Détendez vous !

mais...

Ne soyez pas trop paresseux

Par

Joris van der Hoeven

INRIA Rocquencourt

24 janvier 2000

Plan

1. L'approche zélée
2. L'approche paresseuse
3. L'approche détendue
4. Résultats expérimentals
5. Coefficients particuliers

1. L'approche zélée

Multiplication de séries formelles

Entrée : $\begin{cases} f = f_0 + \cdots + f_{n-1}\, z^{n-1} \\ g = g_0 + \cdots + g_{n-1}\, z^{n-1} \end{cases}$

Sortie : $h = h_0 + \cdots + h_{n-1}\, z^{n-1} = f\,g + O(z^n)$.

Algorithmes classiques de multiplication

- Multiplication naïve en $O(n^2)$.
- Diviser pour régner en $O(n^{\log_2 3})$.
- Multiplication F.F.T. en $O(n \log n \log \log n)$.

Autres opérations sur des séries formelles

Algorithme	Temps	Espace
Multiplication	$n \log n \log \log n$	n
Division	$M(n)$	n
Équations différentielles	$M(n)$	n
Fonctions holonomes	n	n
Composition algébrique	$M(n) \log n$	n
Composition générale	$M(n)\sqrt{n \log n}$	$n \log n$
Composition char. fini	$M(n) \log n$	n
Inversion $\to$ compostion	$\uparrow$	$\uparrow$

$M(n)$: temps pour la multiplication

Diviser pour régner

Pour n pair, décomposer :

$$
\begin{aligned}
f^{\downarrow} &= f_0 + \cdots + f_{n/2-1}\, z^{n/2-1}\,;\\
f^{\uparrow} &= f_{n/2} + \cdots + f_{n-1}\, z^{n/2-1}\,;\\
g^{\downarrow} &= g_0 + \cdots + g_{n/2-1}\, z^{n/2-1}\,;\\
g^{\uparrow} &= g_{n/2} + \cdots + g_{n-1}\, z^{n/2-1}.
\end{aligned}
$$

Appliquer récursivement :

$$
\begin{aligned}
f\,g &= f^{\downarrow}\,g^{\downarrow} + f^{\uparrow}\,g^{\uparrow}\,z^{n}\\
&+ \left[(f^{\downarrow} + f^{\uparrow})\,(g^{\downarrow} + g^{\uparrow}) - f^{\downarrow}\,g^{\downarrow} - f^{\uparrow}\,g^{\uparrow}\right] z^{n/2}
\end{aligned}
$$

Graphiquement

$g^{\uparrow}$	$*$	$f^{\uparrow}\,g^{\uparrow}$
$g^{\downarrow}$	$f^{\downarrow}\,g^{\downarrow}$	$*$
$\times$	$f^{\downarrow}$	$f^{\uparrow}$

$$* = (f^{\downarrow} + f^{\uparrow})\,(g^{\downarrow} + g^{\uparrow}) - f^{\downarrow}\,g^{\downarrow} - f^{\uparrow}\,g^{\uparrow}$$

Méthode de Newton

Logarithme

$$\log f = \log f_0 + \int \frac{f'}{f}$$

Exponentiation

Pour n pair, soient

$$\begin{array}{rcl} f & = & f_0 + \cdots + f_{n-1}\, z^{n-1}\,; \\ g & = & g_0 + \cdots + g_{n/2-1}\, z^{n/2-1} \end{array}$$

telles que

$$\log g - f = O(z^{n/2}).$$

Posons

$$\tilde{g} = g - (\log g - f)\, g$$

Alors

$$\log \tilde{g} - f = O(z^{n}).$$

$\longrightarrow$ algorithme d'exponentiation en $O(M(n))$.

Inversion

L'équation $f \circ g - z = 0$ induit l'itération

$$\tilde{g} = g - \frac{f \circ g - z}{f' \circ g}$$

Composition polynomiale

Position du problème

Entrées :

- $f = f_0 + \cdots + f_{p-1} z^{p-1}$ (avec $p \to \infty$) ;
- $g = g_1 z + \cdots + g_{q-1} z^{q-1}$ (avec q fixe) ;
- Un ordre $n \geqslant p$ (avec $n \to \infty$).

Sortie : $h = h_0 + \cdots + h_{n-1} z^{n-1}$, telle que

$$h = f \circ g + O(z^n)$$

Algorithme par dichotomie ($p, q, n \in 2^{\mathbb{N}}$)

$$f \circ g = f^{\downarrow} \circ g + (f^{\uparrow} \circ g) \times g^{p/2}$$

Algorithme en temps $O(\frac{p\,q}{n} M(n) \log n)$, car

- $1 + 2 + \cdots + \frac{p\,q}{n}$ multiplications de longueur n.
- $\frac{2\,p\,q}{n}$ multiplications de longueur $n/2$.
- $\frac{4\,p\,q}{n}$ multiplications de longueur $n/4$;
- Etc.
- $p/2$ multiplications de longueur q.

Composition générale

Problème

Entrée : $f_0 + \cdots + f_{n-1}\, z^{n-1}$ et $g_1\, z + \cdots + g_{n-1}\, z^{n-1}$
Sortie : $h_0 + \cdots + h_{n-1}\, z^{n-1}$ avec $h = f \circ g + O(z^n)$

Algorithme de Brent & Kung

Idée : découper $g = g_* + g^*$

$$\begin{aligned} g_* &= g_1\, z + \cdots + g_{q-1}\, z^{q-1}; \\ g^* &= g_q\, z^q + \cdots + g_{n-1}\, z^{n-1}. \end{aligned}$$

Puis écrire :

$$f \circ g = f \circ g_* + (f' \circ g_*)\, g^* + \frac{1}{2}\, (f'' \circ g_*)\, (g^*)^2 + \cdots$$

Calcul des $f^{(n)} \circ g_*$

Par itération direct ou inverse :

$$\begin{aligned} f^{(i)} \circ g_* &= \frac{(f^{(i-1)} \circ g_*)'}{g_*'}; \\ \frac{1}{(i-1)!}\, f^{(i-1)} \circ g_* &= f_{i-1} + i \int \left(\frac{1}{i!}\, f^{(i)} \circ g_* \right) g_*'. \end{aligned}$$

2. Approche paresseuse

Principe

On considère des séries formelles comme des flots de coefficients. Les coefficients sont calculés un par un et à chaque étape on n'effectue que les calculs strictement nécessaires.

Implantation

Une série formelle f est un algorithme qui ne prend rien en entrée et qui rend le premier coefficient f_0 de f et la série "reste" $(f - f_0)/z$.

Conséquence importante

On calcule $(f\,g)_n$ dès que f_0, ..., f_n et g_0, ..., g_n sont connus. En particulier, f_{n+1} et g_{n+1} peuvent dépendre de $(f g)_0, \ldots, (f g)_n$.

Application

Calcul de l'exponentielle $g = e^f$ d'une série f par

$$g = \int f' g$$

Inconvénient

On ne peut utiliser la multiplication F.F.T. ou diviser pour régner.

3. Approche détendue

Idée fondamentale

$$\text{Anticipation} \longrightarrow \text{Accélération}$$

Exemple : multiplication à l'ordre $n = 3$

Algorithme naïf

g_2	2		
g_1	1	2	
g_0	0	1	2
$\times$	f_0	f_1	f_2

0 $\quad h_0 = f_0\, g_0$.

1 $\quad h_1 = f_0\, g_1 + f_1\, g_0$.

2 $\quad h_2 = f_0\, g_2 + f_1\, g_1 + f_2\, g_0$.

Algorithme détendu

g_2	2		
g_1	1	1	
g_0	0	1	2
$\times$	f_0	f_1	f_2

0 $\quad h_0 = f_0\, g_0$.

1 $\quad h_1 = (f_0 + f_1)\,(g_0 + g_1) - f_0\, g_0 - f_1\, g_1$.

2 $\quad h_2 = f_0\, g_2 + f_1\, g_1 + f_2\, g_0$.

Diviser pour régner

Observation

La multiplication “diviser pour régner est “essentiellement détendue” ; la formule pour h_k ne dépend que de $f_0, \ldots, f_k$ et $g_0, \ldots, g_k$.

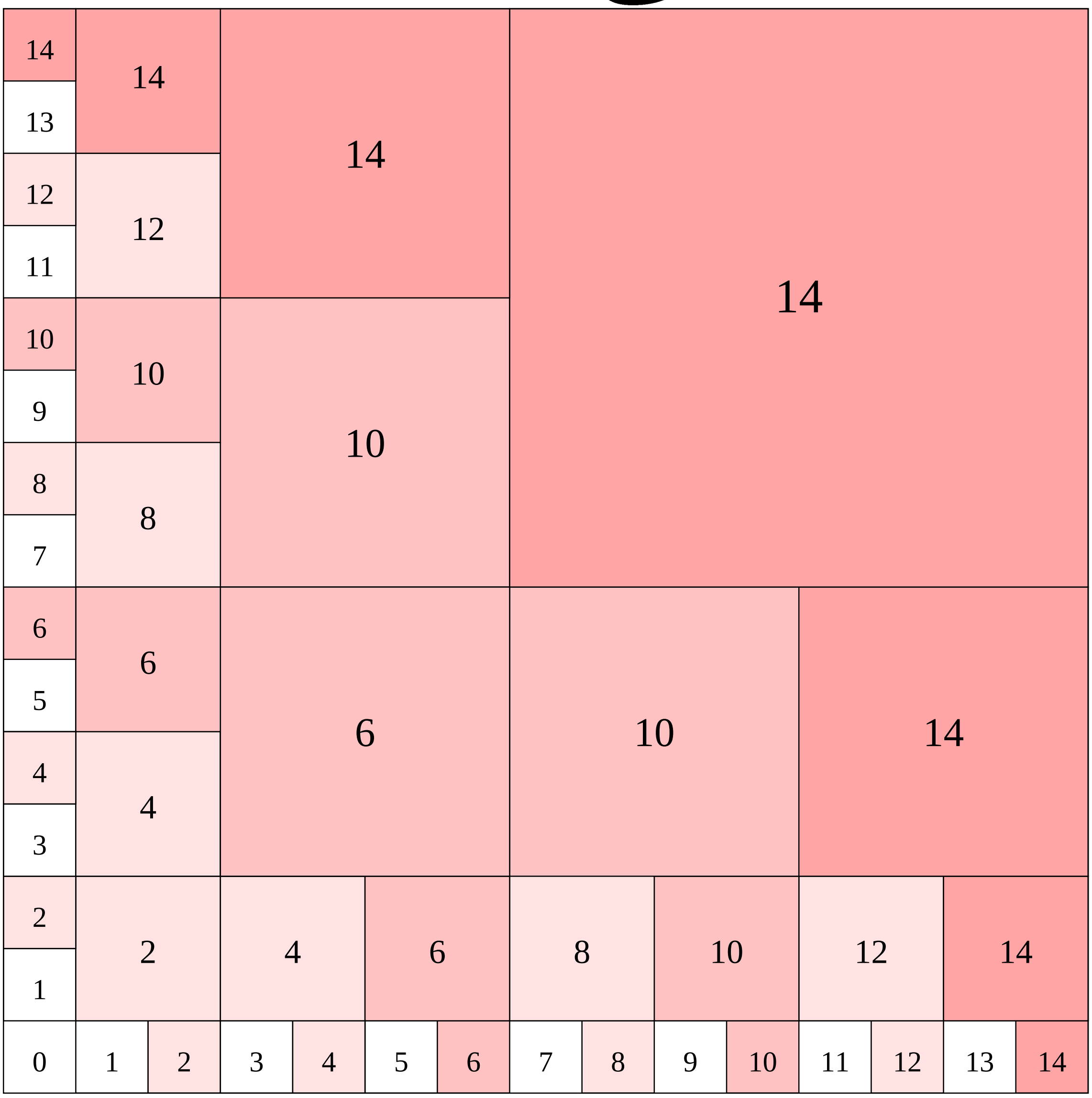
Exemple : multiplication à l’ordre 4

- $h_0 = f_0\, g_0$;
- $h_1 = (f_0 + f_1)\,(g_0 + g_1) - f_0\, g_0 - f_1\, g_1$;
- $h_2 = (f_0 + f_2)\,(g_0 + g_2) - f_0\, g_0 - f_2\, g_2$;
- $h_3 = (f_0 + f_1 + f_2 + f_3)\,(g_0 + g_1 + g_2 + g_3) - (f_0 + f_1)\,(g_0 + g_1) - (f_2 + f_3)\,(g_2 + g_3) + f_0\, g_0 + f_1\, g_1 + f_2\, g_2 + f_3\, g_3$;
- $h_4 = (f_1 + f_3)\,(g_1 + g_3) - f_1\, g_1 - f_3\, g_3$;
- $h_5 = (f_2 + f_3)\,(g_2 + g_3) - f_2\, g_3 - f_2\, g_3$;
- $h_6 = f_3\, g_3$.

g_3	3	3	3	3
g_2	2	3	2	3
g_1	1	1	3	3
g_0	0	1	2	3
$\times$	f_0	f_1	f_2	f_3

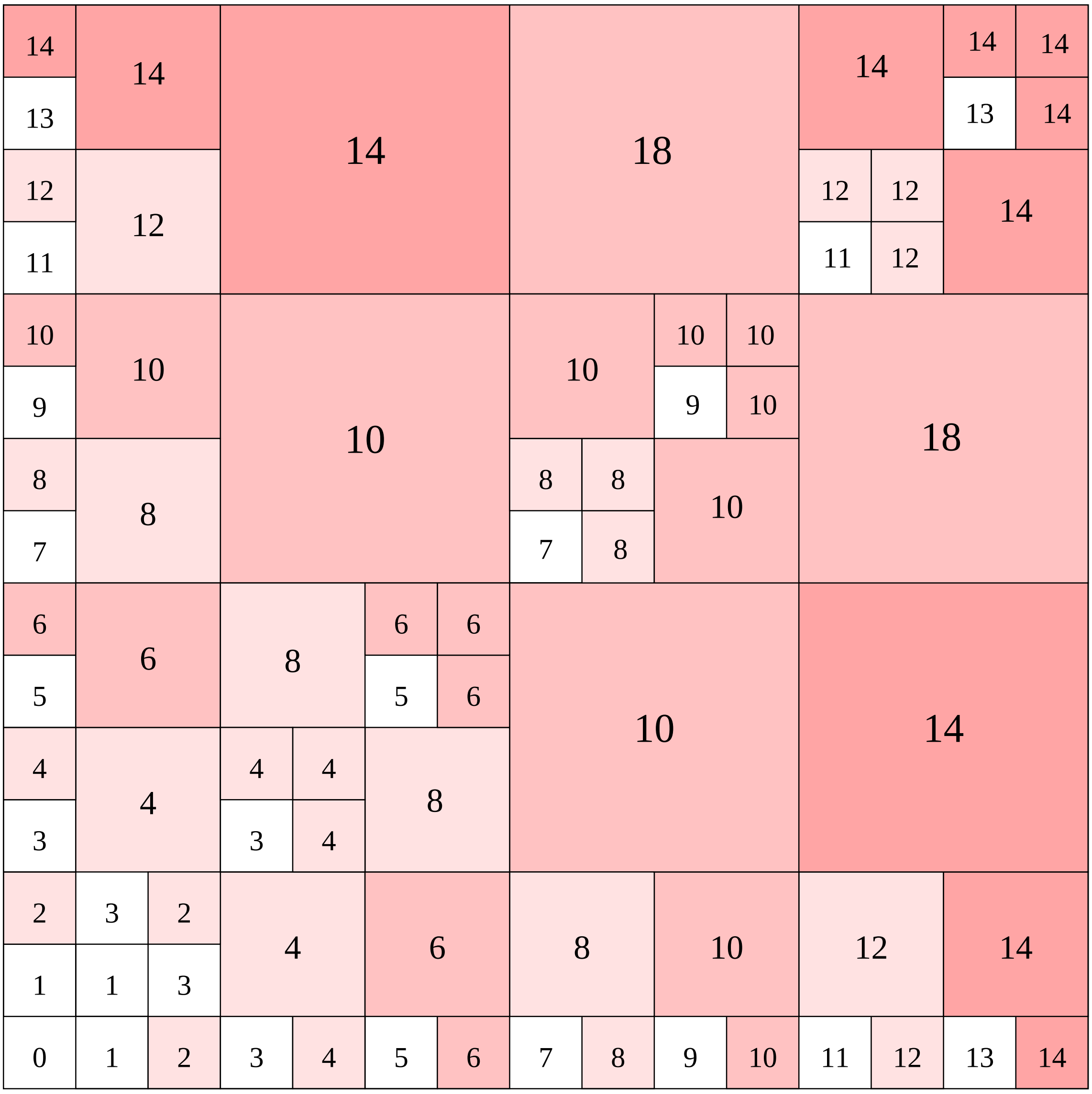
Multiplication rapide

Par image

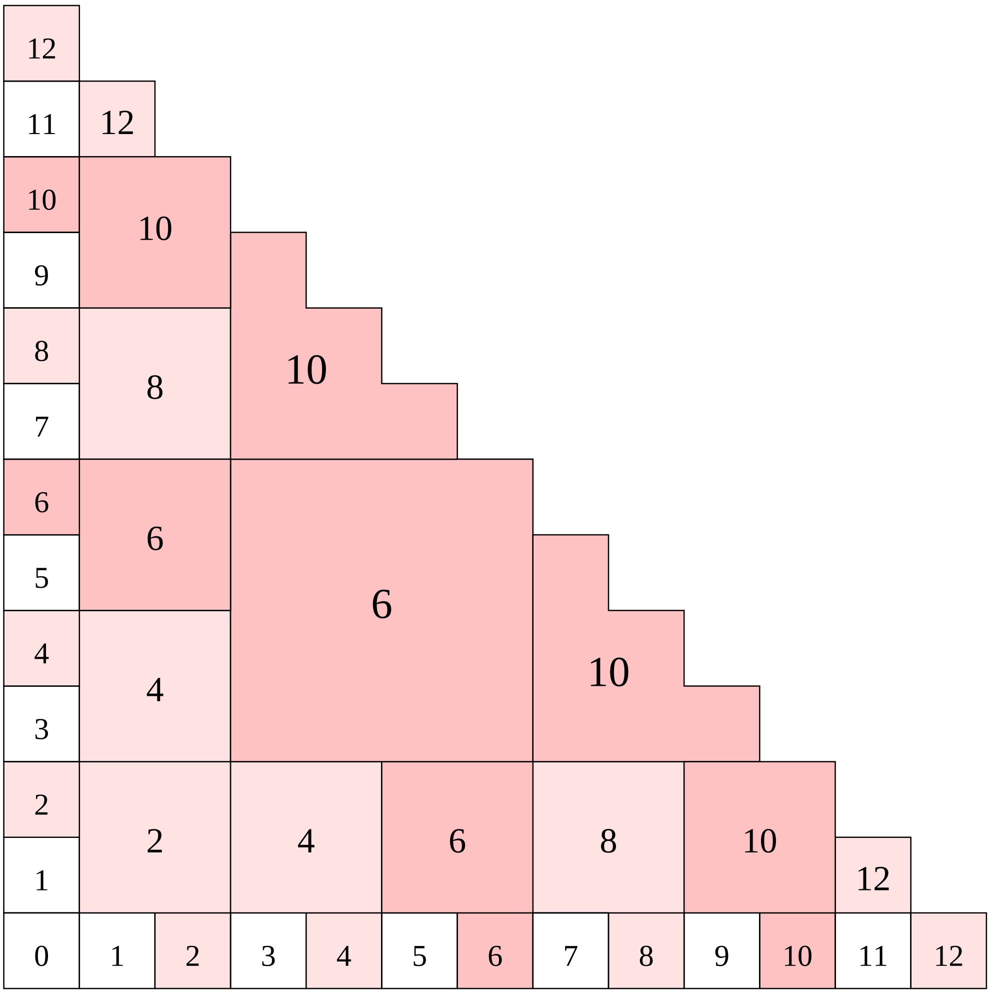


$\longrightarrow$ Algorithme détendu en $O(M(n)\log n)$.

Variante


14
14
14
18
14
14
14
13
13
14
12
12
12
12
14
11
11
12
10
10
10
10
10
10
9
9
10
18
8
8
8
8
10
7
7
8
6
6
8
6
6
10
14
5
5
6
4
4
4
4
8
3
3
4
2
3
2
4
6
8
10
12
14
1
1
3
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14

Multiplication tronquée



Autres algorithmes détendus

Composition polynomiale et algébrique

Algorithmes "essentiellement détendues".

Composition générale

On change q dans l'algorithme de Brent & Kung à chaque puissance de 4.

Algorithme	Temps	Espace
Multiplication D.P.R.	$n^{\log_2 3}$	$n \log n$
Multiplication rapide	$M(n) \log n$	n
Division	$D(n)$	n
Équations différentielles	$D(n)$	n
Fonctions holonomes	n	n
Composition algébrique	$D(n) \log n$	n
Composition générale	$D(n)\sqrt{n \log n}$	$n^{3/2} \log n$
Composition char. fini	$D(n) \log n$	$n \log n$
Inversion $\rightarrow$ compostion	$\uparrow$	$\uparrow$

$D(n)$: temps pour la multiplication détendue

4. Résultats expérimentaux

Exemple 1 : développement de exp $(z\, e^z)$

Exemple 2 : énumération d'alcools

La série génératrice s telle que s_n est le nombre d'alcools de la forme $C_nH_{2n+1}OH$ vérifie

$$s(z) = 1 + z\,\frac{s(z)^3 + 2\,s(z^3)}{3}$$

Exemple 3 : équations fonctionnelles

L'équation différentielle aux différences

$$f(x) = \frac{1}{x}\,(1 + f(x+1) + f'(x)^2) \tag{1}$$

admet une solution formelle unique en x^{-1} :

$$f(x) = \frac{1}{x} + \frac{1}{x^2} - \frac{1}{x^4} - \frac{3}{x^6} + O\left(\frac{1}{x^7}\right)$$

On réécrit (1) pour $f(x) = f(1/z) = g(z)$:

$$g(z) = z\left(1 + g\left(\frac{z}{1+z}\right) - z^4\, g'(z)^2\right) \tag{2}$$

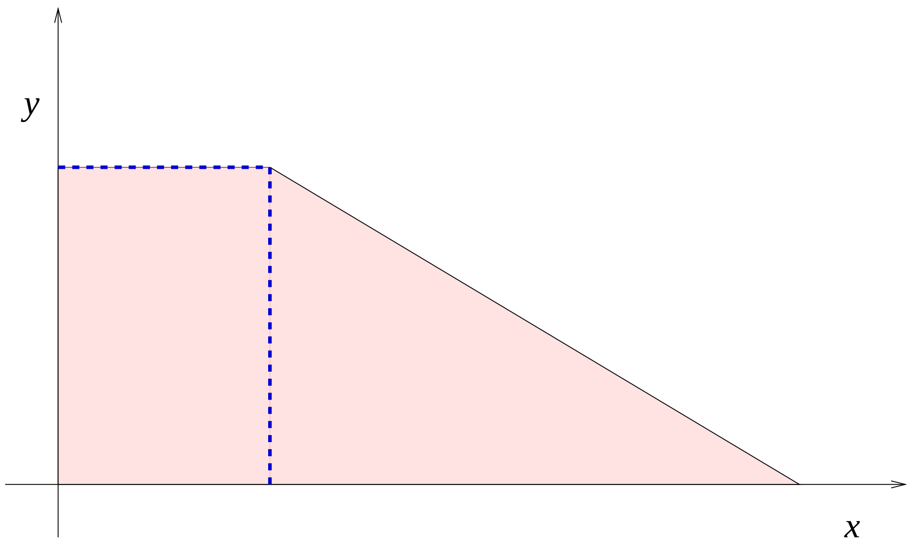
Autres applications

Exemple 4 : é.d.p.

Soit $f \in \mathbb{Q}[[x, y]]$ telle que

$$\begin{aligned} \frac{\partial f}{\partial y} &= \left(\frac{\partial f}{\partial x}\right)^2 + \left(\frac{\partial^2 f}{\partial x^2}\right)^2; \\ f(x,0) &= e^x. \end{aligned}$$

Problème : calculer $[x^n y^m]\, f$.



Arbres 2-3

Série génératrice f vérifie

$$f(z) = z + f(z^2 + z^3)$$

5. Coefficients particuliers

Arithmétique dense rapide

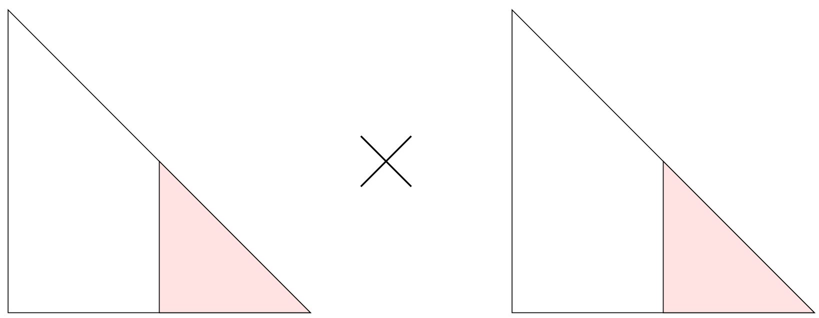
Benchmarks faussés par mauvaise arithmétique.
F.F.T. généralisée pour “anneaux denses”.

Instabilité numérique

$$\begin{aligned} & (1.000\cdot 10^{0}+1.000\cdot 10^{-5}\,z)^{2} \\ = \;& 1.000\cdot 10^{0}+0.000\cdot 10^{-5}\,z+1.000\cdot 10^{-10}\,z^{2}, \end{aligned}$$

puisque $1.000\cdot 10^{0}+1.000\cdot 10^{-5}=1.000\cdot 10^{0}$.
Solution : transformation $z\rightarrow\rho\, z$.

Problême analogue pour séries bivariées



Solution : multiplication tronquée plus fine.