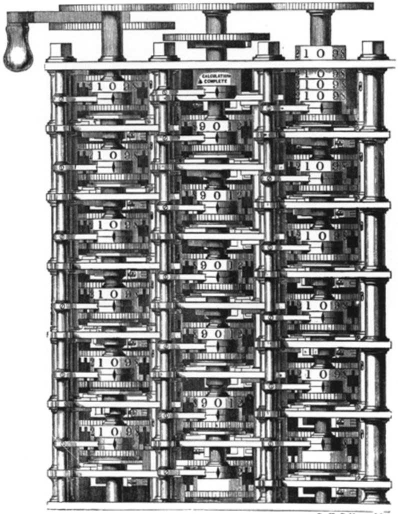


B. H. Babbage, del.

Évaluation numérique à grande précision de fonctions holonomes

Marc Mezzarobba
(stage sous la direction de Bruno Salvy)

Séminaire Algo, 15 octobre 2007

NumGfun

Objet

Évaluer à grande précision des fonctions spéciales.

Général	Toute la classe des fonctions holonomes
Garanti	Précision 10^{-p}
Efficace	Complexité quasi-optimale $O^{\sim}(p)$
Autonome	Entrée = équation différentielle + précision

Plan & références

N-ième terme de suites récurrentes

Prolongement analytique numérique

Bornes fines sur les fonctions holonomes

Remarques sur la constante du scindage binaire

- D.V. and G.V. Chudnovsky. Computer algebra in the service of mathematical physics and number theory. 1990.
- J. van der Hoeven. Fast evaluation of holonomic functions. 1999.

N-ième terme de suites récurrentes

- Suites holonomes
- Grands entiers
- Évaluation par scindage binaire

Prolongement analytique numérique

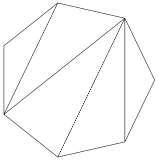
Bornes fines sur les fonctions holonomes

Remarques sur la constante du scindage binaire

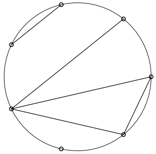
Exemples

Suites entières (combinatoire)

- Nombres de Catalan $C_n = \frac{1}{n+1}\binom{2n}{n}$
  - Mots de Dyck (mots de parenthèses) de longueur $2n$, triangulations du n-gone convexe...
  - $(n+2)C_{n+1} = (4n+2)C_n$, $C_0 = 1$



- Nombres de Motzkin
  - Cordes sans intersection sur n points...
  - $(n+3)M_{n+2} = 3nM_n + (2n+3)M_{n+1}$, $M_0 = 0, M_1 = M_2 = 1$



Exemples

Séries convergentes

- Calcul de π
  - Formule des Chudnovsky
    $$\frac{1}{\pi} = 12 \sum_{k=0}^{\infty} \frac{(-1)^k \,(6k)!\,(13591409 + 545140134k)}{(3k)!\,(k!)^3\, 640320^{3k+3/2}}$$
- Calcul de $\Gamma(z)$ pour $z \in \mathbb{Q}[i]$
  - $1 \leqslant \operatorname{Re} z \leqslant 2$
  - $$\begin{aligned}\Gamma(z) &= \int_0^{\infty} e^{-t} t^{z-1} \mathrm{d}t \\ &= k^z e^{-k} \sum_{n=0}^{\infty} \frac{1}{z^{\uparrow(n+1)}} k^n + \int_k^{\infty} e^{-t} t^{z-1} \mathrm{d}t\end{aligned}$$
  - Bornes sur l'intégrale et le reste de la série

(Formules *ad hoc*)

Suites holonomes

Définition

Une suite $(u_n)_{n\in\mathbb{N}}$ est holonome, ou P-récursive, si elle est solution d'une réurrence linéaire (homogène) à coefficients polynomiaux :

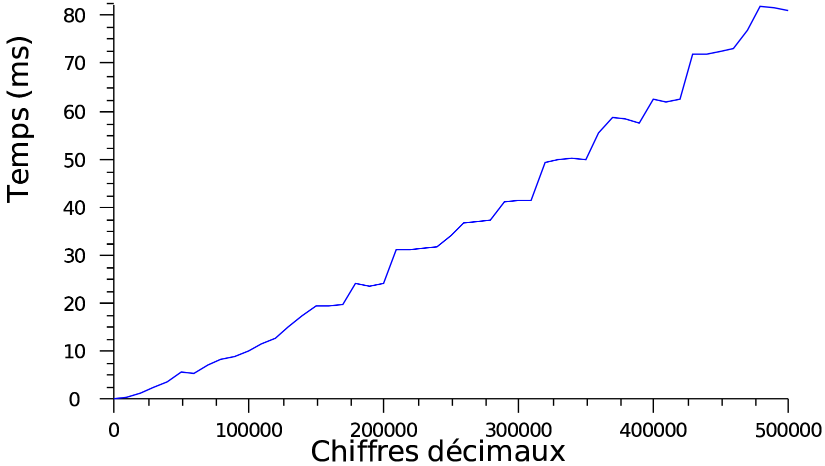
$$a_r(n)\, u_{n+s} + \cdots + a_1(n)\, u_{n+1} + a_0(n)\, u_n = 0, \qquad a_j \in \mathbb{Q}(i)[n].$$

Toutes les suites des exemples précédents sont holonomes.

Multiplication rapide de grands entiers

- Coût du produit équilibré d'entiers de n chiffres, en opérations binaires :
  - naïf : $\mathrm{M}(n) = \Theta(n^2)$
  - Karatsuba : $\mathrm{M}(n) = \Theta(n^{\log_2 3}) = O(n^{1,59})$
  - FFT : $\mathrm{M}(n) = n\,(\log n)\,2^{O(\log^* n)}$
- Algorithmes rapides pertinents en pratique (GMP)

Multiplication rapide de grands entiers



(GMP 4.2.2, Athlon XP 2.25 GHz, RAM PC3200)

Multiplication rapide de grands entiers

- Coût du produit équilibré d'entiers de n chiffres, en opérations binaires :
  - naïf : $\mathrm{M}(n) = \Theta(n^2)$
  - Karatsuba : $\mathrm{M}(n) = \Theta(n^{\log_2 3}) = O(n^{1,59})$
  - FFT : $\mathrm{M}(n) = n\,(\log n)\,2^{O(\log^* n)}$
- Algorithmes rapides pertinents en pratique (GMP)

Multiplication rapide de grands entiers

- Coût du produit équilibré d'entiers de n chiffres, en opérations binaires :
  - naïf : $\mathrm{M}(n) = \Theta(n^2)$
  - Karatsuba : $\mathrm{M}(n) = \Theta(n^{\log_2 3}) = O(n^{1,59})$
  - FFT : $\mathrm{M}(n) = n\,(\log n)\,2^{O(\log^* n)}$
- Algorithmes rapides pertinents en pratique (GMP)
- Réduire les autres opérations à $O(\log n)$ voire $O(1)$ multiplications
  - Division : $O(\mathrm{M}(n))$ (méthode de Newton)
  - Pgcd : $O(\mathrm{M}(n) \log n)$
    « C'est beaucoup » : attention aux manipulations de rationnels !

Écriture matricielle des récurrences

- $a_r(n)\,u_{n+s} + \cdots + a_1(n)\,u_{n+1} + a_0(n)\,u_n = 0$
- $$\begin{bmatrix} u_{n+1} \\ \vdots \\ u_{n+s-1} \\ u_{n+s} \end{bmatrix} = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \square & \square & \dots & \square \end{bmatrix} \begin{bmatrix} u_n \\ \vdots \\ u_{n+s-2} \\ u_{n+s-1} \end{bmatrix}$$

Écriture matricielle des récurrences

- $a_r(n)\,u_{n+s} + \cdots + a_1(n)\,u_{n+1} + a_0(n)\,u_n = 0$
- $$\begin{bmatrix} u_{n+1} \\ \vdots \\ u_{n+s-1} \\ u_{n+s} \end{bmatrix} = \frac{1}{q(n)} \underbrace{\begin{bmatrix} q & & & \\ & \ddots & & \\ & & & q \\ \square & \square & \dots & \square \end{bmatrix}}_{A(n)} \begin{bmatrix} u_n \\ \vdots \\ u_{n+s-2} \\ u_{n+s-1} \end{bmatrix}$$

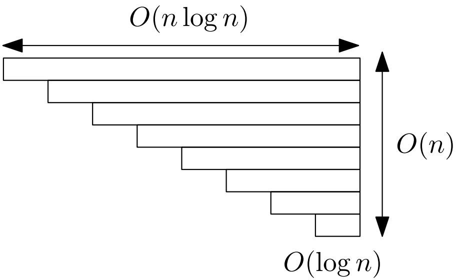
Écriture matricielle des récurrences

- $a_r(n)\, u_{n+s} + \cdots + a_1(n)\, u_{n+1} + a_0(n)\, u_n = 0$
- $$\begin{bmatrix} u_{n+1} \\ \vdots \\ u_{n+s-1} \\ u_{n+s} \end{bmatrix} = \frac{1}{q(n)} \underbrace{\begin{bmatrix} q & & & \\ & & \ddots & \\ & & & q \\ \square & \square & \dots & \square \end{bmatrix}}_{A(n)} \begin{bmatrix} u_n \\ \vdots \\ u_{n+s-2} \\ u_{n+s-1} \end{bmatrix}$$
- $$\begin{bmatrix} u_N \\ \vdots \\ u_{N+s-1} \end{bmatrix} = \frac{A(N-1)\cdots A(0)}{q(N-1)\cdots q(0)} \begin{bmatrix} u_0 \\ \vdots \\ u_{s-1} \end{bmatrix}$$

  « Factorielle de matrice de polynôme »

Scindage binaire

$$A(n-1)\cdots A(1)\cdot A(0)$$

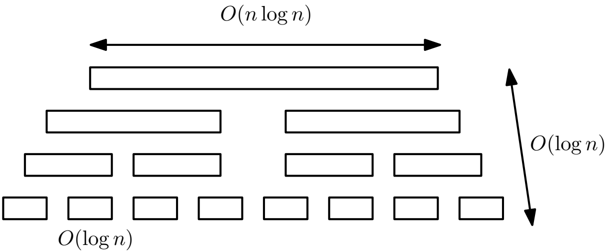


Produit naïf

$\Omega(n^2 \log n)$

Scindage binaire

$$
\begin{aligned}
&A(n-1)\cdots A(1)\cdot A(0)\\
&\qquad = \Big(A(n-1)\cdots A\big(\left\lfloor \tfrac{n}{2}\right\rfloor + 1\big)\Big)\cdot\Big(A\big(\left\lfloor \tfrac{n}{2}\right\rfloor\big)\cdots A(0)\Big)
\end{aligned}
$$



$$
\begin{aligned}
&\mathrm{M}(n \log n)\\
&+ 2\,\mathrm{M}\big(\tfrac{n}{2}\log n\big)\\
&+ \cdots\\
&+ n\,\mathrm{M}(\log n)\\
&= O\big(\mathrm{M}(n \log n)\log n\big)
\end{aligned}
$$

N-ième terme de suites récurrentes

Prolongement analytique numérique

- Évaluation dans le disque de convergence
- Prolongement analytique
- Bit burst

Bornes fines sur les fonctions holonomes

Remarques sur la constante du scindage binaire

Définition des fonctions holonomes

Définition

Une fonction $y(z) : \mathbb{C} \to \mathbb{C}$ est holonome (D-finie) si elle est solution d'une équation différentielle linéaire (homogène) à coefficients polynomiaux :

$$a_r(z)\, y^{(r)}(z) + \cdots + a_1(z)\, y'(z) + a_0(z)\, y(z) = 0, \qquad a_j \in \mathbb{Q}(i)[z].$$

Exemple

$$y(z) = \arctan(z) \quad \leftrightarrow \quad \begin{array}{l} (1+z^2)\, y''(z) + 2z\, y'(z) = 0 \\ y(0) = 0,\ y'(0) = 1 \end{array}$$

- Traiter toute cette classe

Définition des fonctions holonomes

Définition

Une fonction $y(z) : \mathbb{C} \to \mathbb{C}$ est holonome (D-finie) si elle est solution d'une équation différentielle linéaire (homogène) à coefficients polynomiaux :

$$a_r(z)\,y^{(r)}(z) + \cdots + a_1(z)\,y'(z) + a_0(z)\,y(z) = 0, \qquad a_j \in \mathbb{Q}(i)[z].$$

Exemple

$$\arctan(z) \quad = \quad \left\{ \begin{array}{l} (1+z^2)\,y''(z) + 2z\,y'(z) = 0 \\ y(0) = 0,\ y'(0) = 1 \end{array} \right\}$$

- Traiter toute cette classe
- Équation différentielle = structure de données

Singularités des fonctions holonomes

Théorème de Cauchy

Si $a_r(z_0) \neq 0$, l'équation différentielle

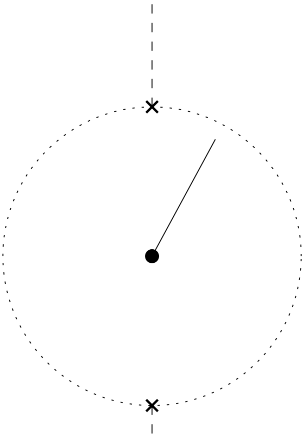
$$a_r(z)\, y^{(r)}(z) + \cdots + a_1(z)\, y'(z) + a_0(z)\, y(z) = 0$$

admet un espace de dimension r de solutions analytiques au voisinage de z_0.

- Singularités = zéros de a_r
- Le disque de convergence des solutions s'étend jusqu'à la plus proche singularité.

Évaluation dans le disque de convergence

Un exemple familier : arctan z



$$(1 + z^2)\, y''(z) + 2z\, y'(z) = 0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Évaluation dans le disque de convergence

Algorithme

$$\boxed{a_r(z)\,y^{(r)}(z) + \cdots + a_1(z)\,y'(z) + a_0(z)\,y(z) = 0 \qquad a_r(0) \neq 0}$$

$$y(z) = \sum_n y_n z^n \qquad S_n(z) = \sum_{k=0}^{n-1} y_n z^n$$

- Récurrence sur les coefficients
  - Coefficients indéterminés :
    $$\begin{aligned} y(z) &= \sum_{n=0}^{\infty} y_n z^n \\ \tfrac{d}{dz}\, y(z) &= \sum_n (n+1) y_{n+1} z^n \\ z \cdot y(z) &= \sum_n y_{n-1} z^n \end{aligned}$$
  - ➥ Les coefficients de Taylor d'une fonction holonome (en un point non singulier) forment une suite holonome.

$$b_s(n)\,y_{n+s} + \cdots + b_0(n)\,y_n = 0$$

Évaluation dans le disque de convergence

Algorithme

$$\boxed{a_r(z)\,y^{(r)}(z) + \cdots + a_1(z)\,y'(z) + a_0(z)\,y(z) = 0 \qquad a_r(0) \neq 0}$$

$$y(z) = \sum_n y_n z^n \qquad S_n(z) = \sum_{k=0}^{n-1} y_n z^n$$

- Récurrence sur les coefficients
  $b_s(n)\,y_{n+s} + \cdots + b_0(n)\,y_n = 0$

Évaluation dans le disque de convergence

Algorithme

$$\boxed{a_r(z)\,y^{(r)}(z)+\cdots+a_1(z)\,y'(z)+a_0(z)\,y(z)=0 \qquad a_r(0)\neq 0}$$

$$y(z)=\sum_n y_n z^n \qquad S_n(z)=\sum_{k=0}^{n-1} y_n z^n$$

- Récurrence sur les coefficients
  $b_s(n)\,y_{n+s}+\cdots+b_0(n)\,y_n=0$
- Récurrence sur les coefficients :
  $y_{n+s} \quad + \quad b_{n+s-1}(n)y_{n+s-1} \quad +\cdots+ \quad b_0(n)y_n \quad = 0$

Évaluation dans le disque de convergence

Algorithme

$$\boxed{a_r(z)\,y^{(r)}(z) + \cdots + a_1(z)\,y'(z) + a_0(z)\,y(z) = 0 \qquad a_r(0) \neq 0}$$

$$y(z) = \sum_n y_n z^n \qquad S_n(z) = \sum_{k=0}^{n-1} y_n z^n$$

- Récurrence sur les coefficients
  $b_s(n)\,y_{n+s} + \cdots + b_0(n)\,y_n = 0$
- Récurrence sur les termes :
  $y_{n+s}z^{n+s} + z b_{n+s-1}(n) y_{n+s-1} z^{n+s-1} + \cdots + z^s b_0(n) y_n z^n = 0$

Évaluation dans le disque de convergence

Algorithme

$$\boxed{a_r(z)\, y^{(r)}(z) + \cdots + a_1(z)\, y'(z) + a_0(z)\, y(z) = 0 \qquad a_r(0) \neq 0}$$

$$y(z) = \sum_n y_n z^n \qquad S_n(z) = \sum_{k=0}^{n-1} y_n z^n$$

- Récurrence sur les coefficients
  $b_s(n)\, y_{n+s} + \cdots + b_0(n)\, y_n = 0$
- Récurrence sur les termes :
  $y_{n+s} z^{n+s} + z b_{n+s-1}(n) y_{n+s-1} z^{n+s-1} + \cdots + z^s b_0(n) y_n z^n = 0$
- Récurrence sur les sommes partielles :
  $S_{n+1}(z) - S_n(z) = y_n\, z^n$

Évaluation dans le disque de convergence

Algorithme

$$\boxed{a_r(z)\,y^{(r)}(z) + \cdots + a_1(z)\,y'(z) + a_0(z)\,y(z) = 0 \qquad a_r(0) \neq 0}$$

$$y(z) = \textstyle\sum_n y_n z^n \qquad S_n(z) = \sum_{k=0}^{n-1} y_n z^n$$

- Récurrence sur les coefficients
  $b_s(n)\,y_{n+s} + \cdots + b_0(n)\,y_n = 0$
- Récurrence sur les termes :
  $y_{n+s}z^{n+s} + zb_{n+s-1}(n)y_{n+s-1}z^{n+s-1} + \cdots + z^s b_0(n)y_n z^n = 0$
- Récurrence sur les sommes partielles :
  $S_{n+1}(z) - S_n(z) = y_n\,z^n$
- Écriture matricielle et scindage binaire

Complexité

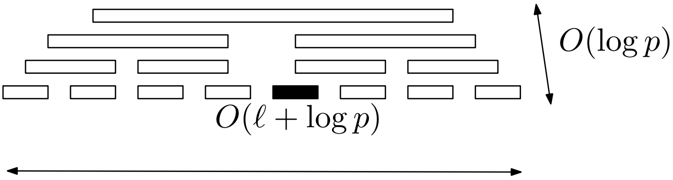
Vitesse de convergence des séries entières

- But : $\left|y(z) - \sum_{k=0}^{n-1} y_n z^n\right| \leqslant 10^{-p}$
- Si $|y_n| \leqslant \alpha^n \varphi(n)$, alors $\left|\sum_{k=n}^{\infty} y_k z^k\right| \leqslant |\alpha z|^n \overbrace{\sum_{k=0}^{\infty} \varphi(n+k)|\alpha z|^k}^{\psi(n)}$
- Rayon de convergence $\rho = 1/\limsup_{n\to\infty} |y_n|^{1/n}$

  ➥ meilleur $\alpha = 1/\rho$
- Nombre de termes : $n \simeq \dfrac{p}{\log(\rho/|z|)}$

Complexité

Scindage binaire

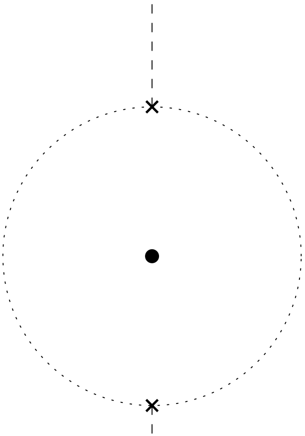


$$\# = \frac{1}{\log(\rho/|z|)} p$$

$$\boxed{\text{➥ Complexité : } O\left(\mathsf{M}\left(\frac{1}{\log(\rho/|z|)}\, p\, (\ell + \log p)\right) \log p\right)}$$

Prolongement analytique

Principe

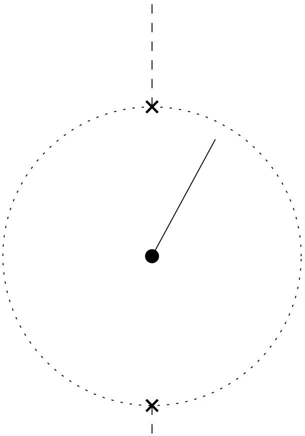


$$(1+z^2)\,y''(z) + 2z\,y'(z) = 0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Prolongement analytique

Principe

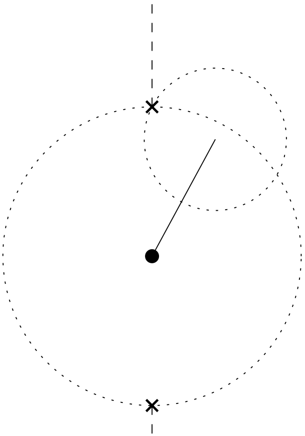


$$(1 + z^2)\, y''(z) + 2z\, y'(z) = 0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Prolongement analytique

Principe

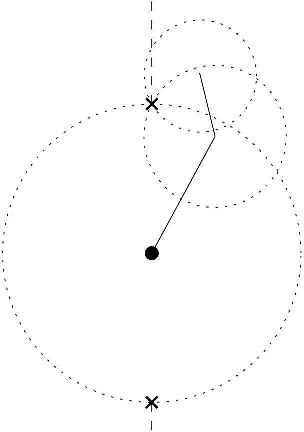


$$(1+z^2)\,y''(z)+2z\,y'(z)=0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Prolongement analytique

Principe

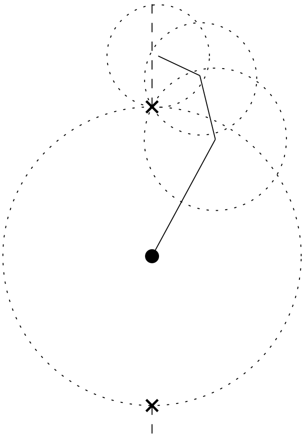


$$(1 + z^2)\, y''(z) + 2z\, y'(z) = 0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Prolongement analytique

Principe

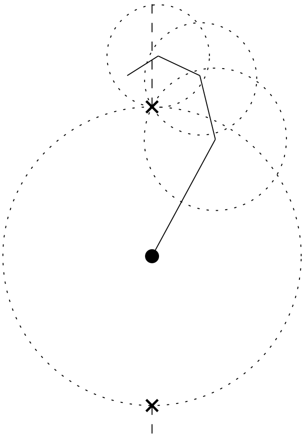


$$(1+z^2)\,y''(z) + 2z\,y'(z) = 0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Prolongement analytique

Principe



$$(1 + z^2)\, y''(z) + 2z\, y'(z) = 0$$

- Singularités : $\pm i$
- Coupes : $\pm[i, i\infty]$

Prolongement analytique

Exemples

- Évaluation à l'extrémité d'un chemin quelconque
  - Hors du disque de convergence
  - Détermination non standard
- Matrice de prolongement analytique
- Application : monodromie locale

Prolongement analytique effectif

- Base de solutions en z_0

$$y_{[z_0,j]}(z) = (z - z_0)^j + \square \cdot (z - z_0)^r + \cdots \qquad j \in [\![0, r-1]\!]$$

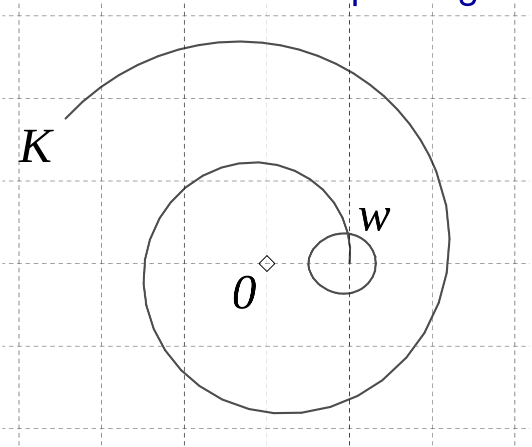
- Matrice de passage

$$M_{z_0 \to z_1} = \begin{bmatrix} y_{[z_0,0]}(z_1) & \cdots & y_{[z_0,r-1]}(z_1) \\ y'_{[z_0,0]}(z_1) & \cdots & y'_{[z_0,r-1]}(z_1) \\ \vdots & & \vdots \\ \frac{1}{(r-1)!} y^{(r-1)}_{[z_0,0]}(z_1) & \cdots & \frac{1}{(r-1)!} y^{(r-1)}_{[z_0,r-1]}(z_1) \end{bmatrix}$$

- Composition des matrices de passage
  = prolongement analytique

$$M_{z_0 \to z_1 \to \cdots \to z_m} = M_{z_{m-1} \to z_m} \cdots M_{z_1 \to z_2} \cdot M_{z_0 \to z_1}$$

Choix du chemin de prolongement analytique



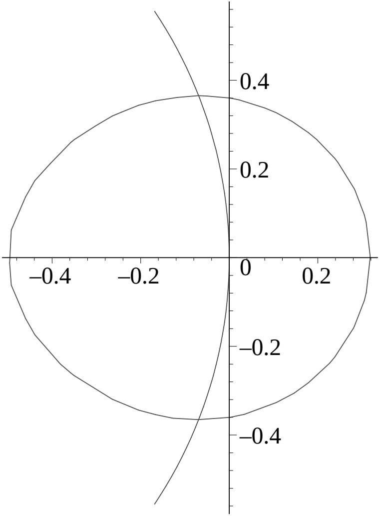
- Une singularité, en 0
- Chemin 1 $\rightsquigarrow K \in \mathbb{C}$
- Discrétisation : w^m
- Heuristiquement optimal

Spirale $e^{\omega t}$ $(\omega \in \mathbb{C})$

Ovale $|w-1|\log|w-1| + \mathrm{Re}\left(|w-1|\dfrac{w}{w-1}\log(w)\right) = 0$

Choix du chemin de prolongement analytique

Cas particuliers



- Radial sortant : $\times 1{,}32$
- Radial entrant : $\times 0{,}5$
- Un tour : 17 pas

D.V. and G.V. Chudnovsky.
Computer assisted number theory with applications. 1987.

J. van der Hoeven. Fast evaluation of holonomic functions. 1999.

Bit burst

- Calculer $f(0{,}a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12} \ldots a_n)$?
  (Résultat et argument à précision 10^{-n})
- Complexité $\Theta\big(\mathrm{M}(n\,(\ell + \log n))\log n\big)$ mauvaise si $\ell = \Theta(n)$

Idée

Prolongement analytique

$$z_0 = 0 \to z_1 = 0{,}a_1 \to z_2 = 0{,}a_1 a_2 a_3 \to z_3 = 0{,}a_1 a_2 a_3 a_4 a_5 a_6 a_7$$
$$\to z_4 = 0{,}a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12} a_{13} a_{14} a_{15} \to \ldots$$

- La diminution des longueurs des pas compense la croissance des tailles des sommets

N-ième terme de suites récurrentes

Prolongement analytique numérique

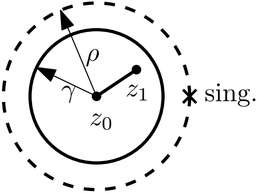
Bornes fines sur les fonctions holonomes

- Problème & résultats
- Utilisation des séries majorantes

Remarques sur la constante du scindage binaire

Bornes sur les fonctions holonomes

- Problème : calculer les nombre de termes nécessaire ?
- [ChCh90] Ordres de grandeur uniquement
- [vdH99] Bornes « données par la formule de Cauchy »



$$\left|\sum_{k=n}^{\infty} y_k z^k\right| \leqslant \left(\frac{|z|}{\gamma}\right)^n \varphi(n)$$

avec $\gamma < \rho$ $\quad (\leqslant +\infty\,!)$

- Idée : bornes dirigées par l'asymptotique

D.V. and G.V. Chudnovsky. Computer algebra in the service of mathematical physics and number theory. 1990.

J. van der Hoeven. Fast evaluation of holonomic functions. 1999.

Bornes sur les restes

Algorithme de calcul

Entrée $\{a_r y^{(r)} + \cdots + a_0 y = 0, y(0) = u_0, \ldots\}$

Sortie	$\left\lvert\sum_{k=n}^{\infty} y_k z^k\right\rvert \leqslant \cdots$	Nombre de termes
Cas général ($\rho < \infty$)	$A\left(\frac{\lvert z\rvert}{\rho}\right)^n \exp(Kn^\beta)$ $(0 \leqslant \beta < 1)$	$\frac{p}{\log(\rho/\lvert z\rvert)} + o(p)$
Point singulier régulier	$A\left(\frac{\lvert z\rvert}{\rho}\right)^n n^N$	$\frac{p}{\log(\rho/\lvert z\rvert)} + o(p)$
$\rho = \infty$	$\frac{A}{n!^{1/N}}$	$O\left(\frac{p}{\log p}\right)$

Résultats

Nombre de chiffres décimaux corrects

		$\arctan \frac{1}{2}$	$\arctan \frac{3}{4}$	$\frac{\cos z}{1-z}, z = \frac{1}{3}$	$(\alpha C + \beta S)(\frac{\pi}{3})$ $(*)$
100	M.	104	104	103	104
	vdH01	177	194	165	167
1000	M.	1004	1005	1004	1006
	vdH01	1716	1874	1591	1595

$(*)$ $\{(1-z^2)y''(z) - zy'(z) + 2(1-2z^2)y(z) = 0, y(0) = 1, y'(0) = 0\}$
(forme algébrique de l'équation de Mathieu) en $z = 1/2$.

		$\exp \frac{z}{1-z^2}, z = \frac{1}{3}$	$\operatorname{erf} \frac{z}{1-z}, z = \frac{1}{3}$	e^{-100}	$\mathrm{Ai}(4i+4)$
100	M.	107	123	102	238
	vdH01	152	146	316	357
1000	M.	1015	1081	1003	1764
	vdH01	1555	1501	> 4000	> 4000

J. van der Hoeven. Fast evaluation of holonomic functions near and in regular singularities.

Équations majorantes

Méthode de Cauchy-Kovalevskaïa

La série $f \in \mathbb{C}[[z]]$ est majorée par $g \in \mathbb{R}_+[[z]]$ (on note $f \trianglelefteq g$) lorsque $|f_n| \leqslant g_n$ pour tout n.

Proposition

Si

$$\begin{aligned} f^{(r)} &= a_{r-1} f^{(r-1)} + \cdots + a_0 f \\ g^{(r)} &= b_{r-1} g^{(r-1)} + \cdots + b_0 g \end{aligned} \qquad \text{avec } \forall j,\ a_j \trianglelefteq b_j$$

et

$$|f(0)| \leqslant g(0), \quad \ldots, \quad |f^{(r-1)}(0)| \leqslant g^{(r-1)}(0),$$

alors $f \trianglelefteq g$.

Singularité à distance finie

Choix de borne dirigé par l'asymptotique

- $y^{(r)} = -\frac{a_{r-1}}{a_r} y^{(r-1)} - \cdots - \frac{a_0}{a_r} y$
  (module de la première singularité $= 1/\alpha$)
- Comportement des solutions :
  $$|y_n| = \alpha^n \exp O(n^{1-\varepsilon})$$
- Série majorante du bon rayon de convergence :
  $$g(z) = A \exp \frac{M}{(1-\alpha z)^N}$$

➡ $g_n = O\left(\alpha^n \exp(K_{M,N}\, n^{1-\frac{1}{N+1}})\right)$

Singularité à distance finie

Équation majorante

- $$g^{(r)} = \frac{M}{(1-\alpha z)^N} \sum_{j=0}^{r-1} \binom{r-1}{j} N^{\uparrow(r-j)} \left(\frac{\alpha}{1-\alpha z}\right)^{r-j} g^{(j)}$$
  - Annule $g(z) = \exp \dfrac{M}{(1-\alpha z)^N}$
  - Bon ordre r pour majorer $y^{(r)} = -\dfrac{a_{r-1}}{a_r} y^{(r-1)} - \cdots - \dfrac{a_0}{a_r} y$
- Obtention de M et N :
  - $$\frac{a_j(z)}{a_r(z)} = \sum_k p_k(n) \mu_k^n z^k \trianglelefteq \frac{M_j}{(1-\alpha z)^{N_j}} \qquad (|\mu_k| \leqslant \alpha)$$
    (On résout la récurrence à coefficients constants.)
- Conclusion : $y(z) \trianglelefteq g(z)$

Autres cas

Majorants calculés

	irrégulier	régulier	$\rho = \infty$
$y(z) \trianglelefteq$	$A \exp \dfrac{M}{(1-\alpha z)^N}$		

Autres cas

- Point singulier régulier
  - Comportement des solutions : $|y_n| = \alpha^n n^{O(1)}$
  - Série majorante : $g(z) = A \dfrac{1}{(1-\alpha z)^N}$
    $(\Rightarrow g_n = O(\alpha^n n^{N-1}))$
  - Équation majorante (cf. critère de Fuchs) :
    $$y^{(r)} = \frac{M_{r-1}}{(1-\alpha z)^1} y^{(r-1)} + \cdots + \frac{M_1}{(1-\alpha z)^{r-1}} y' + \frac{M_0}{(1-\alpha z)^r} y$$

Majorants calculés

	irrégulier	régulier	$\rho = \infty$
$y(z) \trianglelefteq$	$A \exp \dfrac{M}{(1-\alpha z)^N}$	$\dfrac{A}{(1-\alpha z)^N}$	

Autres cas

- Singularité à l'infini (solutions fonctions entières)
  - Comportement des solutions : $|y_n| = O(1/n!^{\kappa})$
  - Série majorante : $g(z) = A \exp\left(M\left(z + \frac{z^2}{2} + \cdots + \frac{z^{N+1}}{N+1}\right)\right)$ $(\Rightarrow g_n = n^{O(1)}/n!^{1/N})$
  - Équation majorante : $y^{(r)} = M((1 + \cdots + z^N)\, y^{(r-1)} + \cdots + (1 + \cdots + z^{N-r+1})\, y)$

Majorants calculés

	irrégulier	régulier	$\rho = \infty$
$y(z) \trianglelefteq$	$A \exp \dfrac{M}{(1-\alpha z)^N}$	$\dfrac{A}{(1-\alpha z)^N}$	$A\, e^{M\left(z + \cdots + \frac{z^N}{N}\right)}$

Valeurs, restes, dérivées

- Série majorante pour f

$$\Downarrow \qquad f \trianglelefteq g \quad \Rightarrow \quad f' \trianglelefteq g'$$

- Séries majorantes pour f, f', f''...

$$\Downarrow \qquad f \trianglelefteq g \quad \Rightarrow \quad |f(z)| \leqslant g(|z|)$$

+ Méthode du col

- Bornes sur les valeurs
- Bornes sur les restes
- Bornes sur les coefficients

N-ième terme de suites récurrentes

Prolongement analytique numérique

Bornes fines sur les fonctions holonomes

Remarques sur la constante du scindage binaire

- Scindage binaire dans une algèbre « quelconque »
- Produit matriciel
- Dérouler une récurrence qui se factorise

Contextes d'utilisation du scindage binaire

- Entiers
- Rationnels ($\rightsquigarrow \mathbb{Z} \times \mathbb{Z}$)
- $\mathbb{Q}(i)$ ($\rightsquigarrow \mathbb{Z}[i] \times \mathbb{Z}$)
- Matrices d'entiers, rationnels...

Contextes d'utilisation du scindage binaire

- Entiers
- Rationnels ($\rightsquigarrow \mathbb{Z} \times \mathbb{Z}$)
- $\mathbb{Q}(i)$ ($\rightsquigarrow \mathbb{Z}[i] \times \mathbb{Z}$)
- Matrices d'entiers, rationnels...
- Corps de nombres $\mathbb{Q}(\alpha)$
- Séries tronquées $\mathbb{Z}[X]/\langle X^k \rangle$
- Matrices de séries tronquées à coefficients dans un corps de nombres
- ...

Contextes d'utilisation du scindage binaire

- Entiers
- Rationnels ($\rightsquigarrow \mathbb{Z} \times \mathbb{Z}$)
- $\mathbb{Q}(i)$ ($\rightsquigarrow \mathbb{Z}[i] \times \mathbb{Z}$)
- Matrices d'entiers, rationnels...
- Corps de nombres $\mathbb{Q}(\alpha)$
- Séries tronquées $\mathbb{Z}[X]/\langle X^k \rangle$
- Matrices de séries tronquées à coefficients dans un corps de nombres
- ...

↪ $\mathbb{Z}$-algèbres

Scindage binaire dans une algèbre « quelconque »

- A une $\mathbb{Z}$-algèbre (libre de type fini comme $\mathbb{Z}$-module), éléments représentés dans une base
- L = complexité quadratique de A
  = nombre de multiplications pour calculer $x \cdot y \in A$ par des opérations $+$ et $\times$ dans $\mathbb{Z}$
  - les mult. par des constantes ne comptent pas
  - les opérandes des mult. non constantes doivent être des formes linéaires $\lambda(a, b)$

Scindage binaire dans une algèbre « quelconque »

- A une $\mathbb{Z}$-algèbre (libre de type fini comme $\mathbb{Z}$-module), éléments représentés dans une base
- L = complexité quadratique de A

Proposition

Le calcul par scindage binaire d'un produit $x_1 \dots x_n$ d'éléments de A de hauteur (taille coef.) $\leqslant h$ prend au plus

$$\frac{L}{2}\,\mathrm{M}\Big((h+K)n\log_2 n\Big)(1+o_{n\to\infty}(1))$$

opérations binaires, pour un certain K.

Exemple

Gagner 20% dans $\mathbb{Q}(i)$

- Karatsuba :

$$(x+iy)(x'+iy') = (u-v)+i(w-u-v)$$

$$\text{où} \quad \begin{cases} u = xx' \\ v = yy' \\ w = (x+y)(x'+y') \end{cases}$$

3 + 1 (dénominateurs) = 4 mult. au lieu de 5

- Généralisation : produit dans $\mathbb{K}[X]/\langle Q\rangle$ en $2\deg Q - 1$ multiplications dans $\mathbb{K}$ (Toom-Cook)
(car $\mathbb{K} = 0$)

Produit matriciel

- Théorie : $O(s^\omega)$, où $\omega < 2{,}376$ (Coppersmith-Winograd)
- Gagne pour $s > 10^{50}$ ou 10^{100}...

- Petites matrices
- Grands entiers : chaque multiplication en moins se voit...
- Tirer parti de la commutativité

- (Question intéressante en soi :) combien de multiplications exactement pour multiplier deux matrices de taille s sur un anneau commutatif ?

Produit de petites matrices

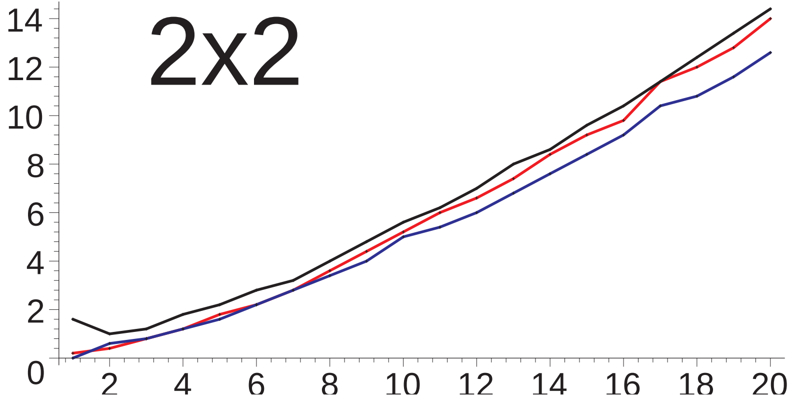
Taille	2	3	4	5	6	7	8	9	10
Naïf	8	27	64	125	216	343	512	729	1000
NCom	**7**	**23**	49	100	161	273	343	529	700
Com	**7**	**23**	**46**	**93**	**141**	**235**	**316**	**473**	**595**

Taille	11	12	13	14	15	16	17	18	19
Naïf	1331	1728	2197	2744	3375	4096	4913	5832	6859
NCom	992	1125	1580	1778	2300	2401	3218	3342	4369
Com	**831**	**987**	**1333**	**1561**	**2003**	**2212**	**2865**	**3231**	**3943**

- Strassen : 7 mult. (non com.) en taille 2×2
- Waksman : $n^2 \left\lceil \frac{n}{2} \right\rceil + (2n-1) \left\lfloor \frac{n}{2} \right\rfloor \simeq \frac{n^3}{2} + n^2 - \frac{n}{2}$ mult. com.

Produit matriciel en pratique (et en Maple)

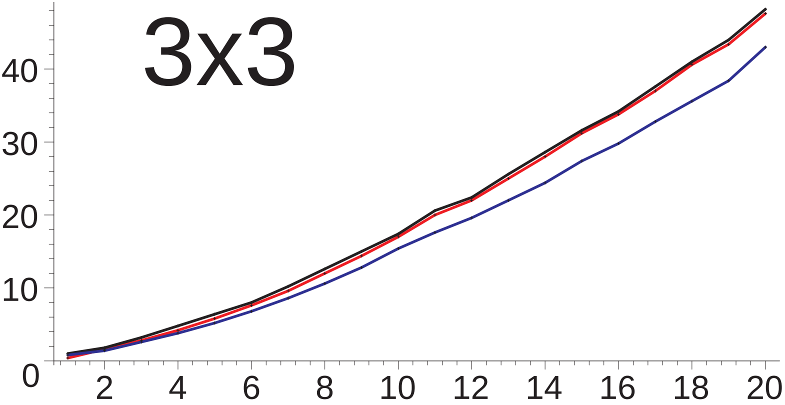
Matrices denses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

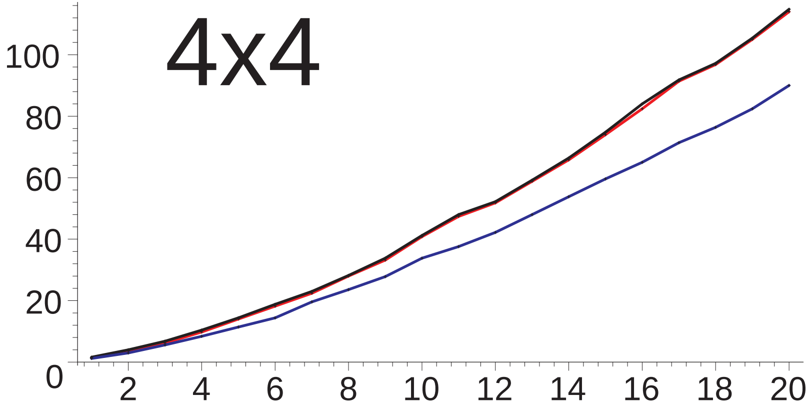
Matrices denses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

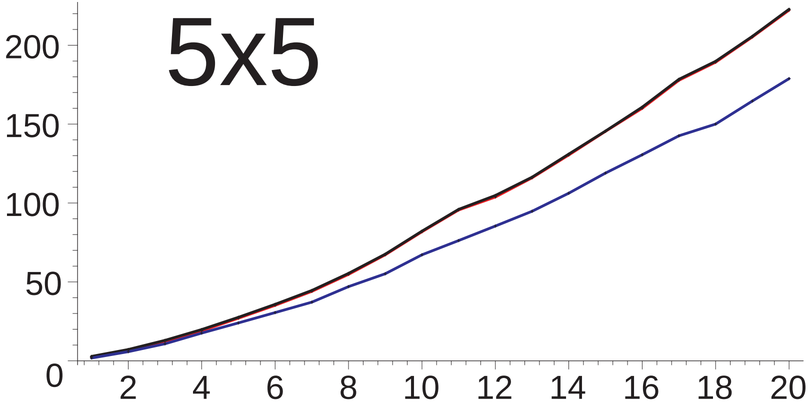
Matrices denses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

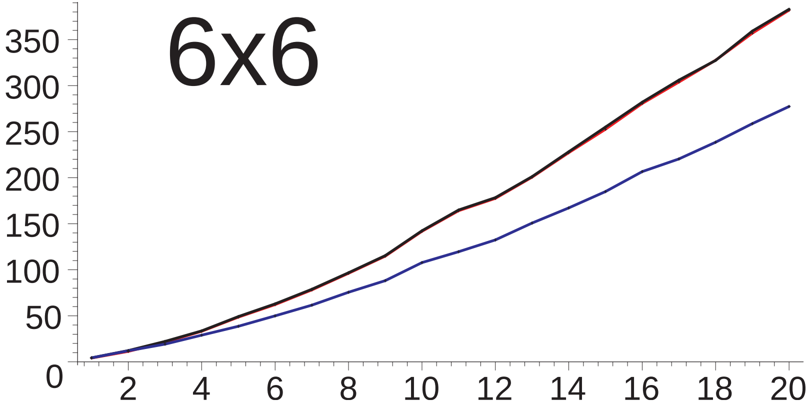
Matrices denses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

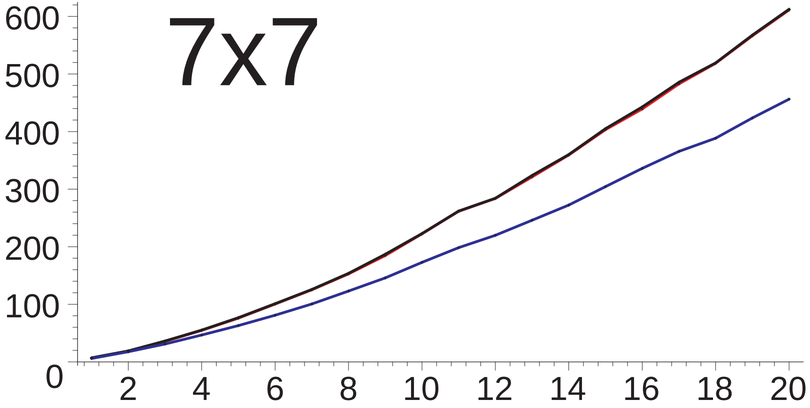
Matrices denses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

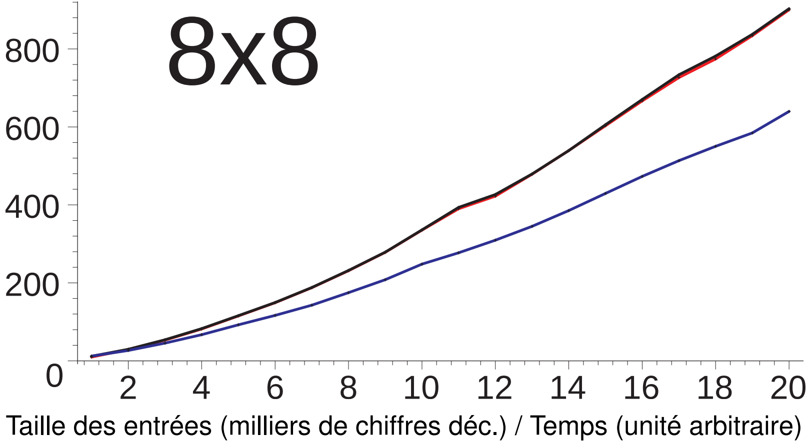
Matrices denses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

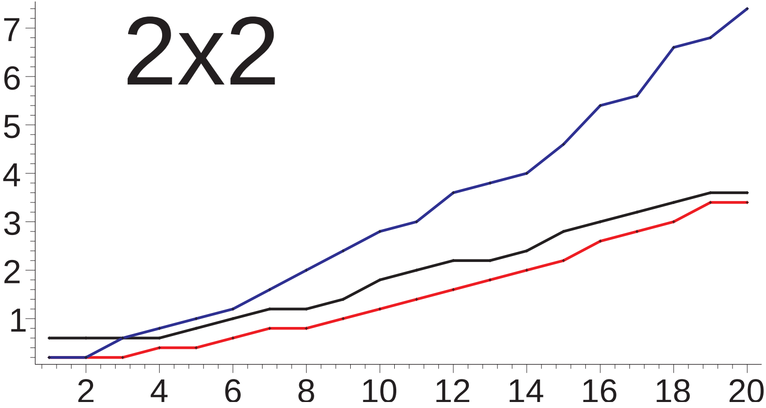
Produit matriciel en pratique (et en Maple)

Matrices denses



Produit matriciel en pratique (et en Maple)

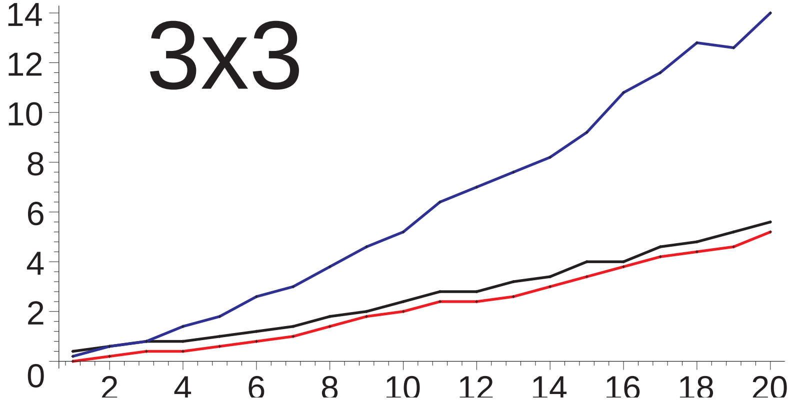
Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

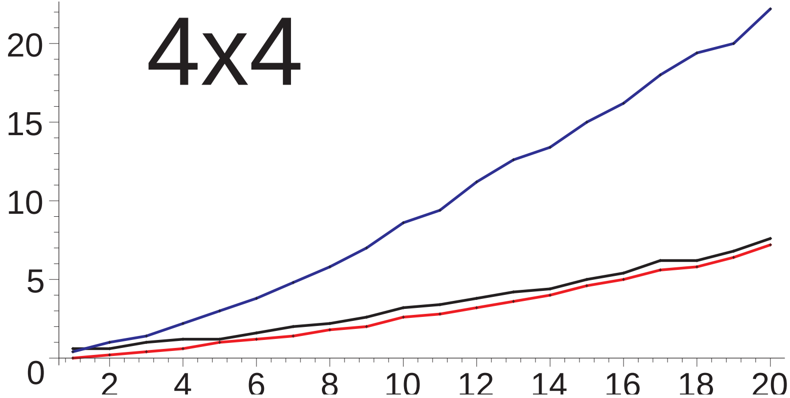
Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

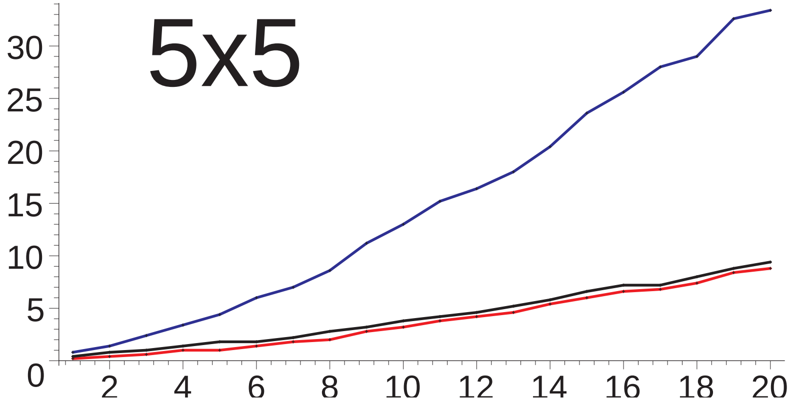
Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

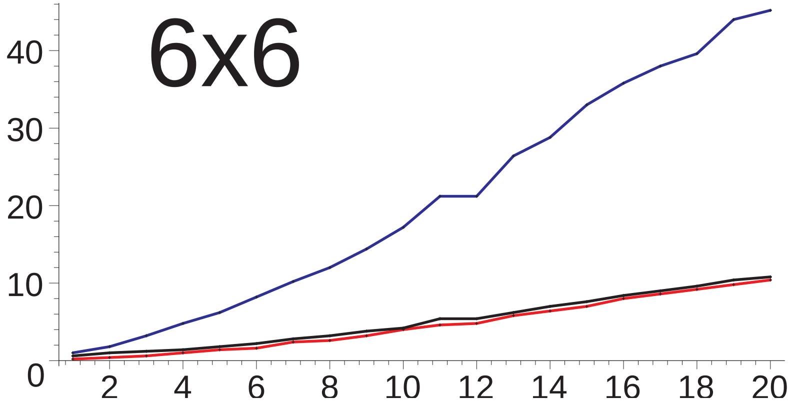
Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

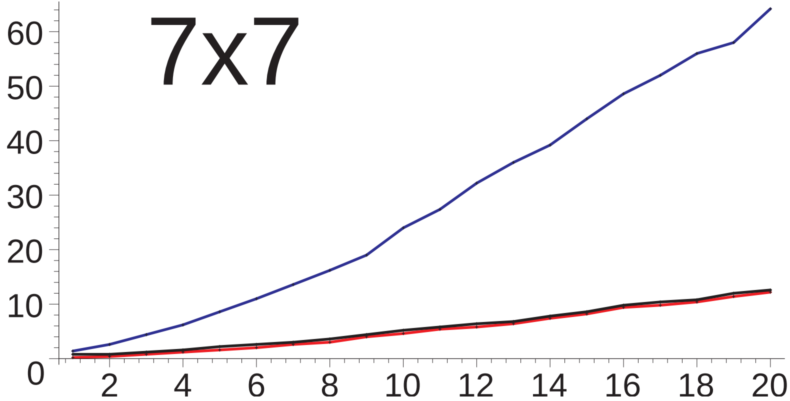
Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

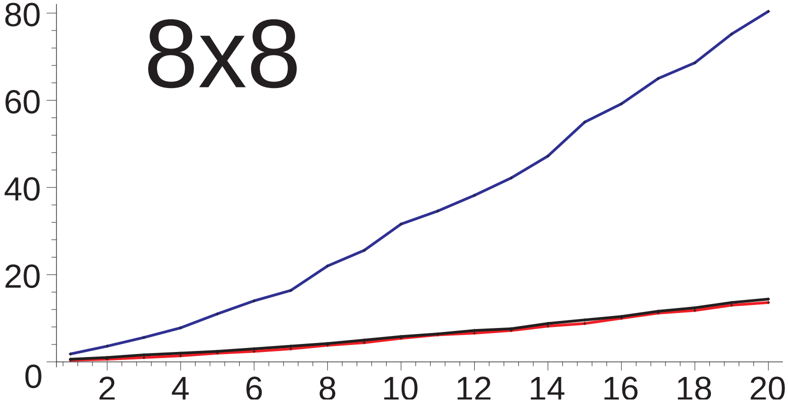
Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Produit matriciel en pratique (et en Maple)

Matrices creuses



Taille des entrées (milliers de chiffres déc.) / Temps (unité arbitraire)

Dérouler une récurrence qui se factorise

$$\boxed{L = L_k \cdots L_1 \qquad \text{avec} \qquad L_j = S^{r_j} - c^{[j]}_{r_j - 1} S^{r_j - 1} - \cdots - c^{[j]}_0}$$

$$L \cdot u = 0$$

$$\begin{aligned}
u^{[1]} &= L_1 \cdot u & u_{n+r_0} &= c^{[0]}_0 u_n + \cdots + c^{[0]}_{r_0-1} u_{n+r_0-1} + u^{[1]}_n \\
u^{[2]} &= L_2 \cdot u^{[1]} & u^{[1]}_{n+r_1} &= c^{[1]}_0 u^{[1]}_n + \cdots + c^{[1]}_{r_1-1} u^{[1]}_{n+r_1-1} + u^{[0]}_n \\
&\vdots & & \\
u^{[k]} &= L_k \cdot u^{[k-1]} & u^{[k]}_{n+r_k} &= c^{[k]}_0 u^{[k]}_n + \cdots + c^{[k]}_{r_k-1} u^{[k]}_{n+r_k-1} = 0 \\
&= 0 & &
\end{aligned}$$

$$
\begin{bmatrix} u_{n+1}^{[k-1]} \\ \vdots \\ u_{n+r_{k-1}}^{[k-1]} \\ \\ \vdots \\ \\ u_{n+1}^{[1]} \\ \vdots \\ u_{n+r_1}^{[1]} \\ u_{n+1}^{[0]} \\ \vdots \\ u_{n+r_0}^{[0]} \end{bmatrix}
=
\left[\begin{array}{c|c|c|c}
C_{k-1} & & & \\ \hline
 & \ddots & & \\ \hline
 & 1 & C_1 & \\ \hline
 & & 1 & C_0
\end{array}\right]
\begin{bmatrix} u_{n}^{[k-1]} \\ \vdots \\ u_{n+r_{k-1}-1}^{[k-1]} \\ \\ \vdots \\ \\ u_{n}^{[1]} \\ \vdots \\ u_{n+r_1-1}^{[1]} \\ u_{n}^{[0]} \\ \vdots \\ u_{n+r_0-1}^{[0]} \end{bmatrix}
$$

Résumé

- Évaluation efficace de fonctions holonomes (code disponible)
- Bornes fines sur les coefficients et les restes de leurs développements de Taylor

Perspectives

- Généralisation des bornes
- *Bit burst* en pratique

- Conditions initiales en des points singuliers, connexion
- Constante du scindage binaire
- Précisions intermédiaires
- Récurrences d'ordre élevé
- ...

Résumé

- Évaluation efficace de fonctions holonomes (code disponible)
- Bornes fines sur les coefficients et les restes de leurs développements de Taylor

Perspectives

- Généralisation des bornes
- *Bit burst* en pratique

- Conditions initiales en des points singuliers, connexion
- Constante du scindage binaire
- Précisions intermédiaires
- Récurrences d'ordre élevé
- ...

Merci !