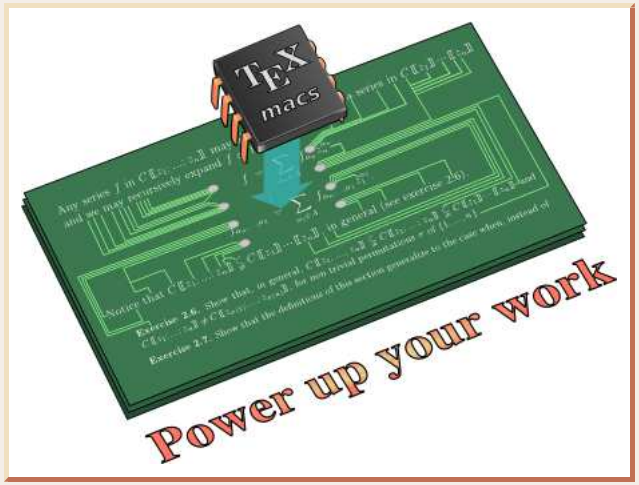
Complexité de l'arithméthique tordue

Joris van der Hoeven

CNRS, École polytechnique



INRIA, Rocquencourt, 2012

http://www.TEXMACS.org

Position des problèmes

Définitions

$\mathbb{K}$: corps effectif de caractéristique nulle, $\delta = x\,\partial/\partial x$
$\mathbb{K}[x,\delta]_{n,r} = \{L \in \mathbb{K}[x,\delta] : \deg_x L < n, \deg_\delta L < r\}$

Complexités fondamentales

- $\mathsf{M}(n) = \mathcal{O}(n \log n \log\log n)$: multiplication de deux polynômes dans $\mathbb{K}[x]_n$
- $\mathcal{O}(r^\omega)$, $\omega < 2.376$: multiplication de matrices dans $\mathbb{K}^{r\times r}$
- $\mathsf{SM}(n,r)$: multiplication de deux opérateurs dans $\mathbb{K}[x,\delta]_{n,r}$
- $\mathsf{SV}(n,r)$: application de $L \in \mathbb{K}[x,\delta]_{n,r}$ à $V \in \mathbb{K}[x]_n^r$
- $\mathsf{SF}(n,r)$: système fondamental pour $L \in \delta^r + K[x,\delta]_{n,r}$ à l'ordre $\mathcal{O}(x^n)$
- $\mathsf{SA}(n,r)$: annulateur pour $V \in \mathbb{K}[x]_n^r$ dans $\delta^r + K[x,\delta]_{n,r}$ à l'ordre $\mathcal{O}(x^n)$

Autres opérations

- Division exacte, division avec reste, division étendue
- Pgcd, ppcm et « pgcd/ppcm étendu »

Multiplication naïve

Entrées : $K, L \in \mathbb{K}[x,\delta]_{n,r}$
Sortie : $K\,L \in \mathbb{K}[x,\delta]_{2n-1,2r-1}$

- $n^2\,r^2$ produits $(K_{i,j}\,x^i\,\delta^j)\,(L_{i',j'}\,x^{i'}\,\delta^{j'}) = K_{i,j}\,L_{i',j'}\,x^{i+i'}\,(\delta+i')^j\,\delta^{j'}$
- Complexité : $\mathcal{O}(n^2\,r^3)$

Multiplication FFT

Entrées : $K, L \in \mathbb{K}[x,\delta]_{n,r}$
Sortie : $K\,L \in \mathbb{K}[x,\delta]_{2n-1,2r-1}$

Formule de Takayama (cas $r \leqslant n$, complexité en $\mathcal{O}(\mathsf{M}(n\,r)\,r)$)

$$\begin{aligned} K\,L &= \sum_{k<r} \frac{1}{k!} \left(\frac{\partial}{\partial\delta}\right)^k K * \left(\frac{x\,\partial}{\partial x}\right)^k L \\ K * L &= \sum_{i,j,i',j'} K_{i,j}\,L_{i',j'}\,x^{j+j'}\,\delta^{i+i'} \end{aligned}$$

Développement de L en x (cas $n \leqslant r$, complexité en $\mathcal{O}(\mathsf{M}(n\,r)\,n)$)

$$\begin{aligned} K(x,\delta)\,L(x,\delta) &= \sum_{k<n} K(x,\delta)\,(x^k\,L_k(\delta)) \\ &= \sum_{k<n} x^k\,K(x,\delta+k)\,L_k(\delta) \end{aligned}$$

Multiplication par évaluation-interpolation

Lemme. *Soit* $x^{;k} = (1, x, ..., x^{k-1}) \in \mathbb{K}[x]^k$ *pour chaque* k.
Alors $L \in \mathbb{K}[x, \delta]_{n,r}$ *est uniquement déterminé par* $L(x^{;r}) \in \mathbb{K}[x]^r_{n+r-1}$ *et*

1. *On peut calculer* $L(x^{;r})$ *à partir de* L *en temps* $\mathcal{O}(n\,\mathsf{M}(r)\log r)$.
2. *On peut calculer* L *à partir de* $L(x^{;r})$ *en temps* $\mathcal{O}(n\,\mathsf{M}(r)\log r)$.

Démonstration. Plus précisément : conversion entre L et

$$\mathrm{M}_L^{n+r-1,r} = \begin{pmatrix} L(1)_0 & \cdots & L(x^{r-1})_0 \\ \vdots & & \vdots \\ L(1)_{n+r-1} & \cdots & L(x^{r-1})_{n+r-1} \end{pmatrix}$$

Écrire $L = \sum_{i,j} L_{i,j}\, x^j\, \delta^i$ comme polynôme en x

$$L = x^{n-1} L_{n-1}(\delta) + \cdots + L_0(\delta)$$

Pour tout i et j, on a

$$L_i(\delta)(x^j) = x^j\, L_i(j).$$

Donc $\mathrm{M}_L^{n+r-1,r}$ est une matrice bande triangulaire inférieure, avec $\leqslant n$ bandes.
La i-ième bande sous diagonale se convertit par une évaluation/interpolation multi-point du *polynôme* $L_i \in \mathbb{K}[\delta]_r$ en les points $0, ..., r-1$. □

Résultats de complexité

Théorème. *On a :*

$$\mathsf{SM}(n,r) \;=\; \begin{cases} \mathcal{O}(n^{\omega-1}\,r + n\,\mathsf{M}(r)\log r) & si\ n \leqslant r \\ \mathcal{O}(n^2\,r^{\omega-2}) & si\ n \geqslant r \end{cases}$$

Démonstration. Soient $K, L \in \mathbb{K}[x,\delta]_{n,r}$. Alors

$$\mathrm{M}_{KL}^{2n+2r-3,2r-1} \;=\; \mathrm{M}_{K}^{2n+2r-3,n+2r-1}\,\mathrm{M}_{L}^{n+2r-2,2r-1}$$

Cas $n \geqslant r$: décomposition en $\lceil n/r \rceil$ blocs. □

Théorème. *Si $n \geqslant r$, alors*

$$\begin{aligned} \mathsf{SM}(n,r) &= \mathcal{O}(\mathsf{SV}(n,r) + n\,\mathsf{M}(r)\log r) \\ \mathsf{SV}(n,r) &= \mathcal{O}(\mathsf{SM}(n,r) + n\,\mathsf{M}(r)\log r) \end{aligned}$$

Récapitulatif multiplication

$n \preccurlyeq r$	$r \preccurlyeq n \preccurlyeq r^{4-\omega}$	$r^{4-\omega} \preccurlyeq n$
$\mathcal{O}(n^{\omega-1} r + n\,\mathsf{M}(r)\log r)$	$\mathcal{O}(n^2 r^{\omega-2})$	$\tilde{\mathcal{O}}(n r^2)$

Question (en cours)

Pour $n \succcurlyeq r$, est-ce que l'on a $\mathsf{SM}(n,r) = \tilde{\mathcal{O}}(n r^{\omega-1})$?

Désormais

$n \geqslant r$

Correspondence de Hilbert

Idéal principal d'opérateurs $(L) \longleftrightarrow$ Espace des solutions H_L

Espaces des solutions en des points non singuliers

$L = L_r \partial^r + \cdots + L_0$, $L_r(0) \neq 0$, $I \in \mathbb{K}^r \Longrightarrow$
Unique solution $f \in \mathbb{K}[[x]]$ de $Lf = 0$ avec $f^{(i)}(0) = I_i$ $(i = 0, ..., r-1)$

Système fondamental de solutions $H \in \mathbb{K}[[x]]^r$ avec

$$H_i \;=\; x^i + O(x^r)$$

Annulateur de $V \in \mathbb{K}[[x]]^r$

$\dim V = r \Longrightarrow$ $\exists!$ opérateur unitaire $L \in \delta^r + \mathbb{K}[[x]][\delta]_r$ avec $LV = 0$

$$L = \mathrm{ppcm}\left(\delta - \frac{\delta V_0}{V_0}, ..., \delta - \frac{\delta V_{r-1}}{V_{r-1}}\right)$$

Solutions locales

Théorème. *Soit $L \in \mathbb{K}[x,\delta]_{n,r}$ non singulier. Alors on peut calculer H à l'ordre $\mathcal{O}(x^n)$ en temps $\mathcal{O}(\mathsf{SM}(n,r)\log n)$.*

Démonstration. Puisque L est non singulier, on peut écrire

$$\begin{aligned} L &= \Delta_r(\delta) + x\,C_{r-1}\,\Delta_{r-1}(\delta) + \cdots + x^r\,C_0\,\Delta_0(\delta) && (C_i \in \mathbb{K}[x]) \\ \Delta_k(\delta) &= \delta\,(\delta-1)\cdots(\delta-k+1). \end{aligned}$$

On a $R = \Delta_r(\delta) - L \in x\,\mathbb{K}[x,\delta]_{n-1,r} : \mathbb{K}[[x]] \to x^r\,\mathbb{K}[[x]]$. On a la formule *recursive*

$$H = \begin{pmatrix} 1 \\ \vdots \\ x^{r-1} \end{pmatrix} + \Delta_r(\delta)^{-1}(R(H)).$$

L'opérateur $\Delta_r(\delta)^{-1}(R(H))$ opère terme par terme :

$$\Delta_r(\delta)^{-1}\left(\sum_{k\geqslant r} A_k\,x^k\right) = \sum_{k\geqslant r} \frac{A_k}{\Delta_r(k)}\,x^k.$$

H se calcule donc de façon détendue en temps $\mathcal{O}(\mathsf{SM}(n,r)\log n)$. □

Annulateurs

Théorème. *Supposons* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *avec*

$$p := v^{\max}(V) := \max\{v(Y) : Y \in \mathrm{Vect}(V) \setminus \{0\}\} < \infty.$$

Étant donnée H *à l'ordre* $\mathcal{O}(x^{n+p})$*, on l'unique annulateur* $L = \mathrm{ann}(H) \in \delta^r + \mathbb{K}[[x]][\delta]_r$ *de* H *à l'ordre* $\mathcal{O}(x^n)$ *se calcule en temps* $\mathcal{O}(\mathsf{SM}(n+p, r) \log r)$.

Calcul de $\mathrm{ann}_n(H) \in \delta^r + \mathbb{K}[x, \delta]_{n,r}$:

- Si $r = 1$, alors $\mathrm{ann}_n(H) := \delta - (\delta H_0 / H_0) \bmod x^n$.
- Sinon, soit $r = a + b$ avec $a := \lceil r/2 \rceil$.
- Calculer $A := \mathrm{ann}_n(H_0, ..., H_{a-1})$.
- Évaluer $I := (A(H_a), ..., A(H_{r-1})) \bmod x^n$.
- Caluler $B := \mathrm{ann}_n(I_0, ..., I_{b-1})$.
- Retourner $L = B\,A \bmod x^n$.

Positionnement en un point non singulier

Lemme.

1. *On peut trouver* $x_0 \in \mathbb{K}$ *où* $L \in \mathbb{K}[x, \partial]$ *est non singulier en temps* $\mathcal{O}(\mathsf{M}(n))$.
2. *Soit* $L \in \mathbb{K}[x, \delta]_{n,r}$. *On peut réécrire* $u^r\, L$ *comme opérateur dans* $\mathbb{K}[u, \delta_u]_{n+2r,r}$ *en temps* $\mathcal{O}(r\, \mathsf{M}(n) \log n)$, *où* $x = x_0 + u$.

Démonstration.

1. Le terme dominant $P = L_{\deg_\delta L}$ de L en x admet au plus n racines.
   On peut trouver une non-racine de P parmi $1, ..., 2^n$ en temps $\mathcal{O}(\mathsf{M}(n))$
2. Réécrire L comme opérateur dans $\mathbb{K}[x, \partial]_{n+r,r}$ en temps $\mathcal{O}(r\, \mathsf{M}(n) \log n)$.
   Réécrire L „ dans $\mathbb{K}[u, \partial_u]_{n+r,r}$ en temps $\mathcal{O}(r\, \mathsf{M}(n))$.
   Réécrire $u^r\, L$ „ dans $\mathbb{K}[u, \delta_u]_{n+2r,r}$ en temps $\mathcal{O}(r\, \mathsf{M}(n) \log n)$. □

Division exacte

Théorème. *Soient* $K, L \in \mathbb{K}[x,\delta]_{n,r}$ *tels que* $L = Q\,K$ *pour* $Q \in \mathbb{K}[x,\delta]$.
Alors on peut calculer Q *en temps* $O(\mathsf{SM}(n,r)\log n)$.

Algorithme

- Réduire au cas non singulier.
- Calculer système fondamental H avec $L(H) = 0$ à l'ordre $\mathcal{O}(x^{n+r})$.
- Évaluer $I = K(H)$ et calculer une $\mathbb{K}$-base G de $\mathrm{Vect}(I)$ à l'ordre $\mathcal{O}(x^{n+r})$.
- Calculer l'annulateur $\Omega = \mathrm{ann}(G)$ de G à l'ordre $\mathcal{O}(x^n)$.
- Retourner la troncature de $Q_s\,\Omega$ à l'ordre $\mathcal{O}(x^n)$, où $Q_s = L_{\deg_\delta L} / K_{\deg_\delta K}$.

Interpolation différentielle

Lemme. *Soit* $H=(H_0,\dots,H_{r-1})\in\mathbb{K}[[x]]^r$ *tel que* $p=v^{\max}(\mathrm{Vect}(H))+1<\infty$.
Pour $G\in(x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L\in\mathbb{K}[[x]][\delta]_r$ *avec* $L(H)=G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p,r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0=v(H_0)<\cdots<\alpha_{r-1}=v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned}\Phi\colon\mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r\\ \Phi(V_0,\dots,V_{r-1}) &= (x^{\alpha_0}V_0,\dots,x^{\alpha_{r-1}}V_{r-1});\end{aligned}$$

$$\begin{aligned}\Psi\colon\mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r\\ \Psi(K) &= \Phi^{-1}(K(\Phi(1)))\\ &= (x^{-\alpha_0}K(x^{\alpha_0}),\dots,x^{-\alpha_{r-1}}K(x^{\alpha_{r-1}})).\end{aligned}$$

Écrivant $K=\sum_{i,k}K_{i,k}\,x^k\,\delta^i$ et $\Psi(K)_{i,k}=(\Psi(K)_i)_k$, on a

$$\begin{pmatrix}\Psi(K)_{0,k}\\ \vdots\\ \Psi(K)_{r-1,k}\end{pmatrix}=\begin{pmatrix}1 & k+\alpha_0 & \cdots & (k+\alpha_0)^{r-1}\\ \vdots & \vdots & & \vdots\\ 1 & k+\alpha_{r-1} & \cdots & (k+\alpha_{r-1})^{r-1}\end{pmatrix}\begin{pmatrix}K_{0,k}\\ \vdots\\ K_{r-1,k}\end{pmatrix}.$$

Donc, Ψ et Ψ^{-1} opèrent terme par terme et se calculent à l'ordre $\mathcal{O}(x^n)$ et temps $\mathcal{O}(n\,\mathsf{M}(r)\log r)$.

.....

□

Lemme. *Soit* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *tel que* $p = v^{\max}(\mathrm{Vect}(H)) + 1 < \infty$.
Pour $G \in (x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L \in \mathbb{K}[[x]][\delta]_r$ *avec* $L(H) = G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0 = v(H_0) < \cdots < \alpha_{r-1} = v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned} \Phi\colon \mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r \\ \Phi(V_0, ..., V_{r-1}) &= (x^{\alpha_0} V_0, ..., x^{\alpha_{r-1}} V_{r-1}); \end{aligned}$$

$$\begin{aligned} \Psi\colon \mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r \\ \Psi(K) &= \Phi^{-1}(K(\Phi(1))) \\ &= (x^{-\alpha_0} K(x^{\alpha_0}), ..., x^{-\alpha_{r-1}} K(x^{\alpha_{r-1}})). \end{aligned}$$

Posant $H_i = x^{\alpha_i} + E_i$ avec $E_i = o(x^{\alpha_i})$, l'équation $L(H) = G$ se réécrit

$$L(H) = G$$

.....

□

Interpolation différentielle

Lemme. *Soit* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *tel que* $p = v^{\max}(\mathrm{Vect}(H)) + 1 < \infty$.
Pour $G \in (x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L \in \mathbb{K}[[x]][\delta]_r$ *avec* $L(H) = G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0 = v(H_0) < \cdots < \alpha_{r-1} = v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned} \Phi\colon \mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r \\ \Phi(V_0, ..., V_{r-1}) &= (x^{\alpha_0} V_0, ..., x^{\alpha_{r-1}} V_{r-1}); \end{aligned}$$

$$\begin{aligned} \Psi\colon \mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r \\ \Psi(K) &= \Phi^{-1}(K(\Phi(1))) \\ &= (x^{-\alpha_0} K(x^{\alpha_0}), ..., x^{-\alpha_{r-1}} K(x^{\alpha_{r-1}})). \end{aligned}$$

Posant $H_i = x^{\alpha_i} + E_i$ avec $E_i = o(x^{\alpha_i})$, l'équation $L(H) = G$ se réécrit

$$\begin{aligned} L(H) &= G \\ (L(x^{\alpha_0}), ..., L(x^{\alpha_{r-1}})) + L(E) &= G \end{aligned}$$

.....

□

Lemme. *Soit* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *tel que* $p = v^{\max}(\mathrm{Vect}(H)) + 1 < \infty$.
Pour $G \in (x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L \in \mathbb{K}[[x]][\delta]_r$ *avec* $L(H) = G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0 = v(H_0) < \cdots < \alpha_{r-1} = v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned} \Phi\colon \mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r \\ \Phi(V_0, ..., V_{r-1}) &= (x^{\alpha_0} V_0, ..., x^{\alpha_{r-1}} V_{r-1}); \end{aligned}$$

$$\begin{aligned} \Psi\colon \mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r \\ \Psi(K) &= \Phi^{-1}(K(\Phi(1))) \\ &= (x^{-\alpha_0} K(x^{\alpha_0}), ..., x^{-\alpha_{r-1}} K(x^{\alpha_{r-1}})). \end{aligned}$$

Posant $H_i = x^{\alpha_i} + E_i$ avec $E_i = o(x^{\alpha_i})$, l'équation $L(H) = G$ se réécrit

$$\begin{aligned} (L(x^{\alpha_0}), ..., L(x^{\alpha_{r-1}})) + L(E) &= G \\ \Phi(\Psi(L)) + L(E) &= G \end{aligned}$$

.....

□

Lemme. *Soit* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *tel que* $p = v^{\max}(\mathrm{Vect}(H)) + 1 < \infty$.
Pour $G \in (x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L \in \mathbb{K}[[x]][\delta]_r$ *avec* $L(H) = G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0 = v(H_0) < \cdots < \alpha_{r-1} = v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned} \Phi\colon \mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r \\ \Phi(V_0, ..., V_{r-1}) &= (x^{\alpha_0} V_0, ..., x^{\alpha_{r-1}} V_{r-1}); \end{aligned}$$

$$\begin{aligned} \Psi\colon \mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r \\ \Psi(K) &= \Phi^{-1}(K(\Phi(1))) \\ &= (x^{-\alpha_0} K(x^{\alpha_0}), ..., x^{-\alpha_{r-1}} K(x^{\alpha_{r-1}})). \end{aligned}$$

Posant $H_i = x^{\alpha_i} + E_i$ avec $E_i = o(x^{\alpha_i})$, l'équation $L(H) = G$ se réécrit

$$\begin{aligned} \Phi(\Psi(L)) + L(E) &= G \\ \Phi(\Psi(L)) &= G - L(E) \end{aligned}$$

.....

□

Lemme. *Soit* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *tel que* $p = v^{\max}(\mathrm{Vect}(H)) + 1 < \infty$.
Pour $G \in (x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L \in \mathbb{K}[[x]][\delta]_r$ *avec* $L(H) = G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0 = v(H_0) < \cdots < \alpha_{r-1} = v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned} \Phi\colon \mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r \\ \Phi(V_0, ..., V_{r-1}) &= (x^{\alpha_0} V_0, ..., x^{\alpha_{r-1}} V_{r-1}); \end{aligned}$$

$$\begin{aligned} \Psi\colon \mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r \\ \Psi(K) &= \Phi^{-1}(K(\Phi(1))) \\ &= (x^{-\alpha_0} K(x^{\alpha_0}), ..., x^{-\alpha_{r-1}} K(x^{\alpha_{r-1}})). \end{aligned}$$

Posant $H_i = x^{\alpha_i} + E_i$ avec $E_i = o(x^{\alpha_i})$, l'équation $L(H) = G$ se réécrit

$$\begin{aligned} \Phi(\Psi(L)) &= G - L(E) \\ L &= \Psi^{-1}(\Phi^{-1}(G - L(E))). \end{aligned}$$

.....

□

Lemme. *Soit* $H = (H_0, ..., H_{r-1}) \in \mathbb{K}[[x]]^r$ *tel que* $p = v^{\max}(\mathrm{Vect}(H)) + 1 < \infty$.
Pour $G \in (x^p\,\mathbb{K}[[x]])^r$, *il existe un unique* $L \in \mathbb{K}[[x]][\delta]_r$ *avec* $L(H) = G$,
et on peut calculer L *à l'ordre* $\mathcal{O}(x^n)$ *en temps* $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$.

Démonstration. Modulo changement de base : $\alpha_0 = v(H_0) < \cdots < \alpha_{r-1} = v(H_{r-1})$ et H_i unitaires. Soient

$$\begin{aligned} \Phi\colon \mathbb{K}[[x]]^r &\to \mathbb{K}[[x]]^r \\ \Phi(V_0, ..., V_{r-1}) &= (x^{\alpha_0} V_0, ..., x^{\alpha_{r-1}} V_{r-1}); \end{aligned}$$

$$\begin{aligned} \Psi\colon \mathbb{K}[[x]][\delta]_r &\to \mathbb{K}[[x]]^r \\ \Psi(K) &= \Phi^{-1}(K(\Phi(1))) \\ &= (x^{-\alpha_0} K(x^{\alpha_0}), ..., x^{-\alpha_{r-1}} K(x^{\alpha_{r-1}})). \end{aligned}$$

Posant $H_i = x^{\alpha_i} + E_i$ avec $E_i = o(x^{\alpha_i})$, l'équation $L(H) = G$ se réécrit

$$L = \Psi^{-1}(\Phi^{-1}(G - L(E))).$$

Cette équation est *récursive* ($x^{-\alpha_i} L(E_i) \prec L$, donc $\Phi^{-1}(L(E)) \prec L$).
$\rightsquigarrow$ Résolution détendue à l'ordre $\mathcal{O}(x^n)$ en temps $\mathcal{O}(\mathsf{SM}(n+p, r)\log n)$. □

Division avec reste (définitions)

Pour $A, B \in \mathbb{K}(x)[\delta]$, uniques $Q = \mathrm{quo}(A,B), R = \mathrm{rem}(A,B) \in \mathbb{K}(x)[\delta]$ avec

$$A \;=\; Q\,B + R \qquad (\deg_\delta R < \deg_\delta B)$$

Si $A, B \in \mathbb{K}[x,\delta]$ et $I = B_{\deg_\delta B}$, uniques $Q = \mathrm{pquo}(A,B)$, $R = \mathrm{prem}(A,B) \in \mathbb{K}[x,\delta]$ avec

$$I^{\deg_\delta A - \deg_\delta B + 1}\, A \;=\; Q\,B + R \qquad (\deg_\delta R < \deg_\delta B)$$

Soit $J = \mathrm{pgcd}(I,Q,R)$. En divisant la dernière relation par J, on obtient

$$C\,A \;=\; Q\,B + R \qquad \begin{array}{l}(\deg_\delta R < \deg_\delta B \\ \mathrm{pgcd}(C,Q,R) = 1)\end{array}$$

$Q = \mathrm{quo}^*(A,B)$: pseudo-quotient simplifié
$R = \mathrm{rem}^*(A,B)$: pseudo-reste simplifié

Division avec reste (algorithme)

Proposition. *Soient* $K, L \in \mathbb{K}[x,\delta]_{n,r}$ *avec* $n \geqslant r$ *et* $s = \deg_\delta K > 0$. *Soit*

$$J\,L \;=\; Q\,K + R$$

la pseudo-division de L *par* K *avec simplification. Si* $n' \geqslant n$ *vérifie* $A, Q, R \in \mathbb{K}[x,\delta]_{n',r}$, *alors* A, Q *et* R *se calculent en temps* $\mathcal{O}(\mathsf{SM}(n',r)\log n')$.

Algorithme (n' connu)

- Calculer système fondamental H pour $K(H) = 0$ à l'ordre $\mathcal{O}(x^{2n'+r})$.
- Calculer $G = L(H)$ avec $R(H) = J\,G$ à l'ordre $\mathcal{O}(x^{2n'+r})$.
- Interpoler $\Omega \in \mathbb{K}[[x]][\delta]_s$ avec $\Omega(H) = x^s\,G$ à l'ordre $\mathcal{O}(x^{2n'+r})$.
- On a $R = x^{-s}\,A\,\Omega$ et $x^{-s}\,\Omega$ est connu à l'ordre $\mathcal{O}(x^{2n'})$.
  $x^{-s}\,\Omega_0, \ldots, x^{-s}\,\Omega_{s-1}$ fractions rationnelles tronquées de degrés $<n'$.
  Reconstruction rationnelle de J et de R.
- Calculer Q avec $Q\,K = J\,L - R$ par l'algorithme de division exacte.

Pgcd, ppcm (définitions)

Pour $K, L \in \mathbb{K}(x)[\delta]$, il existe des uniques $\Gamma = \mathrm{pgcd}(K, L)$ et $\Lambda = \mathrm{ppcm}(K, L)$ unitaires dans $\mathbb{K}(x)[\delta]$ avec

$$\begin{aligned} \mathbb{K}(x)[\delta]\,\Gamma &= \mathbb{K}(x)[\delta]\,K + \mathbb{K}(x)[\delta]\,L \\ \mathbb{K}(x)[\delta]\,\Lambda &= \mathbb{K}(x)[\delta]\,K \cap \mathbb{K}(x)[\delta]\,L. \end{aligned}$$

Aussi uniques $A, B, C, D \in \mathbb{K}(x)[\delta]$ avec

$$\begin{pmatrix} \Gamma \\ 0 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} K \\ L \end{pmatrix},$$

$\deg_\delta A\,K, \deg_\delta B\,L < \deg_\delta \Lambda$ et $C\,K = -D\,L = \Lambda$. $\mathrm{Eucl}(K, L) = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$.

De même qu'au dessus : $\mathrm{pgcd}^*(K, L)$, $\mathrm{ppcm}^*(K, L)$ et $\mathrm{Eucl}^*(K, L)$.

Pgcd (calcul)

Théorème. *Soient* $K, L \in \mathbb{K}[x,\delta]_{n,r}$ *et* $n' \geqslant n$ *tels que* $\Lambda^* = \mathrm{lcm}^*(K,L) \in \mathbb{K}[x,\delta]_{n',r}$. *Si* K, L *et* $\mathrm{lcm}^*(K,L)$ *sont non singuliers, alors on peut calculer* Γ^* *en temps* $\mathcal{O}(\mathsf{SM}(n',r)\log n')$.

Algorithme

- Systèmes fondamentaux G, H pour $K(G)=0$, $L(H)=0$ à l'ordre $\mathcal{O}(x^{2n'+2r})$.
- Calculer base B de $V = \mathrm{Vect}(G) \cap \mathrm{Vect}(H)$ à l'ordre $\mathcal{O}(x^{2n'+2r})$.
- Calculer $\Omega = \mathrm{ann}(B) = \mathrm{pgcd}(K,L)$ à l'ordre $O(x^{2n'})$.
- Reconstruire $\Gamma^* = \mathrm{pgcd}^*(K,L)$ à partir de $\Omega \bmod x^{2n'}$.

Avertissement

$K = \mathrm{ann}(1,x)$, $L = \mathrm{ann}(\mathrm{e}^x, x)$ et $\mathrm{ppcm}(K,L) = \mathrm{ann}(1,x,\mathrm{e}^x)$ tous non singuliers, mais $\mathrm{pgcd}(K,L) = \mathrm{ann}(x) = \delta - 1$ est singulier.

Certification

Arrêt précoce

Si $\mathrm{Vect}(G) \cap \mathrm{Vect}(H) = \varnothing$ modulo $\mathcal{O}(x^{n'})$ pour un certain n',
alors $\mathrm{pgcd}^*(K, L) = 1$.

Matrices Euclidiennes

Calcul de $\mathrm{Eucl}^*(K, L)$ donne $\mathrm{pgcd}^*(K, L)$ et certification.

Pseudo-division de K et L par Γ^*

n' trop petit $\rightsquigarrow$ l'algorithme donne un $\widetilde{\Gamma^*}$ de degré éventuellement trop élevé
Mais $\widetilde{\Gamma^*}$ est correct si $\widetilde{\Gamma^*}$ pseudo-divise à la fois K et L

Bornes effectives

Borne pour $v(L(\phi))$ pour tout $\phi \in \mathrm{Ker}\, K \setminus \{0\}$ (K, L non singuliers) ?