Algorithmique efficace pour des opérations de base en calcul formel

Alin Bostan

Laboratoire STIX

Thèse de doctorat de l'École polytechnique

Directeurs : **Marc Giusti** et **Bruno Salvy**

9/12/2003

Cadre de mon travail

- Calcul formel : mathématiques effectives et complexité.
- Conception, analyse et mise en application d'algorithmes exacts.
- Complexité algébrique : bornes supérieures, étude comparative.
- Étalon : coût du produit des polynômes $\mathsf{M}(\mathbf{n})$.
- Expérimentation : validation par implantation.

Contributions

Algorithmes de meilleure complexité pour :

- *évaluation multipoint et interpolation* des polynômes
- *calculs* avec des nombres algébriques
- *résolution* des systèmes polynomiaux
- *manipulation* des suites récurrentes
- *opérations* sur des polynômes différentiels

Méthodologie

- **Principes algorithmiques classiques :**
  - *changement de représentation*
  - *diviser–pour–régner* $\rightsquigarrow$ remplace n par $\log(n)$
  - *pas de bébé / pas de géant* $\rightsquigarrow$ gains de $n^{1/2}$
- **Nouveau paradigme algorithmique :**
  - *transformation automatique des programmes*

Multiplication rapide des polynômes

On peut multiplier deux polynômes de degré au plus n en $\mathsf{M}(n) =$

- $O(n^2)$ par l'**algorithme naïf**
- $O\big(n^{\log_2(3)}\big) = O\big(n^{1.58}\big)$ par l'**algorithme de Karatsuba**
- $O\big(n \log(n) \log\log(n)\big)$ par la **transformée de Fourier rapide**

▶ Les constantes cachées dans les $O(\cdots)$ sont **cruciales** en pratique.
A. Schönhage : Do **not** waste a factor of 2 !

▶ Dans les meilleures implantations actuelles (Magma, NTL), l'algo. de Karatsuba est activé pour $\mathbf{n \approx 20}$ et la FFT pour $\mathbf{n \approx 100}$.

▶ Certaines applications pratiques nécessitent $\mathbf{n \approx 100000}$.
Pour ces degrés, les algorithmes rapides deviennent **indispensables** !

Opérateur de Newton formel

Soit $\varphi : k[[T]] \to k[[T]]$. Pour résoudre $\varphi(g) = 0$ dans $k[[T]]$, on applique la **méthode de la tangente de Newton** :

$$g_{i+1} = g_i - \frac{\varphi(g_i)}{\varphi'(g_i)}.$$

- Le nombre de coefficients **corrects** double à chaque itération.
- **Coût total** $=$ **2** $\times$ $\Big($ le coût de la **dernière** itération $\Big)$.

Th. [Brent 1975] *Inverse, logarithme et exponentielle des séries à précision* $\mathbf{n}$ *en* $\mathbf{O}(\mathsf{M}(\mathbf{n}))$.

Diverses représentations des polynômes

(1) **Monomiale :** $P = T^n + p_{n-1}T^{n-1} + \cdots + p_1 T + p_0$.

(2) **en évaluation sur** $\big(a_0, a_1, \ldots, a_n\big)$ **:**

$$\Big(P(a_0), P(a_1), \ldots, P(a_n)\Big).$$

(3) **de Newton, par sommes des puissances des racines :**

$$\Big(\sum_{P(\alpha)=0} 1, \quad \sum_{P(\alpha)=0} \alpha, \quad \ldots, \quad \sum_{P(\alpha)=0} \alpha^n\Big).$$

Th. [Borodin et al. 1974, Schönhage 1982] *Conversions :*

(1) $\longleftrightarrow$ (2) *en* $\mathbf{O}\big(\mathsf{M}(\mathbf{n})\log(\mathbf{n})\big)$ *par évaluation / interpolation.*

(1) $\longleftrightarrow$ (3) *en* $\mathbf{O}(\mathsf{M}(\mathbf{n}))$ *à base d'inversion ou exp. de séries.*

Sommes et produits composés

Th. [Bostan, Flajolet, Salvy, Schost]† $f, g \in k[T], D = \deg(f)\deg(g)$.

$\mathrm{car}(k)$	$f \otimes g = \prod_{\substack{f(\alpha)=0 \\ g(\beta)=0}} (T - \alpha\beta)$	$f \oplus g = \prod_{\substack{f(\alpha)=0 \\ g(\beta)=0}} \big(T - (\alpha+\beta)\big)$
$p = 0,\ p \geq D$	$O\big(\mathsf{M}(D)\big)$	$O\big(\mathsf{M}(D)\big)$
$0 < p < D$	$O\big(\mathsf{M}(D)\log(D)\big)$	$O\Big(\mathsf{M}\big(D^{1+\frac{1}{\log(p)}}\big)\log(D)\Big)$

- Idée : $f \oplus g$ et $f \otimes g$ plus simples en représentation de Newton.
- Algorithmes quasi-optimaux en la taille de la sortie.
- Gain de l'ordre $\sqrt{D}$ sur le calcul classique de résultants à 2 variables.

† Fast Computation with Two Algebraic Numbers, *RR INRIA, no. 4579, oct. 2002.*

Principe de Tellegen

Soit $\mathbf{M}$ *une matrice* $\mathsf{m} \times \mathsf{n}$ *et soit* $\mathbf{M^t}$ *sa transposée. Tout algorithme de complexité* L *calculant le produit matrice-vecteur* $\mathbf{Mv}$ *peut être transformé en un algorithme de complexité*

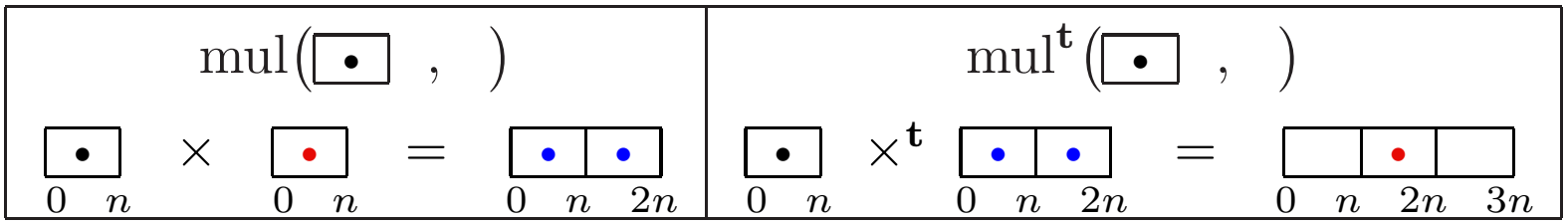
$$\mathsf{L} - \mathsf{n} + \mathsf{m}$$

qui calcule le produit matrice transposée-vecteur $\mathbf{M^t w}$.

- issu de la théorie des *réseaux électriques* : Tellegen (1952).
- introduit en *calcul formel* par Fiduccia et Hopcroft (1972).
- utilisé comme *théorème d'existence*, model des *circuits arithmétiques*.
- [Bostan, Lecerf, Schost] † : Version effective, transformation de code.

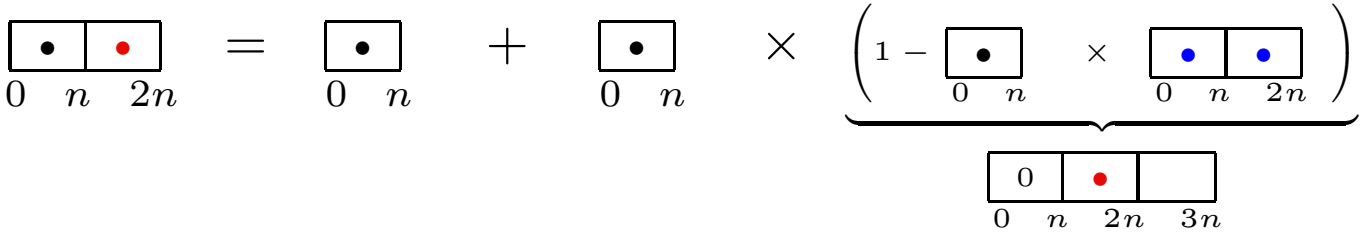
† Tellegen's Principle Into Practice, *Proceedings ISSAC 2003, 37–44.*

Multiplication transposée



Exemple : Itération de Newton pour l'inverse d'une série F.

$$\lceil 1/F \rceil^{2n} = \lceil 1/F \rceil^{n} + \lceil 1/F \rceil^{n} \times \left(1 - \lceil 1/F \rceil^{n} \times \lceil F \rceil^{2n}\right)$$



- **Produit médian** de [Hanrot, Quercia, Zimmerman 2002] !
- Principe de Tellegen : à tout algo. de *multiplication* en $\mathsf{M}(\mathbf{n})$ correspond un algo. de *multiplication transposée* en $\mathsf{M}(\mathbf{n}) + \mathbf{O}(\mathbf{n})$.

Algorithme de Karatsuba et son transposé

Input (c, d).

$c \leftarrow c$;

$d \leftarrow d$;

$e \leftarrow c + d + e$;

$U \leftarrow \mathrm{mul}(a, c)$;

$V \leftarrow \mathrm{mul}(b, d)$;

$W \leftarrow \mathrm{mul}(a + b, e)$;

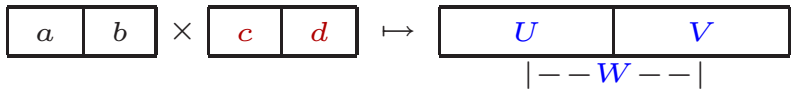
$U \leftarrow U$;

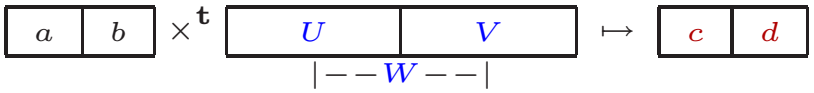
$V \leftarrow V$;

$W \leftarrow W - U - V$;

Output (U, V, W).

Algorithme de Karatsuba et son transposé





Input (c, d).

$c \leftarrow c$;

$d \leftarrow d$;

$e \leftarrow c + d + e$;

$U \leftarrow \mathrm{mul}(a, c)$;

$V \leftarrow \mathrm{mul}(b, d)$;

$W \leftarrow \mathrm{mul}(a + b, e)$;

$U \leftarrow U$;

$V \leftarrow V$;

$W \leftarrow W - U - V$;

Output (U, V, W).

Input (U, V, W).

$W \leftarrow W$;

$V \leftarrow V - W$;

$U \leftarrow U - W$;

$e \leftarrow \mathrm{mul}^{\mathbf{t}}(a + b, W)$;

$d \leftarrow \mathrm{mul}^{\mathbf{t}}(b, V)$;

$c \leftarrow \mathrm{mul}^{\mathbf{t}}(a, U)$;

$e \leftarrow e$;

$d \leftarrow d + e$;

$c \leftarrow c + e$;

Output (c, d).

Produits diamant

Produit diamant de Carlitz de $f, g \in k[T]$ par dessus $H \in k[X, Y]$

$$f \diamond_H g = \prod_{\substack{f(\alpha)=0 \\ g(\beta)=0}} \big(T - H(\alpha, \beta)\big)$$

Th. [Bostan, Flajolet, Salvy, Schost]† *Algorithme pour* $f \diamond_H g$ *en*

$$O\left(\sqrt{D}\left(\mathsf{M}(D) + D^{1.4}\right)\right).$$

- Gain d'ordre $\sqrt{D}$ sur le calcul classique de résultants à 3 variables.
- Idée : $f \diamond_H g$ est le polynôme caractéristique de H dans

$$Q = k[X, Y]/(f(X), g(Y))$$

- En représentation de Newton, $f \diamond_H g$ s'écrit

$$\left[\mathrm{trace}_Q(1), \mathrm{trace}_Q(H), \ldots, \mathrm{trace}_Q(H^D)\right].$$

---

† Fast Computation with Two Algebraic Numbers, *RR INRIA, no. 4579, oct. 2002.*

Projection des puissances = (composition modulaire)$^{\mathbf{t}}$.

projection des puissances			*composition modulaire*			
$\widehat{Q}$	$\to$	$k[[T]]_{\le D}$	$k[T]_{\le D}$	$\to$	Q	
ℓ	$\mapsto$	$\sum_{i=0}^{D} \ell(H^i)T^i + O(T^{D+1})$	p	$\mapsto$	$p(H)$	$\bmod (f,g)$

- [Brent & Kung 1978] : algo. pour la composition modulaire en

$$O\left(\sqrt{D}\left(\mathsf{M}(D) + D^{1.4}\right)\right).$$

- [Shoup, Kaltofen 1999] : Principe de Tellegen $\rightsquigarrow$ **existence** d'un algorithme pour la projection des puissances de même complexité.

- [Bostan, Flajolet, Salvy, Schost]† : Tellegen effectif $\rightsquigarrow$ permet d'**exhiber** un tel algorithme.

---

† Fast Computation with Two Algebraic Numbers, *RR INRIA, no. 4579, oct. 2002.*

Résolution des systèmes de polynômes

- $\mathcal{I}$ idéal de dimension zéro de $k[X_1, \ldots, X_n]$.
- Q l'algèbre quotient $k[X_1, \ldots, X_n]/\mathcal{I}$ de dimension D.

Th. [Bostan, Salvy, Schost]† : *Paramétrisation rationnelle*

$$\mathcal{V}(\mathcal{I}) \;=\; \left\{ \left(\frac{G_1(a)}{G(a)}, \ldots, \frac{G_n(a)}{G(a)}\right) \;\middle|\; P(a) = 0 \right\}$$

en $O(D^3)$ *à partir des* $\mathbf{M_{x_i}}$ *et en* $O(D^{2.5})$ *à partir de* $\mathbf{M_Q}$.

▶ algorithme RUR [Rouillier 1999] : $O(D^3)$, à partir de $\mathbf{M_Q}$.

---

† Fast Algorithms for Zero-Dimensional Polynomial Systems Using Duality, *Applicable Algebra in Engineering, Communication and Computing, 14 (4), 239–272, 2003.*

Évaluation multipoint et interpolation

Th. [† Bostan, Lecerf, Schost , † Bostan, Schost , † Bostan, Gaudry, Schost]

Question	cas général	progression arithmétique	progression géométrique
Évaluation	$\frac{3}{2}\,\mathsf{M}(n)\log(n)+\ldots$	$\frac{3}{4}\,\mathsf{M}(n)\log(n)+\ldots$	$2\,\mathsf{M}(n)+\ldots$
Interp.	$\frac{5}{2}\,\mathsf{M}(n)\log(n)+\ldots$	$\frac{3}{4}\,\mathsf{M}(n)\log(n)+\ldots$	$2\,\mathsf{M}(n)+\ldots$
Interp.-év.	$4\,\mathsf{M}(n)\log(n)+\ldots$	$\mathsf{M}(n)+\ldots$	$\mathsf{M}(n)+\ldots$

† Tellegen's Principle Into Practice, *Proceedings ISSAC 2003, 37–44.*

† Polynomial evaluation and interpolation on special sets of points, *preprint.*

† Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves, *Proceedings Fq7, 2003.*

Équivalence évaluation - interpolation

Th. [Bostan, Schost] †

Tout algorithme qui exécute **l'évaluation** *(resp.* **l'interpolation***) sur une famille distinguée de points, peut être transformé en un algorithme qui exécute* **l'interpolation** *(resp.* **l'évaluation***) sur la même famille de points, de* **même complexité** *à un nb. constant de multiplications près.*

Conséquences :

- $\mathsf{I}(n) \in O\big(\mathsf{E}(n) + \mathsf{M}(n)\big)$ *et* $\mathsf{E}(n) \in O\big(\mathsf{I}(n) + \mathsf{M}(n)\big)$.
- Évaluation et interpolation sur $u_i = a + bz^i + cz^{2i}$ en $O(\mathsf{M}(n))$.

† On the complexities of multipoint evaluation and interpolation, *preprint*.

Récurrences à coefficients polynomiaux

Th. [Bostan, Gaudry, Schost] † *Calcul du Nième terme d'une suite récurrente à coefficients polynomiaux en* :

$$\mathbf{O}\big(\mathsf{M}(\sqrt{\mathbf{N}})\big).$$

Corollaires *Même complexité pour calculer*

- *le coefficient de T^N dans $f(T)^{O(N)}$.*
- *$u_N = (a+1)(a+2)\cdots(a+N)$, où $a \in k$.*

▶ Record cryptographique : comptage de points de la Jacobienne d'une courbe hyperelliptique / corps de caractéristique $p \approx 2^{32} - 5$.

▶ Meilleur algorithme déterministe pour la factorisation des entiers.

---

† Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves, *Proceedings Fq7, 2003.*

Perspectives

- Moyen terme : étendre les techniques d'évaluation-interpolation au cadre différentiel linéaire multivarié.

- Court terme : approximants de Padé-Hermite *différentiels*.