** Soit  $F \in K[x, y]_d$ , soit  $F = F_1 \cdots F_r$  sa factorisation dans  $K[x, y]$  et soit  $F = \mathfrak{F}_1 \cdots \mathfrak{F}_s$  sa factorisation dans  $K[[x]][[y]]$ . Alors

$$\mathcal{L} = \left\{ (\ell_1, \dots, \ell_s) \in K^s \mid \sum_{i=1}^s \ell_i \frac{\mathfrak{F}'_i}{\mathfrak{F}_i} F \in K[x, y]_{d-1} \right\}$$

est un sous-espace vectoriel de  $K^s$  de dimension  $r$ . De plus, si

$F_i = \prod_{j=1}^s \mathfrak{F}_j^{\mu_{i,j}}$ , alors  $\{\mu_1, \dots, \mu_r\}$  est une base de  $\mathcal{L}$ .

But : Trouver  $\sigma < +\infty$  tel que le théorème reste juste en remplaçant  $\mathcal{L}$  par

$$\mathcal{L}_\sigma = \left\{ (\ell_1, \dots, \ell_s) \in K^s \mid \sum_{i=1}^s \ell_i \frac{\mathfrak{F}'_i}{\mathfrak{F}_i} F \in K[x, y]_{d-1} + (x^\sigma) K[[x]][[y]] \right\}$$

Lemme :  $\mathcal{L} = \langle \mu_1, \dots, \mu_r \rangle \subseteq \mathcal{L}_\sigma$ .

## Exemple

Soit  $F = y^3 - y + x^2 \in \mathbb{Q}[x, y]$ .

On a  $F(0, y) = y(y - 1)(y + 1)$ ; remontée en précision  $\sigma = d + 1 = 4$ :

$$\mathfrak{F}_1 \bmod x^\sigma = y - 1 + \frac{1}{2}x^2 + \mathcal{O}(x^4);$$

$$\mathfrak{F}_2 \bmod x^\sigma = y - x^2 + \mathcal{O}(x^4);$$

$$\mathfrak{F}_3 \bmod x^\sigma = y + 1 + \frac{1}{2}x^2 + \mathcal{O}(x^4).$$

Donc  $\sum_{i=1}^3 \ell_i \frac{\mathfrak{F}'_i}{\mathfrak{F}_i} F \bmod x^\sigma = \ell_1 \mathfrak{F}_2 \mathfrak{F}_3 + \ell_2 \mathfrak{F}_3 \mathfrak{F}_1 + \ell_3 \mathfrak{F}_1 \mathfrak{F}_2 \bmod x^\sigma =$   
 $(\ell_1 + \ell_2 + \ell_3)y^2 + (\ell_1 - \ell_3)y + (\ell_3 - \ell_1)x^2 - \ell_2 + (\ell_2 - \frac{\ell_1}{2} - \frac{\ell_3}{2})x^2y.$

$$\mathcal{L}_\sigma = \left\{ (\ell_1, \ell_2, \ell_3) \in \mathbb{Q}^3 \mid \ell_2 - \frac{\ell_1}{2} - \frac{\ell_3}{2} = 0 \right\} = \langle (1, 0, 2), (0, 1, -1) \rangle.$$

►  $\sigma = d + 1$  ne suffit pas pour lire la factorisation.

► En précision  $d + 2 = 5$ ,  $\mathcal{L}_5 = \langle (1, 1, 1) \rangle$ , donc  $F$  est irréductible.

**$\sigma = d(d-1) + 1$  suffit**

[Belabas et al., en préparation 2004]

Si  $F_1 = \mathfrak{F}_1 \cdots \mathfrak{F}_m$  et  $\sum_{i=1}^s \ell_i \frac{\mathfrak{F}'_i}{\mathfrak{F}_i} F = Q + \mathcal{O}(x^{d(d-1)+1})$  alors  $\ell_1 = \cdots = \ell_m$ .

Soit  $\varphi_j(x) \in \bar{K}[[x]]$  tel que  $\mathfrak{F}_j(x, \varphi_j(x)) = 0$ , alors

$$Q(x, \varphi_j) = \ell_j \frac{\mathfrak{F}'_j F}{\mathfrak{F}_j}(x, \varphi_j) + \mathcal{O}(x^\sigma) = \ell_j F'(x, \varphi_j) + \mathcal{O}(x^\sigma).$$

Pour tout  $j \in \{1, \dots, m\}$  :

1.  $\text{Res}_y(\ell_j F' - Q, \mathfrak{F}_j) \in \mathcal{O}(x^\sigma)$ .
2.  $\text{Res}_y(\ell_j F' - Q, F_1) = \prod_{i=1}^m \text{Res}_y(\ell_j F' - Q, \mathfrak{F}_i) \in \mathcal{O}(x^\sigma)$ .
3.  $\deg_x(\text{Res}_y(\ell_j F' - Q, F_1)) \leq d(d-1)$ .
4.  $F_1$  divise  $\ell_j F' - Q$ .

$$\sigma = 3d - 2 \text{ suffit si } \text{char}(K) = 0 \text{ ou} \\ \text{char}(K) \geq d(d-1) + 1$$

Soient  $\phi_1, \dots, \phi_d$  les racines de  $F$  dans  $\bar{K}[[x]][y]$ .

Il suffit :  $(\ell_j F' - Q)(x, \phi_j) = 0 \pmod{x^{d(d-1)+1}}$ .

Hypothèse :  $(\ell_j F' - Q)(x, \phi_j) = 0 \pmod{x^\sigma}$ .

- Il existe  $A \in K[x, y]_{3d-4}$  tel que  $(Q/F'(x, \phi_j))' = A/F'^3(x, \phi_j)$ .
- $A(x, \phi_j) = 0 \pmod{x^{\sigma-1}}$ .
- $F$  divise  $A$ , en particulier  $(Q/F')(x, \phi_j)$  est de dérivée nulle dans  $\bar{K}[[x]]$ , donc  $= \ell_j \pmod{x^{\text{char}(K)}}$  et aussi modulo  $x^\sigma$ .

## Exemple dû à van Hoeij

Soit  $p$  un nombre premier,  $F = y^{p+1} + x^{p+1} - 1 \in \mathbb{F}_{p^2}[x, y]$ .

- $F$  est irréductible dans  $\mathbb{F}_{p^2}[x, y]$ .
- $\mathcal{L}_{p(p+1)} \neq \mathcal{L}_{p(p+1)+1} = \langle (1, 1, \dots, 1) \rangle$ .

► Il est donc nécessaire de remonter en précision  $d(d-1) + 1$  dans cet exemple.

## Algorithme

1. Factoriser  $F(0, y)$ . On obtient  $\mathfrak{F}_1 \bmod x, \dots, \mathfrak{F}_s \bmod x$  ;
2. (Remontée) Calculer  $\mathfrak{F}_1 \bmod x^\sigma, \dots, \mathfrak{F}_s \bmod x^\sigma$  ;
3. (Recombinaison) Calculer une base échelonnée réduite  $\{\mu_1, \dots, \mu_r\}$  de  $\mathcal{L}_\sigma$  :
  - Construction du système linéaire,
  - Calcul de la forme échelon réduite.

Sortie : Retourner  $F_i = \prod_{j=1}^s \mathfrak{F}_j^{\mu_{i,j}} \bmod x^{d+1}$ , pour  $i$  de 1 à  $r$ .

## Analyses de complexités

$$\mathcal{L}_\sigma = \left\{ (\ell_1, \dots, \ell_s) \in K^s \mid \sum_{i=1}^s \ell_i \frac{\mathcal{F}'_i}{\mathcal{F}_i} F \in K[x, y]_{d-1} + (x^\sigma)K[[x]][[y]] \right\}$$

**Théorème [BoLeSaScWi04]** Soit  $K$  un corps de caractéristique zéro ou supérieure à  $d(d-1)$ . Soit  $F \in K[x, y]_d$  et soit  $\sigma = 3d-2$ . Alors

$$\mathcal{L}_\sigma = \mathcal{L}.$$

**Corollaire [BoLeSaScWi04]** Sous les hypothèses précédentes, l'étape de recombinaison est dominée par le calcul d'une forme échelon réduite d'une matrice de taille

- $3d^2 \times s$ , par un algorithme déterministe,
- $6d \times s$ , par un algorithme probabiliste.

## Algorithme probabiliste

$$\Lambda_\tau = \left\{ \ell_{1:s} \in K^s \mid \sum_{i=1}^s \ell_i \text{coeff} \left( \frac{\mathcal{F}'_i}{\mathcal{F}_i} F, x^j y^k \right) = 0, k \leq d-1, d \leq j+k \leq \tau-1 \right\}.$$

**Lemme**  $\pi(L_\tau) \subseteq \Lambda_\tau \subseteq \pi(L_{\tau-d+1})$ .

$$\Lambda_\tau^a = \left\{ \ell_{1:s} \in K^s \mid \sum_{i=1}^s \ell_i \text{coeff} \left( \frac{\mathcal{F}'_i F}{\mathcal{F}_i} (x, ax), x^j \right) = 0, d \leq j \leq \tau-1 \right\}.$$

**Lemme** Pour tout  $b \in K$ , il existe un polynôme non nul  $P_b \in K[z]$  de degré au plus  $(s-r)(d-1)$  tel que si  $P_b(a) \neq 0$  alors  $\Lambda_\tau = \Lambda_\tau^a \cap \Lambda_\tau^b$ .

## Détail des complexités de la recombinaison

Entrée :  $\mathfrak{F}_{1:s}$  à précision  $\mathcal{O}(x^\tau)$ .

On prend  $\tau = 4d - 3$ .

Substitution  $y \mapsto ax : \mathcal{O}(d^2)$ .

Construction du système :  $\mathcal{O}(dM(d))$ .

Forme échelon réduite :  $\mathcal{O}(d^w \log(d))$  [Storjohann, 2000].

Calcul des  $F_i : \mathcal{O}(dM(d))$ .

Sortie :  $F_1, \dots, F_r$ .

## En pratique...

Soit  $K$  un corps de caractéristique zéro ou supérieure à  $d$ .

Soit  $F \in K[x, y]_d$  et soit  $\sigma = d + 1$  ( $\tau = 2d$ ).

**Théorème [Sasaki et al. 1992, BoLeSaScWi04]** *Si la forme échelon réduite de  $\mathcal{L}_\sigma$  ne contient que des 0 et des 1, alors*

$$\mathcal{L}_\sigma = \mathcal{L}.$$

**Corollaire [BoLeSaScWi04]** La recombinaison est dominée par le calcul d'une forme échelon réduite d'une matrice de taille

- $1/2d^2 \times s$ , par un algorithme déterministe,
- $2d \times s$ , par un algorithme probabiliste.

$$F = S_n = \prod (y \pm \sqrt{x+1} \pm \dots \pm \sqrt{x+n}), K = \mathbb{Z}/754974721\mathbb{Z}.$$

## Déterministe

$n$	degré total	nouveau Hensel	ancien Hensel	construction système	forme échelon	taille matrice
7	128	1.72 s	4.48 s	3.19 s	0.86 s	64 × 8256
8	256	8.19 s	35.1 s	27.3 s	13.0 s	128 × 32896
9	512	38.2 s	168 s	234 s	198 s	256 × 131328
10	1024	177 s	786 s	2007 s	3108 s	512 × 524800

## Probabiliste

$n$	degré total	factorisation fibre	nouveau Hensel	construction système	forme échelon	taille matrice
7	128	0.13 s	3.04 s	0.13 s	0.02 s	64 × 256
8	256	0.37 s	15.4 s	0.57 s	0.18 s	128 × 512
9	512	1.11 s	73.2 s	2.56 s	1.55 s	256 × 1024
10	1024	3.68 s	348 s	11.4 s	12.1 s	512 × 2048
11	2048	13.4 s	1700 s	52.2 s	95.2 s	1024 × 4096

$$F(x, y) = S_n(x^2, y)S_n(y^2, x)$$

$n$	degré total	Maple 9	Magma 2.9-15	Asir	notre code
3	8	0.589 s	0.04 s	0.01 s	0.02 s
5	32	50 min	4.36 s	2.36 s	0.75 s
7	128	> 41 h	> 1 jour	> 41 h	17.7 s
9	512	erreur	> 4 jours	erreur	394 s

## Complexité de la remontée

Théorème. [BolesasCWi, ISSAC 2004]

À partir de  $\mathfrak{F}_1, \dots, \mathfrak{F}_s \bmod x$ , on peut calculer  $\mathfrak{F}_1, \dots, \mathfrak{F}_s \bmod x^\sigma$  en

$$4 \mathbf{M}(\sigma) \mathbf{M}(d) \log s + \mathcal{O}(\mathbf{M}(d)(\mathbf{M}(\sigma) + \log d))$$

opérations dans  $K$ .

Meilleur algorithme connu avant [Shoup, Lemme de Hensel + « diviser pour régner »] :

$$\frac{27}{2} \mathbf{M}(\sigma) \mathbf{M}(d) \log s + \mathcal{O}(\mathbf{M}(d)(\mathbf{M}(\sigma) + \log d))$$

opérations dans  $K$ .

## Remontée par Newton

Problème : Connaissant  $\mathfrak{F}_i \bmod x$ , déterminer  $\mathfrak{F}_i \bmod x^\sigma$ .

Algorithme à convergence quadratique : Soit  $\mathfrak{F}_i^{(\kappa)} = \mathfrak{F}_i \bmod x^\kappa$ , pour  $i = 1, \dots, s$ . Pour  $\kappa = 1, 2, 4, \dots$  et chaque  $i$ , calculer dans :

$$A_{i,\kappa}[Y] = K[[x]][[y]]/(\mathfrak{F}_i^{(\kappa)})$$

1.  $\Delta := F'^{(-1)}F(Y) \in (x^\kappa)$  ;
2.  $Y' := Y - \Delta(Y), F(Y') = 0 \bmod \mathcal{O}(x^{2\kappa})$  ;
3.  $\mathfrak{F}_i^{(\kappa)}(Y) = 0 = \mathfrak{F}_i^{(\kappa)}(Y' + \Delta(Y)) = \mathfrak{F}_i^{(\kappa)}(Y') + (\mathfrak{F}_i^{(\kappa)})'(Y')\Delta(Y') \bmod x^{2\kappa}$  ;
4.  $\delta(Y') = (\mathfrak{F}_i^{(\kappa)})'(Y')\Delta(Y') \in \mathcal{O}(x^\kappa), \delta(Y) - \delta(Y') \in (x^\kappa)$  ;
5.  $\mathfrak{F}_i^{(2\kappa)} = \mathfrak{F}_i^{(\kappa)} + \delta$ .

## Réduction modulaire simultanée

**Problème** : Soit  $R = K[[x]]/(x^k)$ ,  $r \in R[y]_{d-1}$  et  $\mathfrak{F}_i \in R[y]_{d_i-1}$ .  
Calculer  $r \bmod \mathfrak{F}_i$ .

**Algorithme rapide classique** : de type diviser-pour-régner, par divisions répétées par les noeuds de l'arbre des sous-produits.

**Complexité** :  $10 M(d) \log s + \mathcal{O}(M(d))$  opérations dans  $R$ .

**Nouvel algorithme** :  $2 M(d) \log s + \mathcal{O}(M(d))$  opérations dans  $R$ .

**Idée** : donner un algorithme pour le *problème transposé* et en déduire un de même complexité par *transposition de programme*.

**Raison pour l'accélération** : Division des polynômes remplacée par multiplication transposée (moins chère)!

## Réduction simultanée transposée

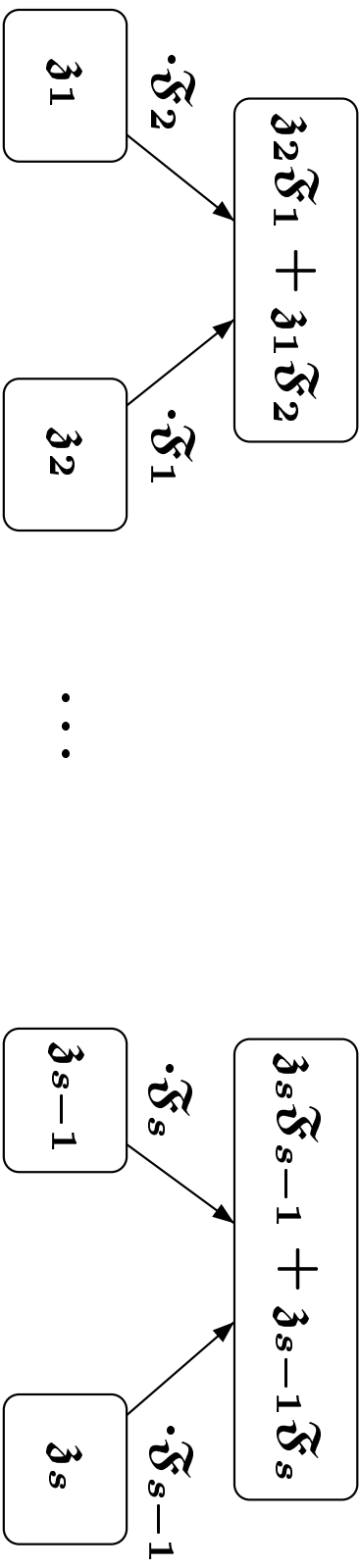
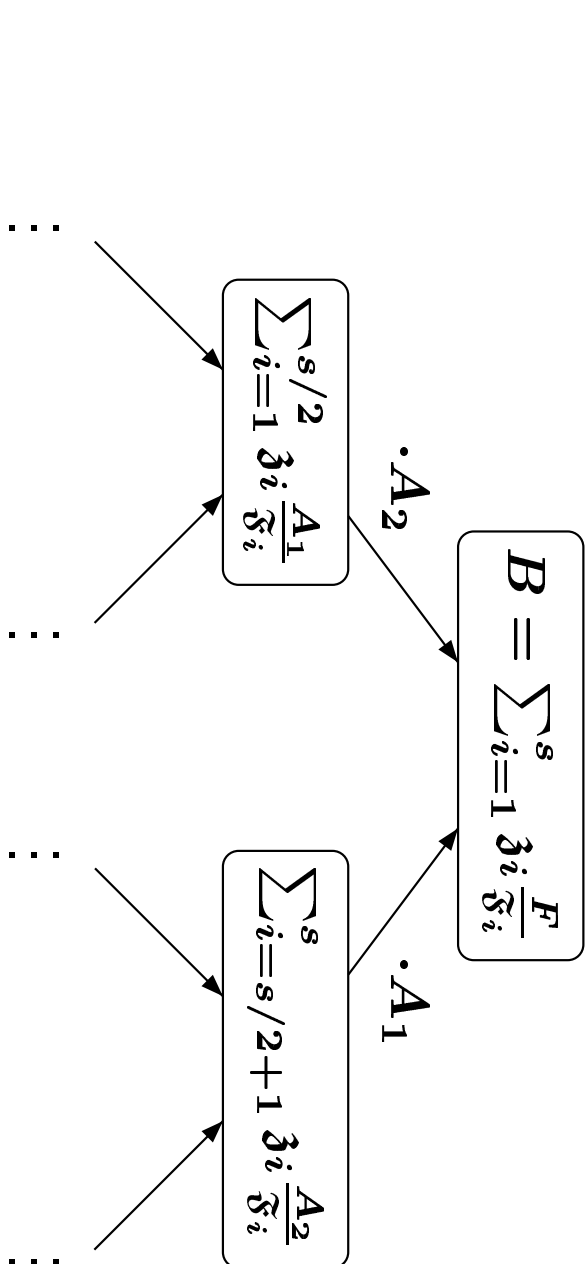
Lemme Le problème transposé de la réduction simultanée est :

Étant donné  $s$  polynômes  $c_j$  dans  $R[y]_{d_j-1}$ , calculer les  $d$  premiers coefficients du développement en série de Taylor dans  $R[[y]]$  de

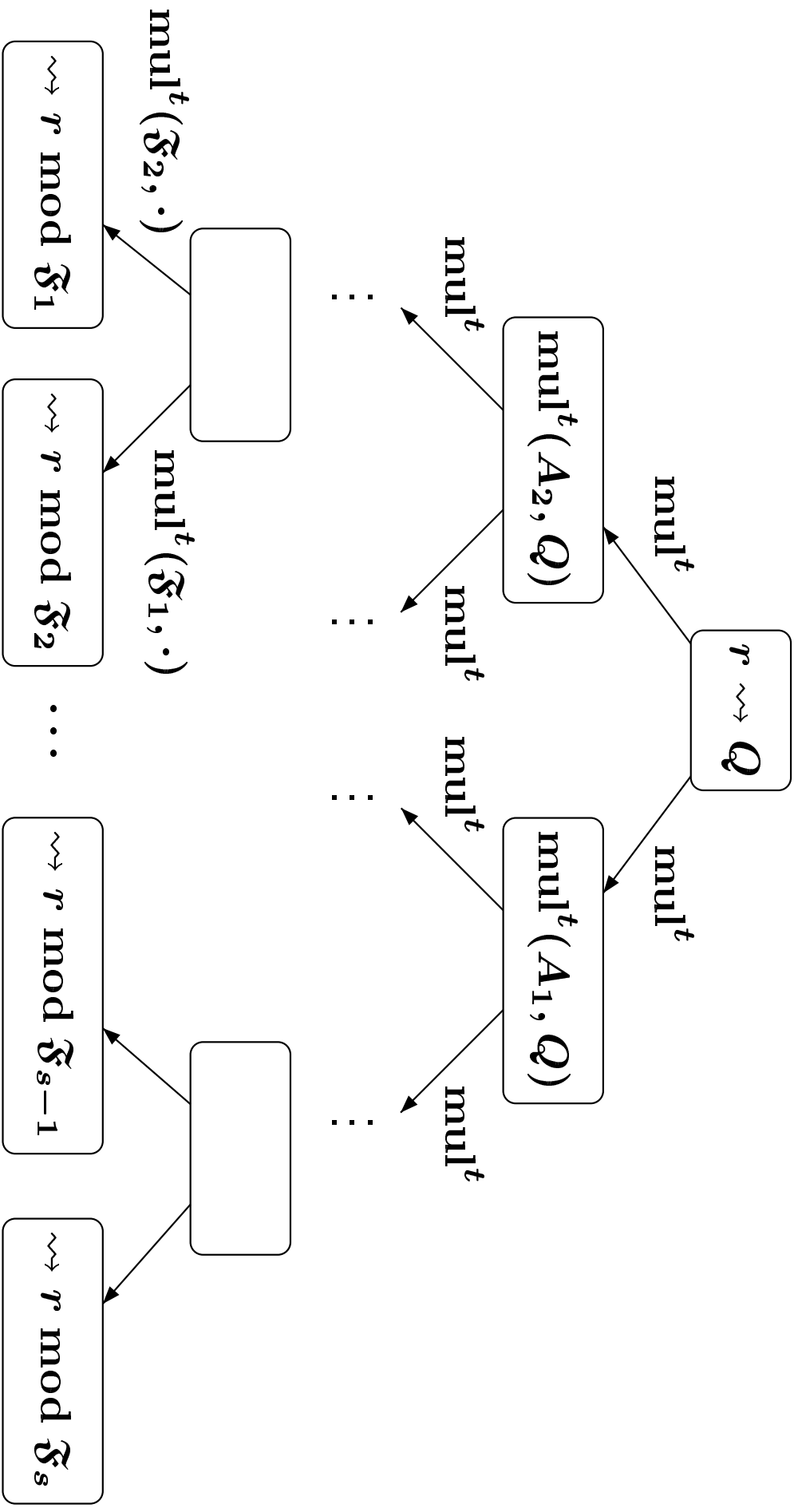
$$\sum_{j=1}^s \frac{u_j}{\text{rec}(d_j, \mathfrak{F}_j)} = \frac{1}{\text{rec}(d, F)} \text{rec} \left( d-1, \sum_{j=1}^s \mathfrak{z}_j \frac{F}{\mathfrak{F}_j} \right),$$

où

$$u_j = c_j \text{rec}(d_j, \mathfrak{F}_j) \bmod y^{d_j} \quad \text{et} \quad \mathfrak{z}_j = \text{rec}(d_j - 1, u_j).$$



Calcul de  $B = \sum_{i=1}^s z_j \frac{F}{z_j}$  par UpTree.



Réduction modulaire simultanée par TUPTree.

## Perspectives

- Quelle est la meilleure borne pour la précision de la remontée  $\sigma$  ?
- $\sigma \geq 2d - 1$  est nécessaire.
- Conjecture :  $\sigma = 2d + 1$  suffit.
- Améliorer les résultats pour les « petites » caractéristiques.