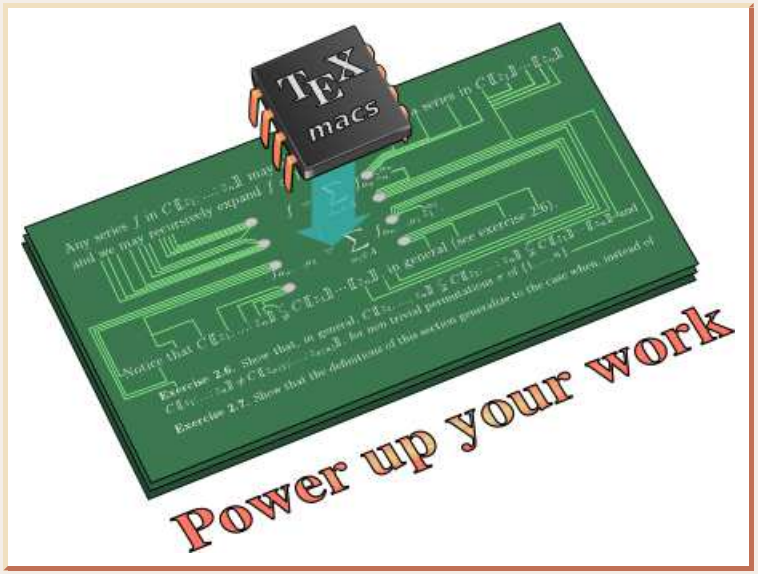
Calcul analytique II

Joris van der Hoeven

CNRS, École polytechnique



JNCF, Luminy, 2011

http://www.TEXMACS.org

Rappels sur la complexité

Multiplication de deux entiers de p chiffres

- $\mathsf{I}(p) = \mathcal{O}(p^2)$: multiplication naïve
- $\mathsf{I}(p) = \mathcal{O}\big(p^{\log 3/\log 2}\big)$: multiplication de Karatsuba
- $\mathsf{I}(p) = \mathcal{O}(p \log p \log\log p)$: multiplication de Schönhage-Strassen

Multiplication de deux polynômes à coefficients dans $\mathbb{K}$ de degré n

- $\mathsf{M}_{\mathbb{K}}(n) = \mathcal{O}_{\mathbb{K}}(n^2)$: multiplication naïve
- $\mathsf{M}_{\mathbb{K}}(n) = \mathcal{O}_{\mathbb{K}}\big(n^{\log 3/\log 2}\big)$: multiplication de Karatsuba
- $\mathsf{M}_{\mathbb{K}}(n) = \mathcal{O}_{\mathbb{K}}(n \log n \log\log n)$: multiplication de Schönhage-Strassen
- $\mathsf{M}_{\mathbb{K}}(n) = \mathcal{O}_{\mathbb{K}}(n \log n)$ si $\mathbb{K}$ admet suffisamment de racines 2^p-ièmes d'unité

Multiplication de deux polynômes de degré n avec des coeffients de p chiffres

- $\mathsf{IM}(p,n) = \mathcal{O}(\mathsf{I}(n\,p))$: Kronecker

Référence

von Zurgathen & Gerhard : Modern computer algebra

Multiplication de Karatsuba

$$\begin{aligned} & (P_{\mathbb{O}} + P_{\mathbb{I}}\, z)\,(Q_{\mathbb{O}} + Q_{\mathbb{I}}\, z) \\ = \;& P_{\mathbb{O}}\, Q_{\mathbb{O}} + ((P_{\mathbb{O}} + P_{\mathbb{I}})\,(Q_{\mathbb{O}} + Q_{\mathbb{I}}) - P_{\mathbb{O}}\, Q_{\mathbb{O}} - P_{\mathbb{I}}\, Q_{\mathbb{I}})\, z + P_{\mathbb{I}}\, Q_{\mathbb{I}}\, z^2 \end{aligned}$$

Multiplication FFT

$$\begin{aligned} \omega^n &= 1 \\ \mathrm{FFT}_\omega(P) &= (P(1), P(\omega), ..., P(\omega^{n-1})) \end{aligned}$$

$$\begin{aligned} \deg(PQ) &< n \\ PQ &= \mathrm{FFT}_\omega^{-1}(\mathrm{FFT}_\omega(P)\,\mathrm{FFT}_\omega(Q)) \end{aligned}$$

Question ouverte : multiplication tronqué en temps $\lambda\,\mathsf{M}_{\mathbb{K}}(n)$ avec $\lambda < 1$?

Division

Division avec reste pour $P, Q \in \mathbb{K}[z]$ avec $\deg P \leqslant 2\,n$ et $\deg Q \leqslant n$: $\mathcal{O}(\mathsf{M}_{\mathbb{K}}(n))$
Inversion de $f \in \mathbb{K}[[z]]$ avec $f_0 \neq 0$ à l'ordre n
Itération de Newton :

$$\begin{aligned} g &= \frac{1}{f} + \mathcal{O}(z^n) \\ \tilde{g} &= g - (f\,g - 1)\,g \\ &= g - \frac{f\,g - 1}{f} + \mathcal{O}(z^{2n}) \\ \tilde{g} &= \frac{1}{f} + \mathcal{O}(z^{2n}) \end{aligned}$$

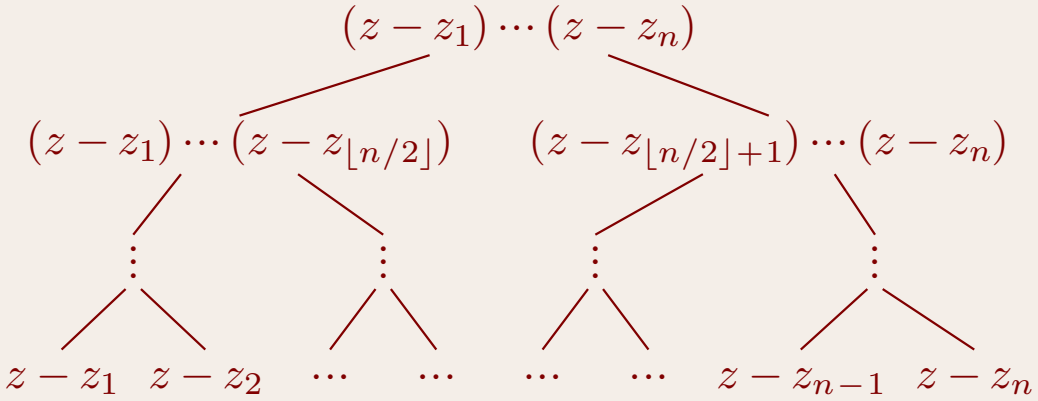
Coût : $\mathsf{D}_{\mathbb{K}}(n) = \mathcal{O}(\mathsf{M}_{\mathbb{K}}(n)) + \mathsf{D}_{\mathbb{K}}(n/2) \quad \rightsquigarrow \quad \mathsf{D}_{\mathbb{K}}(n) = \mathcal{O}(\mathsf{M}_{\mathbb{K}}(n))$

Racines de polynômes : Hensel
Newton pour équations fonctionnelles : Brent & Kung, Sedoglavic

Évaluation multi-points

Entrée : $P \in \mathbb{K}[z]$ avec $\deg P < n$ et points $z_1, \ldots, z_n \in \mathbb{K}$
Sortie : $P(z_1), \ldots, P(z_n)$

Précalcul :



Algorithme :

- Si $n=1$, retourner P_0
- Sinon, soient $Q=(z-z_1)\cdots(z-z_{\lfloor n/2\rfloor})$ et $R=(z-z_{\lfloor n/2\rfloor+1})\cdots(z-z_n)$
- Evaluer $P \operatorname{rem} Q$ en $z_1, \ldots, z_{\lfloor n/2\rfloor}$ et $P \operatorname{rem} R$ en $z_{\lfloor n/2\rfloor+1}, \ldots, z_n$

Coût : $\mathsf{E}_{\mathbb{K}}(n) = 2\,\mathsf{E}_{\mathbb{K}}(n/2) + \mathcal{O}(\mathsf{M}_{\mathbb{K}}(n)) \quad \rightsquigarrow \quad \mathsf{E}_{\mathbb{K}}(n) = \mathcal{O}(\mathsf{M}_{\mathbb{K}}(n)\log n)$

Calcul détendu

Multiplication détendue de $f, g \in \mathbb{K}[[z]]$

Sortie de $(f\,g)_n$ **dès que** $f_0, \ldots, f_n$ et $g_0, \ldots, g_n$
Permet la résolution d'équations récursives et implicites

Inverse g de $1 - f$ avec $f \in z\,\mathbb{K}[[z]]$

$$\begin{aligned} g &= 1 + f\,g \\ g_n &= \sum_{k=0}^{n-1} f_{n-k}\,g_k, \qquad n > 0 \end{aligned}$$

Exponentielle g de f avec $f \in z\,\mathbb{K}[[z]]$

$$\begin{aligned} g &= 1 + \int f'\,g \\ g_n &= \frac{1}{n} \sum_{i=0}^{n-1} (n-i)\,f_{n-i}\,g_i, \qquad n > 0 \end{aligned}$$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$g_0 = 1$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
	g_2							
	g_1							
	g_0							
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$
Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$\begin{aligned} g_0 &= 1 \\ g_1 &= 1 \end{aligned}$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
	g_2							
	g_1							
1	g_0	1						
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$

Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2}
\end{aligned}
$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
	g_2							
1	g_1	1						
1	g_0	1	2					
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$

Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6}
\end{aligned}
$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
$\frac{3}{2}$	g_2	$\frac{3}{2}$						
1	g_1	1	2					
1	g_0	1	2	3				
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$

Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6} \\
g_4 &= \tfrac{73}{24}
\end{aligned}
$$

	$\uparrow$							
	g_5							
	g_4							
$\frac{13}{6}$	g_3	$\frac{13}{6}$						
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3					
1	g_1	1	2	3				
1	g_0	1	2	3	4			
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$

Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6} \\
g_4 &= \tfrac{73}{24} \\
g_5 &= \tfrac{167}{40}
\end{aligned}
$$

	$\uparrow$							
	g_5							
$\frac{73}{24}$	g_4	$\frac{73}{24}$						
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$					
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$				
1	g_1	1	2	3	4			
1	g_0	1	2	3	4	5		
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$

Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6} \\
g_4 &= \tfrac{73}{24} \\
g_5 &= \tfrac{167}{40} \\
g_6 &= \tfrac{4051}{720}
\end{aligned}
$$

	$\uparrow$							
$\frac{167}{40}$	g_5	$\frac{167}{40}$						
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$				
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6			
1	g_1	1	2	3	4	5		
1	g_0	1	2	3	4	5	6	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée naïve : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{1}{2}\,\mathsf{M}_K(n)$

Multiplication détendue naïve : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Exemple d'exponentiation

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6} \\
g_4 &= \tfrac{73}{24} \\
g_5 &= \tfrac{167}{40} \\
g_6 &= \tfrac{4051}{720}
\end{aligned}
$$

	$\uparrow$							
$\frac{167}{40}$	g_5	$\frac{167}{40}$						
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$				
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6			
1	g_1	1	2	3	4	5		
1	g_0	1	2	3	4	5	6	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Multiplication tronquée par Karatsuba pair/impair : $\mathsf{T}_{\mathbb{K}}(n) \sim \frac{9}{16}\,\mathsf{M}_K(n)$

Multiplication détendue par Karatsuba pair/impair : $\mathsf{R}_{\mathbb{K}}(n) = \mathsf{T}_{\mathbb{K}}(n)$

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
	g_3								
	g_2								
	g_1								
1	g_0	1							
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
	g_3								
	g_2								
1	g_1	1							
1	g_0	1	2						
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Multiplication détendue rapide

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
	g_3								
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$					
1	g_1	1	2	3					
1	g_0	1	2	3					
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Multiplication détendue rapide

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
$\frac{13}{6}$	g_3	$\frac{13}{6}$							
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$					
1	g_1	1	2	3					
1	g_0	1	2	3	4				
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$					
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$			
1	g_1	1	2	3	4	5			
1	g_0	1	2	3	4	5			
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
$\frac{167}{40}$	g_5	$\frac{167}{40}$							
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$					
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$			
1	g_1	1	2	3	4	5			
1	g_0	1	2	3	4	5	6		
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
$\frac{4051}{720}$	g_6	$\frac{4051}{720}$	$\frac{4051}{360}$	$\frac{4051}{240}$	$\frac{4051}{190}$	$\frac{4051}{144}$	$\frac{4051}{120}$	$\frac{28357}{720}$	
$\frac{167}{40}$	g_5	$\frac{167}{40}$	$\frac{167}{20}$	$\frac{501}{40}$	$\frac{167}{10}$	$\frac{167}{8}$	$\frac{501}{20}$	$\frac{1169}{40}$	
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$	$\frac{73}{6}$	$\frac{365}{24}$	$\frac{73}{4}$	$\frac{511}{24}$	
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$	$\frac{26}{3}$	$\frac{65}{6}$	13	$\frac{91}{6}$	
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$	9	$\frac{21}{2}$	
1	g_1	1	2	3	4	5	6	7	
1	g_0	1	2	3	4	5	6	7	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
$\frac{4051}{720}$	g_6	$\frac{4051}{720}$	$\frac{4051}{360}$	$\frac{4051}{240}$	$\frac{4051}{190}$	$\frac{4051}{144}$	$\frac{4051}{120}$	$\frac{28357}{720}$	
$\frac{167}{40}$	g_5	$\frac{167}{40}$	$\frac{167}{20}$	$\frac{501}{40}$	$\frac{167}{10}$	$\frac{167}{8}$	$\frac{501}{20}$	$\frac{1169}{40}$	
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$	$\frac{73}{6}$	$\frac{365}{24}$	$\frac{73}{4}$	$\frac{511}{24}$	
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$	$\frac{26}{3}$	$\frac{65}{6}$	13	$\frac{91}{6}$	
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$	9	$\frac{21}{2}$	
1	g_1	1	2	3	4	5	6	7	
1	g_0	1	2	3	4	5	6	7	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

$$\begin{aligned} \mathsf{R}(n) &= O(2\,\mathsf{M}(n/2) + 4\,\mathsf{M}(n/4) + 8\,\mathsf{M}(n/8) + \cdots) \\ &= O(\mathsf{M}(n)\log n). \end{aligned}$$

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
$\frac{4051}{720}$	g_6	$\frac{4051}{720}$	$\frac{4051}{360}$	$\frac{4051}{240}$	$\frac{4051}{190}$	$\frac{4051}{144}$	$\frac{4051}{120}$	$\frac{28357}{720}$	
$\frac{167}{40}$	g_5	$\frac{167}{40}$	$\frac{167}{20}$	$\frac{501}{40}$	$\frac{167}{10}$	$\frac{167}{8}$	$\frac{501}{20}$	$\frac{1169}{40}$	
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$	$\frac{73}{6}$	$\frac{365}{24}$	$\frac{73}{4}$	$\frac{511}{24}$	
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$	$\frac{26}{3}$	$\frac{65}{6}$	13	$\frac{91}{6}$	
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$	9	$\frac{21}{2}$	
1	g_1	1	2	3	4	5	6	7	
1	g_0	1	2	3	4	5	6	7	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Question ouverte : peut on faire mieux que $\mathsf{R}_{\mathbb{K}}(n) = \mathcal{O}(\mathsf{M}_{\mathbb{K}}(n) \log n)$?

Si $\mathbb{K}$ admet suffisamment de racines 2^p-ièmes d'unité : $\mathsf{R}_{\mathbb{K}}(n) = \mathcal{O}\Big(\mathsf{M}_{\mathbb{K}}(n)\, \mathrm{e}^{2\sqrt{\log\log n}}\Big)$

Nombres de Bell exacts

```
Mmx] use "algebramix"
Mmx] z == series (0, 1);
Mmx] B == exp (exp z - 1)
```

$$1 + z + z^2 + \frac{5}{6}\,z^3 + \frac{5}{8}\,z^4 + \frac{13}{30}\,z^5 + \frac{203}{720}\,z^6 + \frac{877}{5040}\,z^7 + \frac{23}{224}\,z^8 + \frac{1007}{17280}\,z^9 + O(z^{10})$$

```
Mmx] B[1000] * 1000!
```

```
29899013356824084214804223538976464839473928098212305047832737888945413625123259596641\
1\
65872540391578300639147082986964028021802248993382881013411276574829121155811755170830\
6\
66039838837273971971676782389800810361809319250755399325279656765435255999301529770267\
1\
07281619733800281695881540007577899106878679451165492535930459233713316342551545242815\
8\
02367257284852612201081016386308535990145447341800455472334713864080523978960296365736\
9\
99295932080550928561633025800627524911700149562106895897725047744775812241800937310491\
7\
97818107578233924187312824632629095993832334781713007323483688294825326897450386817327\
4\
10532925074613888321264138083842196202242956001314953449497244271843922741908252107652\
2\
01346933889741070435350690242062001522697855278356012055718392851567813397125419144780\
4\
76479197990921602015873703820769182603836788465785093563686025690269802153802436873530\
8\
77006737154523895273029510238745997356292232631282773748762989386003970214423843947094\
0\
21177989737557020369751561595003372955621411858485959813344799967960196238368337022346\
9\
46771703060269288691694028444791203978533454759410587065022546491518871238421560825907\
1\
35885619221776405898771057270555581449229994215739476758785884545723062263992367750091\
3\
19644861547658472282284005892044371587560711880627741139497818835632120761570174928529\
6\
97397267899554407350161283097123211048049269727655279783900702416095132827766428865017\
6\
53366696304131436690232979453876337599721772897049270230544262611264917393374756384152\
7\
84943607952408782612639220380791445272655004475989064276373713608901650681165467490310\
8\
98804916827069427310961109285035545084791339423266482359955663377201515204340817580915\
4\
68489969181643341007197836481461051798995640789292580146918580703759556634019451731530\
0\
34209189203377522668309771129566108101617727442045637098112678864654309987785463307376\
5\
44339506878267267349348171320834971956806668304099159992067385998690820326902473886782\
7\
81499414773179
```

```
Mmx]
```

$$
\begin{aligned}
P(z) &= 1.0000 + 1.0000 \cdot 2^{-64}\, z \\
P(z)^2 &= 1.0000^2 + \\
&\quad [(1.0000 + 1.0000 \cdot 2^{-64})^2 - 1.0000^2 - (1.0000 \cdot 2^{-64})^2]\, z + \\
&\quad (1.0000 \cdot 2^{-64})^2\, z^2 \\
&= 1.0000 + (1.0000 - 1.0000 - 1.0000 \cdot 2^{-128})\, z + 1.0000 \cdot 2^{-128}\, z^2 \\
&= 1.0000 - 1.0000 \cdot 2^{-128}\, z + 1.0000 \cdot 2^{-128}\, z^2
\end{aligned}
$$

Préconditionnement

$$P^2 = [P \circ (2^{64}\, z)]^2 \circ (2^{-64}\, z)$$

Problème

$$P = 1.0000 + 1.0000\, z + 1.0000 \cdot 2^{-64}\, z^2$$

Instabilité numérique

$$
\begin{aligned}
P(z) &= 1.0000 + 1.0000 \cdot 2^{-64}\, z \\
P(z)^2 &= 1.0000^2 + \\
&\quad [(1.0000 + 1.0000 \cdot 2^{-64})^2 - 1.0000^2 - (1.0000 \cdot 2^{-64})^2]\, z + \\
&\quad (1.0000 \cdot 2^{-64})^2\, z^2 \\
&= 1.0000 + (1.0000 - 1.0000 - 1.0000 \cdot 2^{-128})\, z + 1.0000 \cdot 2^{-128}\, z^2 \\
&= 1.0000 - 1.0000 \cdot 2^{-128}\, z + 1.0000 \cdot 2^{-128}\, z^2
\end{aligned}
$$

Préconditionnement

$$P^2 = [P \circ (2^{64}\, z)]^2 \circ (2^{-64}\, z)$$

Cas des séries

$$|\log|f_n| + n \log \varrho| = (\log n)^{O(1)} \qquad \text{(généralement)}$$

Nombres de Bell approchés

```
Mmx] use "analyziz"
Mmx] bit_precision := 64;
Mmx] z == series (0.0, 1.0);
Mmx] B == exp (exp z - 1)
```

$1.0000000000000000000 + 1.0000000000000000000\,z + 1.0000000000000000000\,z^2 + 0.8333333333\backslash 33333333369\,z^3 + 0.625000000000000000054\,z^4 + 0.433333333333333364\,z^5 + 0.2819444444444444\backslash 44471\,z^6 + 0.174007936507936507948\,z^7 + 0.102678571428571428570\,z^8 + 0.058275462962962\backslash 9678\,z^9 + O(z^{10})$

```
Mmx] B[10000]
```

$5.593910855120672200 85e - 7996$

```
Mmx] bit_precision := 128;
Mmx] z == series (0.0, 1.0);
Mmx] B == exp (exp z - 1);
Mmx] B[10000]
```

$5.59391085512067159074423017436837541267 9e - 7996$

```
Mmx]
```

Validation des calculs

Inversion naïve

Mêmes estimations d'erreur pour $\dfrac{1}{1-z+z^2}$ et $\dfrac{1}{1-z-z^2}$

Méthode perturbative pour l'inversion

Estimation d'erreur fine pour $\dfrac{1}{1-z+z^2}$

Exponentiation naïve $g = \exp f$

Estimations généralement fines :
$\exp f$ et $\exp |f|$ même type de singularité dominant (où $|f|_n = |f_n|$)

Méthode perturbative pour l'exponentiation

$\tilde{g} \approx \exp f, \quad h = \exp f \,/\, \tilde{g}, \quad h' = (f' - \tilde{g}' \,/\, \tilde{g})\, h$

Nombres de Bell certifiés

```
Mmx] use "analyziz"
Mmx] bit_precision := 64;
Mmx] z == series (0.0, 1.0);
Mmx] B == exp (exp z - 1);
Mmx] B[10000]
```

$5.593910855120672200 85e - 7996$

```
Mmx] z == series (ball 0.0, ball 1.0);
Mmx] B == exp (exp z - 1);
Mmx] B[10000]
```

$5.593910855121e - 7996$

```
Mmx]
```

Modèles de Taylor (Berz et Makino)

Modèles de Taylor d'ordre n sur $\mathcal{B}(0,r)$

$$\begin{aligned}
\mathcal{B}_r(\varphi,K) &= \{f \text{ analytique sur } \mathcal{B}(0,r)\colon \forall |z|\leqslant r, |f(z)-\varphi(z)|\leqslant K\}\\
\mathcal{B}_r(\mathbb{D}[z]_{<n},\mathbb{D}) &= \{\mathcal{B}_r(f_0+\cdots+f_{n-1}\,z^{n-1},K)\colon f_0,\ldots,f_{n-1},K\in\mathbb{D}\}
\end{aligned}$$

Produit

$$\begin{aligned}
&\mathcal{B}_r(f_0+\cdots+f_{n-1}\,z^{n-1},K)\,\mathcal{B}_r(g_0+\cdots+g_{n-1}\,z^{n-1},L)\\
&= \mathcal{B}_r(f_0\,g_0+\cdots+(f_0\,g_{n-1}+\cdots+f_{n-1}\,g_0)\,z^{n-1},E^{\mathrm{tr}}+E^{\mathrm{rnd}})\\
E^{\mathrm{tr}} &= |f_1|\,|g_{n-1}|+|f_2|\,(|g_{n-1}|+|g_{n-2}|)+\cdots+|f_{n-1}|\,(|g_1|+\cdots+|g_{n-1}|) \qquad \text{(up)}\\
E^{\mathrm{rnd}} &= [|f_0|\,|g_{n-1}|+\cdots+(|f_0|+\cdots+|f_{n-1}|)\,|g_0|]\,C\,2^{-p} \qquad \text{(up)}
\end{aligned}$$

Intégration

$$\int \mathcal{B}_r(f_0+\cdots+f_{n-1}\,z^{n-1},K) = \mathcal{B}_r(f_1+\cdots+\tfrac{f_{n-2}}{n-1}\,z^{n-1},K\,r+\tfrac{|f_{n-1}|}{n}\,r^n+E^{\mathrm{rnd}})$$

Réduction de la surestimation

Exemple

$$\begin{aligned} f(x) &= (x-1)^2 \\ f^\bullet(x^\bullet) &= (x^\bullet)^2 -^\bullet 2\, x^\bullet +^\bullet 1 \end{aligned}$$

$$\begin{aligned} f^*(\mathcal{B}(x,\varepsilon)) &= \mathcal{B}(f(x), 2\,|x-1|\,\varepsilon + \mathcal{O}(\varepsilon^2)) \\ f^\bullet(\mathcal{B}(x,\varepsilon)) &= \mathcal{B}(f(x), 2\,|x|\,\varepsilon + 2\,\varepsilon + \mathcal{O}(\varepsilon^2)) \\ \chi_{f^\bullet}(x) &= \frac{|x|+1}{|x-1|} \end{aligned}$$

Idée : utiliser modèle de Taylor à l'ordre $\geqslant 2$

$$\begin{aligned} f^{\mathrm{Taylor}}(\mathcal{B}_r(x,0)) &= \mathcal{B}_r(y_0 + y_1\, t, \varepsilon) \\ f^\bullet(\mathcal{B}(x,r)) &= \mathcal{B}(y_0, |y_1|\, r + \varepsilon) \\ \chi_{f^\bullet}(x) &= 1 \end{aligned}$$

Problème

$$\begin{array}{rcll} Y' & = & P(Y), & Y=(Y_1,\ldots,Y_n), P\in\mathbb{Q}[Y]^n \\ Y(z_0) & = & C & z_0\in\mathbb{Q}[\mathrm{i}], C\in\mathcal{B}(\mathbb{D},\mathbb{D})^n \\ Y(z_1) & = & ? & z_1\in\mathbb{Q}[\mathrm{i}] \end{array}$$

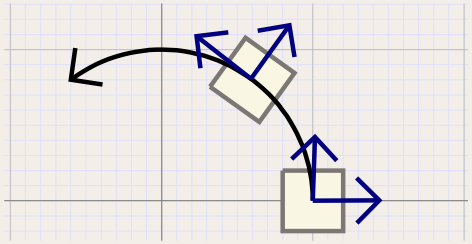
Algorithme

1. Pour $n\asymp p$ et après translation vers $z_0=0$, calculer
$$Y \;\approx\; Y_0+\cdots+Y_{n-1}\,z^{n-1}+\mathcal{O}(z^n).$$
2. Calculer K et $Y^\bullet=\mathcal{B}_{|z_1|}(Y_0+\cdots+Y_{n-1}\,z^n,K)$ avec
$$C+\int P(Y^\bullet) \;\subseteq\; Y^\bullet$$
En cas de succes, retourner $Y^\bullet(z_1)$
Calcul de K : itérer $Y^\bullet\mapsto C+\int P(Y^\bullet)$ en commençant par $Y^\bullet=Y_0+\cdots+Y_{n-1}\,z^n$, et grossir
3. Calculer $Y(z_1/2)$, puis $Y(z_1)$ en fonction de $Y(z_1/2)$

Effet d'enveloppement

Exemple

$$Y' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Y$$



Idée 1 : calculer la dependence en fonction de la condition initiale

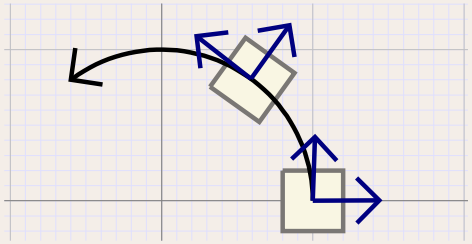
$$\begin{aligned} Y(z,\varepsilon) &= C + \varepsilon + \int_0^z P(Y(t,\varepsilon))\,\mathrm{d}t \\ J(z) = \frac{\partial Y}{\partial \varepsilon}(z,0) &= I + \int_0^z \frac{\partial P}{\partial Y}(Y(t,0))\,\frac{\partial Y}{\partial \varepsilon}(t,0)\,\mathrm{d}t \end{aligned}$$

Idée 2 : encadrements de l'erreur dans coordonnées déterminées par $\tilde{J} \approx J$

$$\begin{aligned} Y^\bullet(z) &= Y_{\mathrm{cen}}(z) + \tilde{J}(z)\,\mathcal{B}(0, Y_{\mathrm{rad}}(z)) \\ \tilde{J}_{21}\left(\tilde{J}_1\,\mathcal{B}_1 + E\right) &= \tilde{J}_{21}\,\tilde{J}_1\left(\mathcal{B}_1 + \tilde{J}_1^{-1}\,E\right) \\ &=: \tilde{J}_2\,\mathcal{B}_2 \end{aligned}$$

Exemple

Volterra



Idée 1 : calculer la dependence en fonction de la condition initiale

$$\begin{aligned} Y(z,\varepsilon) &= C+\varepsilon+\int_0^z P(Y(t,\varepsilon))\,\mathrm{d}t \\ J(z)=\frac{\partial Y}{\partial \varepsilon}(z,0) &= I+\int_0^z \frac{\partial P}{\partial Y}(Y(t,0))\,\frac{\partial Y}{\partial \varepsilon}(t,0)\,\mathrm{d}t \end{aligned}$$

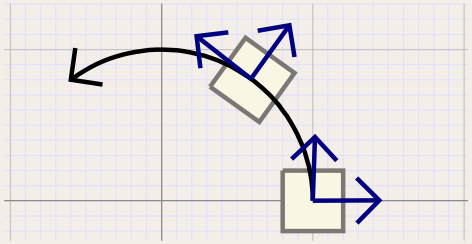
Idée 2 : encadrements de l'erreur dans coordonnées déterminées par $\tilde{J} \approx J$

$$\begin{aligned} Y^{\bullet}(z) &= Y_{\mathrm{cen}}(z)+\tilde{J}(z)\,\mathcal{B}(0,Y_{\mathrm{rad}}(z)) \\ \tilde{J}_{21}\left(\tilde{J}_1\,\mathcal{B}_1+E\right) &= \tilde{J}_{21}\,\tilde{J}_1\left(\mathcal{B}_1+\tilde{J}_1^{-1}\,E\right) \\ &=: \tilde{J}_2\,\mathcal{B}_2 \end{aligned}$$

Effet d'enveloppement

Exemple

$$Y' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Y$$



Idée 1 : calculer la dependence en fonction de la condition initiale

$$\begin{aligned} Y(z,\varepsilon) &= C + \varepsilon + \int_0^z P(Y(t,\varepsilon))\,\mathrm{d}t \\ J(z) = \frac{\partial Y}{\partial \varepsilon}(z,0) &= I + \int_0^z \frac{\partial P}{\partial Y}(Y(t,0))\,\frac{\partial Y}{\partial \varepsilon}(t,0)\,\mathrm{d}t \end{aligned}$$

Idée 2 : encadrements de l'erreur dans coordonnées déterminées par $\tilde{J} \approx J$

$$\begin{aligned} Y^\bullet(z) &= Y_{\mathrm{cen}}(z) + \tilde{J}(z)\,\mathcal{B}(0, Y_{\mathrm{rad}}(z)) \\ \tilde{J}_{21}\left(\tilde{J}_1\,\mathcal{B}_1 + E\right) &= \tilde{J}_{21}\,\tilde{J}_1\left(\mathcal{B}_1 + \tilde{J}_1^{-1}\,E\right) \\ &=: \tilde{J}_2\,\mathcal{B}_2 \end{aligned}$$

Variante pour modèles de Taylor

$$\{ f_0^\bullet + \cdots + f_{n-1}^\bullet\, z^{n-1} + \mathcal{B}_r(0,K)\, z^n \colon f_0^\bullet, \ldots, f_{n-1}^\bullet \in \mathcal{B}(\mathbb{D},\mathbb{D}), K \in \mathbb{D} \}$$

Avantages définition classique

- Multiplication presque aussi efficace que multiplication dans $\mathbb{D}[z]$

Avantages variante

- Pas essentiellement plus lent en précision multiple,
  si on calcule les erreurs en précision simple
- Borne plus fine (par exemple sur $\mathcal{B}(0,s)$ avec $s<r$)
- Parfois de meilleure qualité :

$$\begin{aligned} & \int f_0^\bullet + \cdots + f_{n-1}^\bullet\, z^{n-1} + \mathcal{B}_r(0,K)\, z^n \\ = \;& f_1^\bullet + \cdots + \frac{f_{n-2}^\bullet}{n-1}\, z^{n-1} + \mathcal{B}(0, \frac{\lceil f_{n-1}^\bullet \rceil}{n} + \frac{K}{n+1}) \end{aligned}$$

- Ne nécessite pas une précision $p \geqslant c\, n$ pour être précis

Qualité des estimations

$$\begin{aligned} \varphi := f_0 + \cdots + f_{n-1}\, z^{n-1} &\in f^\bullet_{;n} \quad \text{(donnée)} \\ \varepsilon\, z^n := f_n\, z^n + \cdots &\in f^\bullet_{n;} \quad \text{(à calculer)} \end{aligned}$$

$$\begin{aligned} \Phi(f) &= C + \textstyle\int P(f) \\ \Phi(\varphi^\bullet + \varepsilon^\bullet\, z^n) &\subseteq \varphi^\bullet + \varepsilon^\bullet\, z^n \\ \Phi(\varphi^\bullet) &\subseteq \varphi^\bullet + \delta^\bullet\, z^n \end{aligned}$$

$$\begin{aligned} \Phi(\varphi^\bullet + \varepsilon^\bullet\, z^n) &= \Phi(\varphi^\bullet) + J_\Phi(\varphi^\bullet)\, \varepsilon^\bullet\, z^n + \mathcal{O}((\varepsilon^\bullet\, z^n)^2) \\ &\subseteq \varphi^\bullet + \delta^\bullet\, z^n + \tfrac{r}{n}\, J_P(\varphi^\bullet)\, \varepsilon^\bullet\, z^n \\ \delta^\bullet + \tfrac{r}{n}\, J_P(\varphi^\bullet)\, \varepsilon^\bullet &\subseteq \varepsilon^\bullet \end{aligned}$$

$$\boxed{\varepsilon^\bullet \subseteq \frac{\delta^\bullet}{1 - \left\| \frac{r}{n}\, J_P(\varphi^\bullet) \right\|}}$$

Racines d'un polynôme

```
Mmx] use "analyziz"; include "graphix/points.mmx";
```

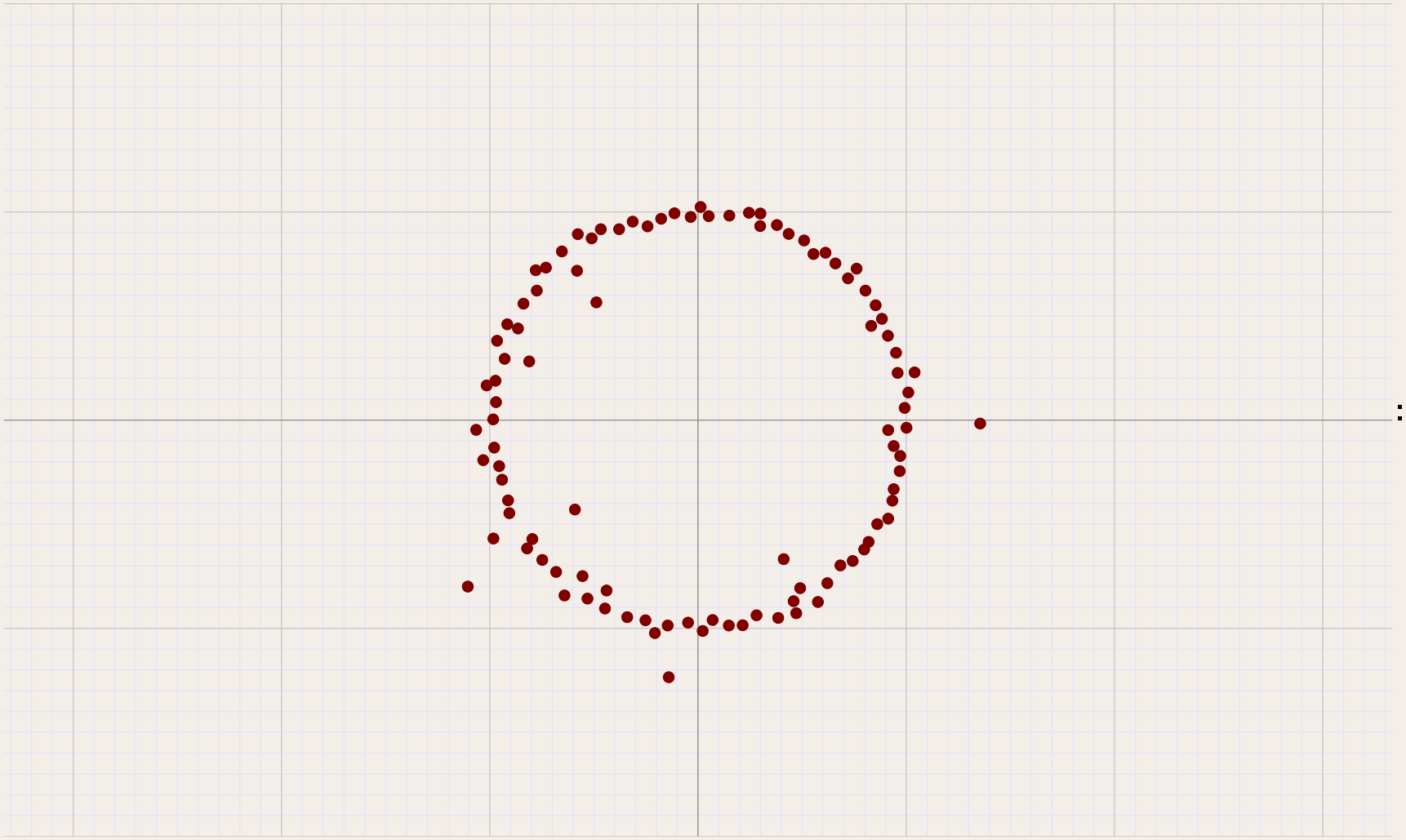
Computed in 33 ms

```
Mmx] pi == 4.0 * arctan 1.0;
```

```
Mmx] rnd () == exp (complex (0.0, uniform_deviate (0.0, 2*pi)));
```

```
Mmx] p == polynomial (rnd () | i in 0 to 100);
```

```
Mmx] $points roots p
```



Compound

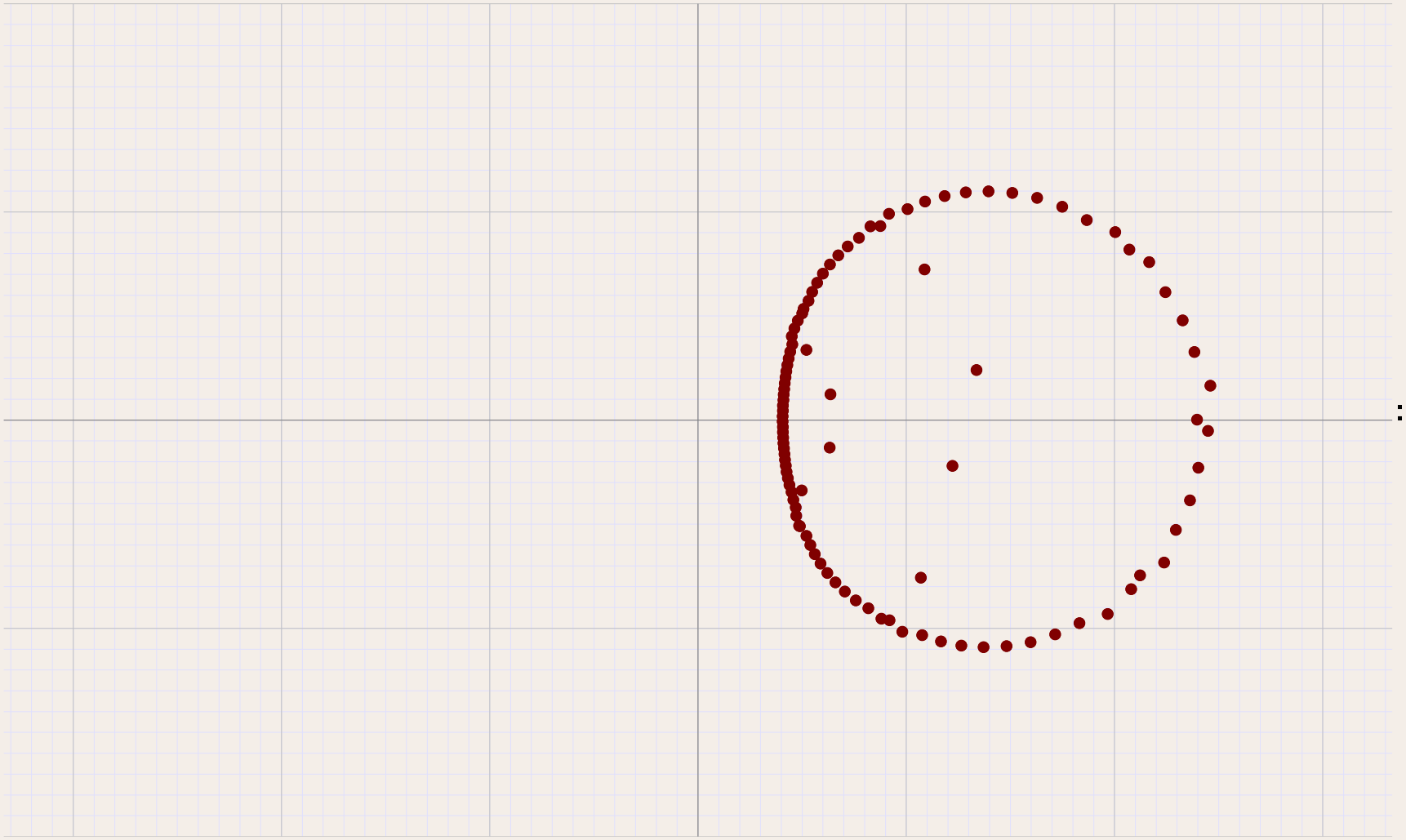
Computed in 454 ms

```
Mmx]
```

Racines d'un polynôme

```
Mmx] p == poly (1.0, -1.0)^100;
```

```
Mmx] $points (roots p)
```



Compound

Computed in 639 ms

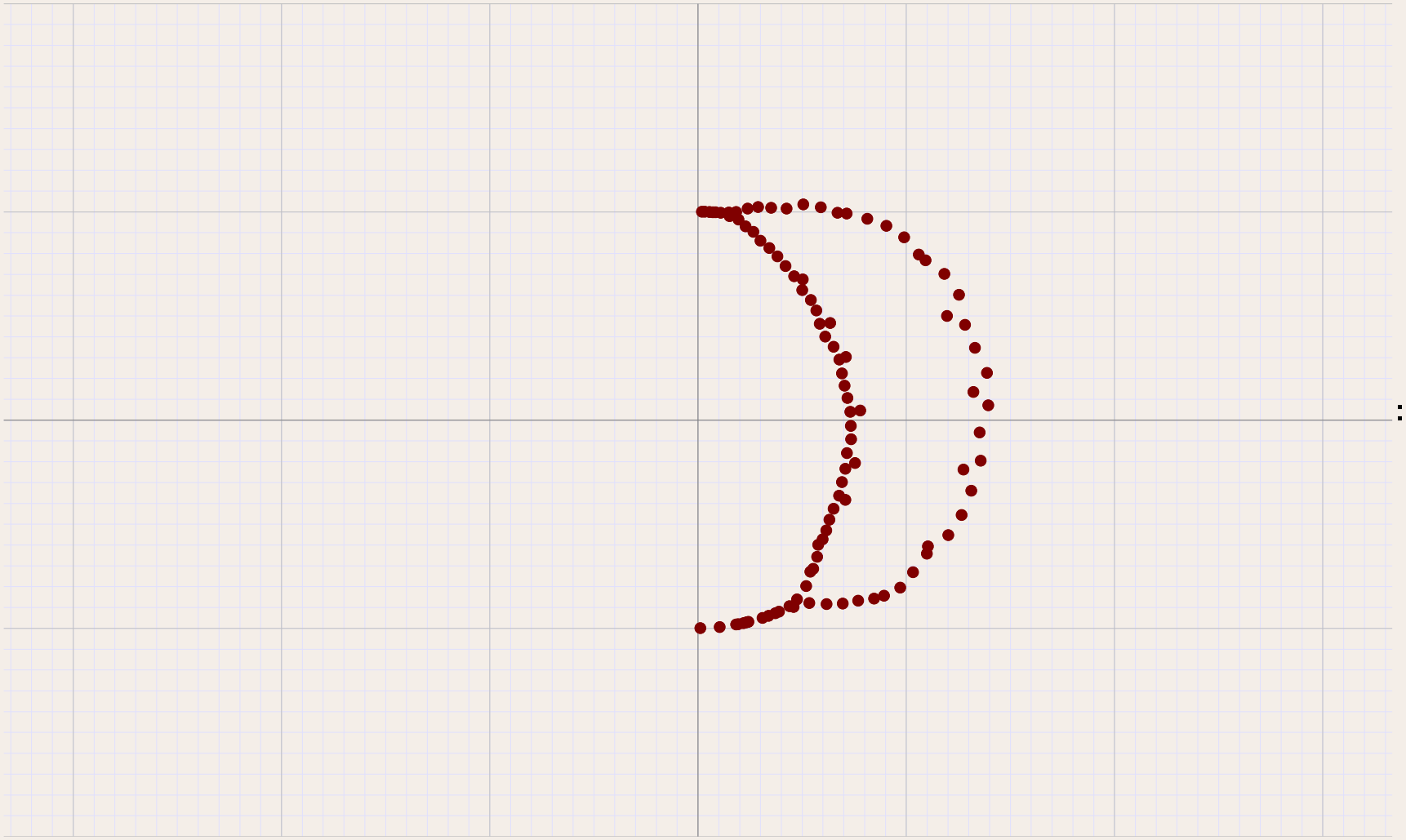
```
Mmx]
```

Racines d'un polynôme

```
Mmx] v == [ rnd () | i in 1 to 100 ];
Mmx] v == [ sqrt rnd () | i in 1 to 100 ];
Mmx] p == annulator v;
```

Computed in 18 ms

```
Mmx] $points (roots p)
```



Compound

Computed in 641 ms

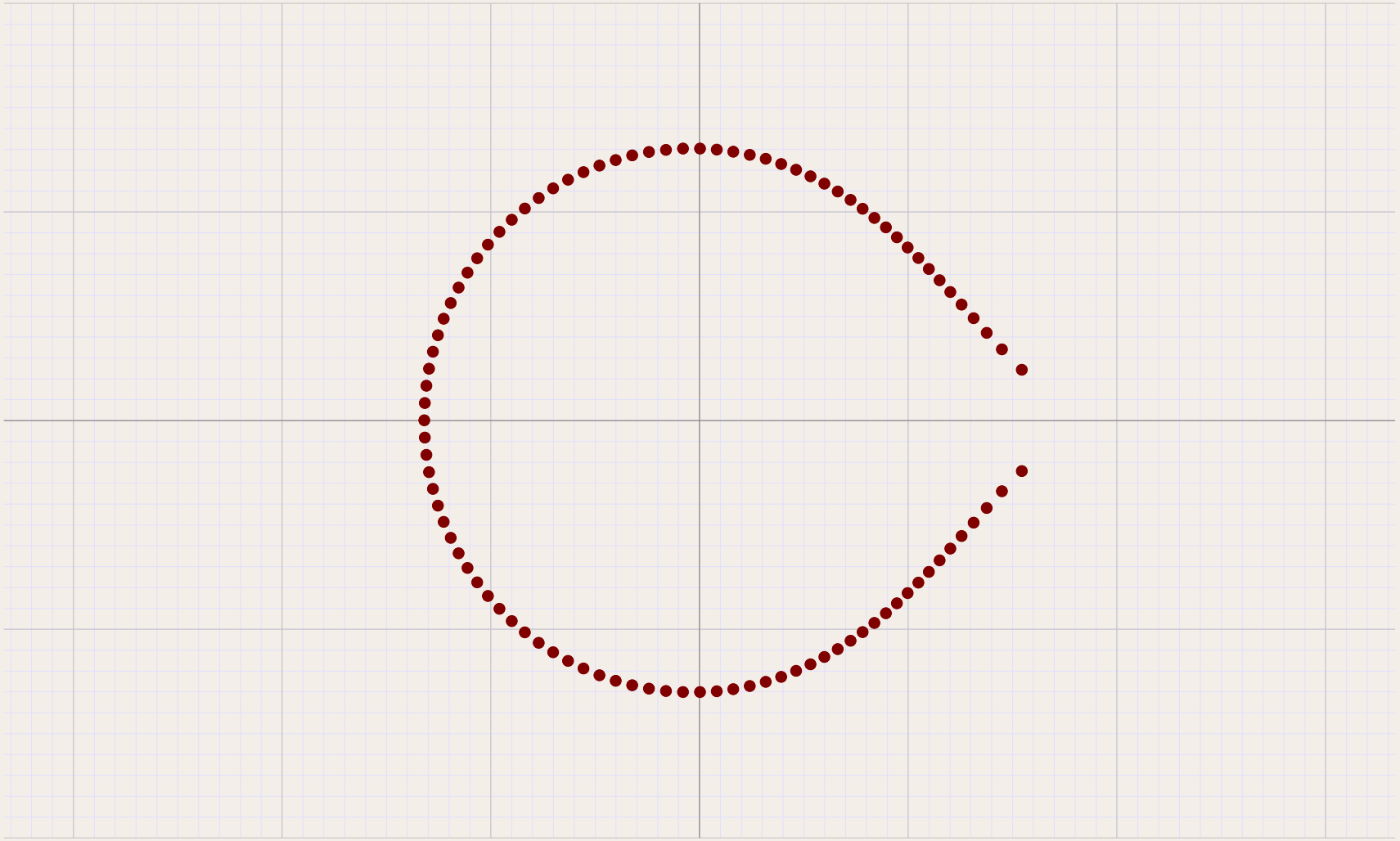
```
Mmx]
```

Racines d'un polynôme

```
Mmx] z == series (0.0, 1.0);
```

```
Mmx] B == exp (exp z - 1);
```

```
Mmx] p == B[0,100];
Mmx] $points (0.5 * roots p)
```



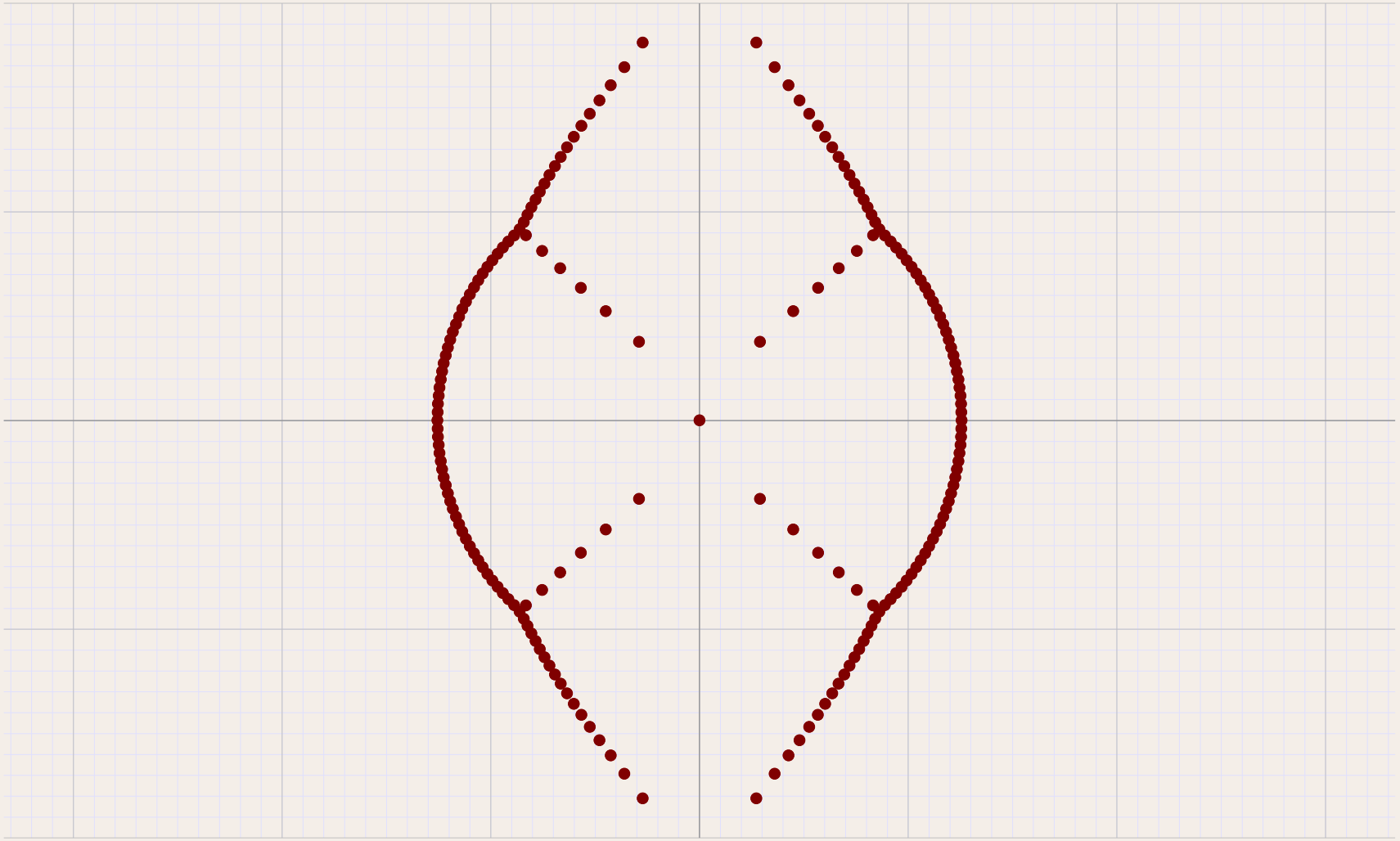
```
Mmx]
```

Racines d'un polynôme

```
Mmx] z == series (0.0, 1.0);
```

```
Mmx] f == integrate exp (-z*z);
```

```
Mmx] p == f[0,200];
Mmx] $points (0.2 * roots p)
```



```
Mmx]
```

Stabilité numérique

Meilleur conditionnement

$$\begin{aligned} P(z) &= z^n - 1 \\ z_k &= \mathrm{e}^{2\pi \mathrm{i} k/n} \end{aligned}$$

Pire conditionnement

$$\begin{aligned} P(z) &= (z-1)^n \\ z_k &= 1 \end{aligned}$$

Meilleur conditionnement

$$\begin{aligned} P(z) &= z^n - 1 + E(z) \\ z_k &= \mathrm{e}^{2\pi \mathrm{i} k/n} + O(n \, \|E\|) \\ \|E\| &= \sup_{|z| \leqslant 1} \|E(z)\| \end{aligned}$$

Pire conditionnement

$$\begin{aligned} P(z) &= (z-1)^n \\ z_k &= 1 \end{aligned}$$

Meilleur conditionnement

$$\begin{aligned} P(z) &= z^n - 1 + E(z) \\ z_k &= \mathrm{e}^{2\pi \mathrm{i} k/n} + O(n\,\|E\|) \\ \|E\| &= \sup_{|z|\leqslant 1} \|E(z)\| \end{aligned}$$

Pire conditionnement

$$\begin{aligned} P(z) &= (z-1)^n + E(z) \\ z_k &= 1 + O\big(\sqrt[n]{\|E\|}\,\big) \end{aligned}$$

Itération d'Aberth (Bini, Fiorentino)

Entrées

- $P = P_n\, z^n + \cdots + P_0 \in \mathbb{C}[z]$
- $z_1, \ldots, z_n \in \mathbb{C}$ (on peut commencer avec $z_k = \mathrm{e}^{2\pi i k/n}$)

Idée

Pour chaque k appliquer la méthode de Newton sur

$$f(z) \;=\; \frac{P(z)}{\prod_{j\neq k}(z - z_j)}$$

Itération

$$z'_k \;:=\; z_k - \frac{P(z_k)}{P'(z_k) - P(z_k)\sum_{j\neq k}\frac{1}{z_k - z_j}}$$

Transformation de Graeffe

Définition

$$\begin{aligned} P(z) &= P_{\text{pair}}(z^2) + P_{\text{imp}}(z^2)\, z \\ G(P)(z) &= P_{\text{pair}}(z)^2 - P_{\text{imp}}(z)^2\, z \end{aligned}$$

Propriété fondamentale

$$\begin{aligned} P_{\text{pair}}(z^2) &= \frac{1}{2}\left(P(z) + P(-z)\right) \\ P_{\text{imp}}(z^2) &= \frac{1}{2\,z}\left(P(z) - P(-z)\right) \\ G(P)(z^2) &= \frac{1}{4}\left((P(z) + P(-z))^2 - (P(z) - P(-z))^2\right) \\ &= P(z)\,P(-z) \end{aligned}$$

Racines 2^p-ièmes en utilisant les nombres tangents dans $\mathbb{C}[\epsilon]\,/\,(\epsilon^2)$

$$\begin{aligned} P(z) &\rightsquigarrow P(z-\epsilon) = P(z) - P'(z)\,\epsilon \\ (z+\epsilon)^{2^k} &= z^{2^k} + 2^k\, z^{2^k-1}\,\epsilon = u + v\,\epsilon \\ z &= \frac{u}{2^k\, v} \end{aligned}$$

Transformation de Graeffe

Définition

$$\begin{aligned} P(z) &= P_{\text{pair}}(z^2) + P_{\text{imp}}(z^2)\, z \\ G(P)(z) &= P_{\text{pair}}(z)^2 - P_{\text{imp}}(z)^2\, z \end{aligned}$$

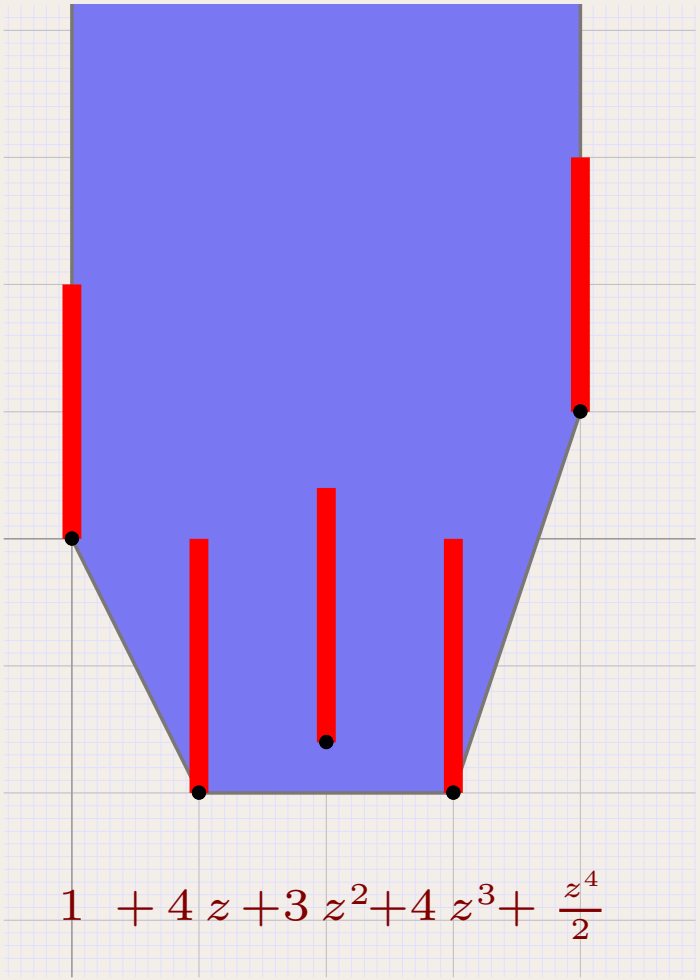
Propriété fondamentale

$$\begin{aligned} \deg P &= \deg G(P) \\ P(z) = 0 &\Rightarrow G(P)(z^2) = 0 \end{aligned}$$

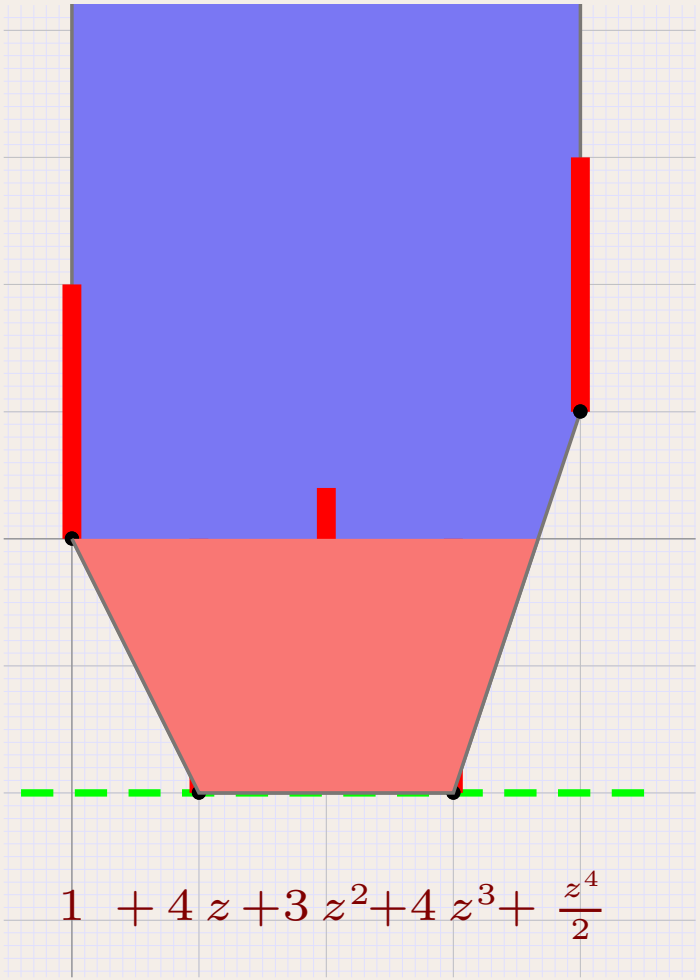
Racines 2^p-ièmes en utilisant les nombres tangents dans $\mathbb{C}[\epsilon]/(\epsilon^2)$

$$\begin{aligned} P(z) &\rightsquigarrow P(z-\epsilon) = P(z) - P'(z)\,\epsilon \\ (z+\epsilon)^{2^k} &= z^{2^k} + 2^k\, z^{2^k-1}\,\epsilon = u + v\,\epsilon \\ z &= \frac{u}{2^k\, v} \end{aligned}$$

Polygone numérique de Newton

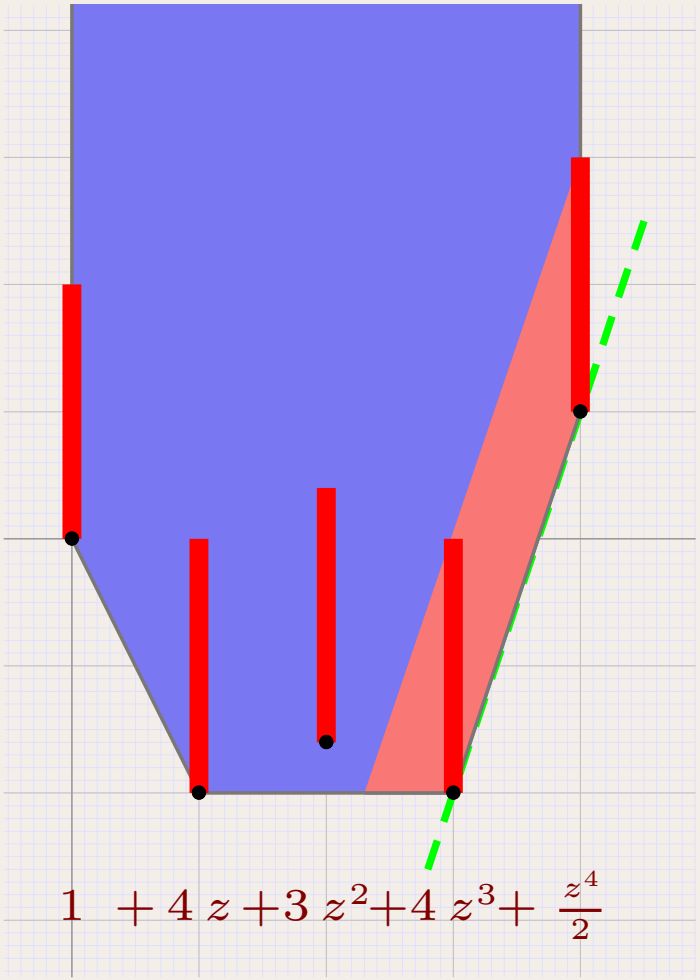


Polygone numérique de Newton



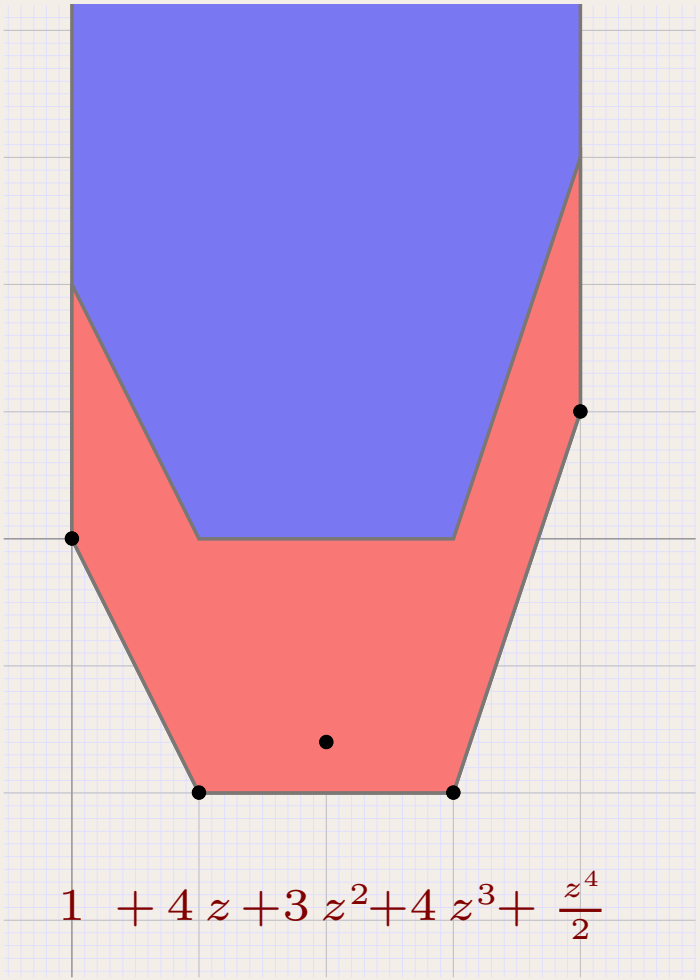
Évaluation en $|z| = 1$

Polygone numérique de Newton



Évaluation en $|z| = 8$

Polygone numérique de Newton

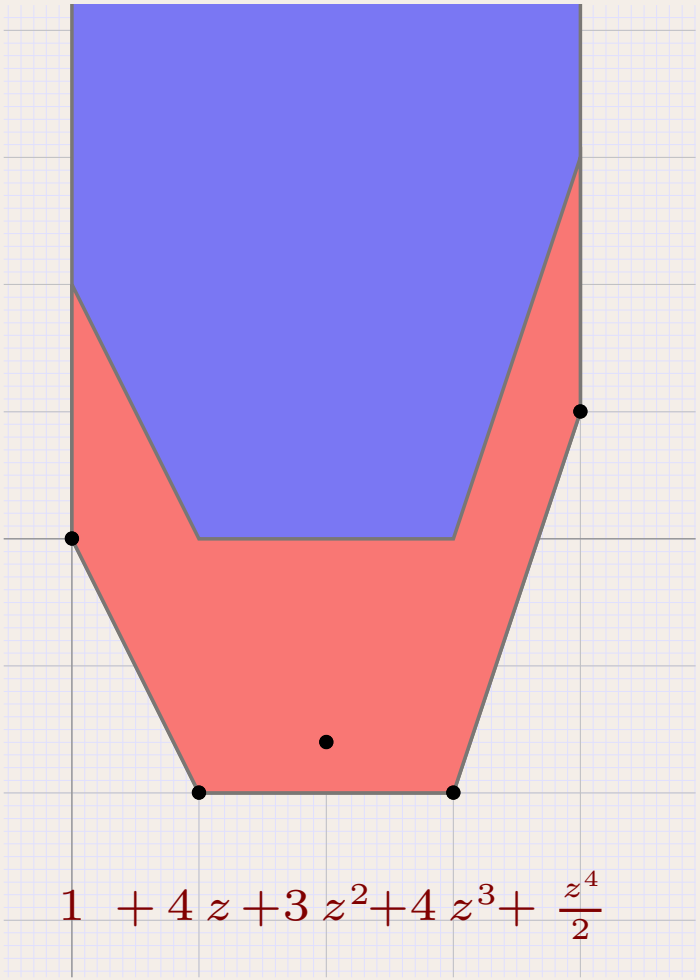


Polygone de Newton

⇕

Comportement en évaluation

Polygone numérique de Newton



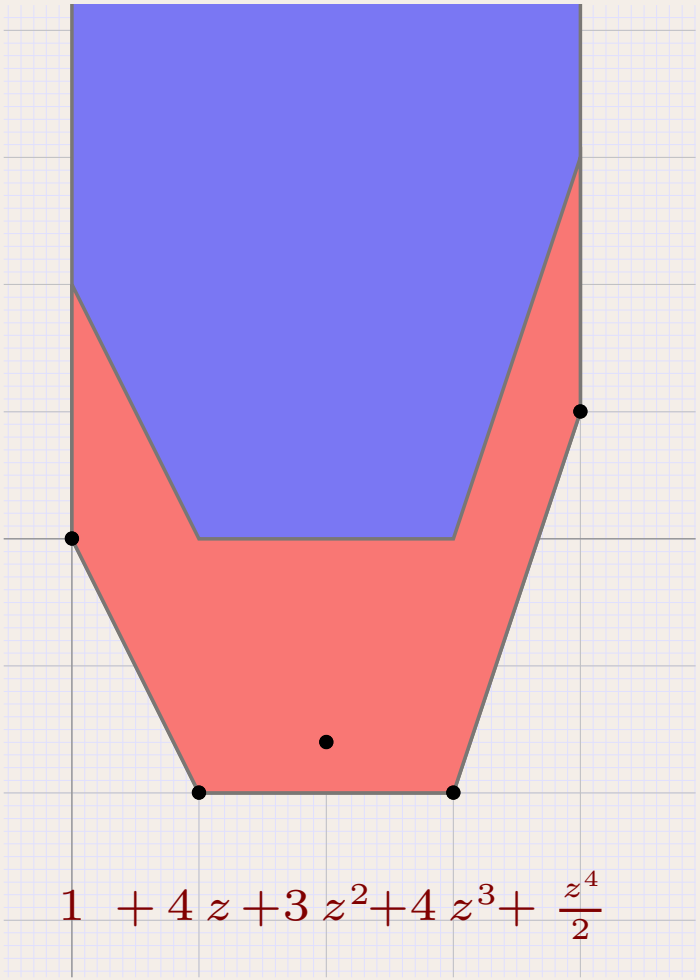
Pentes du polygone de Newton

⇕

Modules des racines

$$
\begin{array}{lcl|lcl}
z_1 & \approx & -0.289 & |z_1| & \approx & 1/4 \\
z_2 & \approx & -0.193 - 0.952\,\mathrm{i} & |z_2| & \approx & 1 \\
z_3 & \approx & -0.193 + 0.952\,\mathrm{i} & |z_3| & \approx & 1 \\
z_4 & \approx & -7.325 & |z_4| & \approx & 8
\end{array}
$$

Polygone numérique de Newton



Pentes du polygone de Newton

$\wr$

Modules des racines

$$\begin{array}{lcl|lcl} z_1 & \approx & -0.289 & |z_1| & \approx & 1/4 \\ z_2 & \approx & -0.193 - 0.952\,\mathrm{i} & |z_2| & \approx & 1 \\ z_3 & \approx & -0.193 + 0.952\,\mathrm{i} & |z_3| & \approx & 1 \\ z_4 & \approx & -7.325 & |z_4| & \approx & 8 \end{array}$$

Question ouverte abordable

Pentes : $\alpha_1 \leqslant \cdots \leqslant \alpha_n$

Racines : $|z_1| \leqslant \cdots \leqslant |z_n|$

$$|\log_2 |z_k| - \alpha_k| \leqslant c \log n$$

pour une certaine constante $c \geqslant 1$

Dilemme fondamental

Problème

Meilleure approximation possible des racines pour précision p donnée
(Perturbation relative des coefficients par des facteurs $\leqslant 2^{-p}$ permise)

Arithmétique naïve en précision machine

Espoir : algorithme en temps $C\,n^2$ avec C petit

Arithmétique rapide en précision multiple

Nécessite une précision d'au moins $p \geqslant n$
Espoir : algorithme en temps $C\,\mathsf{I}((p+n)\,n)\log^{O(1)} n$, avec C pas trop grand

Théorème. (Schönhage, Gourdon) *Pour $P \in \mathbb{Z}[z]\,2^{-p}$ avec $\|P\| \leqslant 1$, on peut calculer en temps $\mathcal{O}(\mathsf{I}((p+n\log n)\,n)\,n)$ des nombres $a_k, b_k \in \mathbb{Z}\,2^{-p}$ avec*

$$\|P - (a_1 + b_1\,z)\cdots(a_n + b_n\,z)\| \;\leqslant\; 2^{-p}$$

Dilemme fondamental

Problème

Meilleure approximation possible des racines pour précision p donnée
(Perturbation relative des coefficients par des facteurs $\leqslant 2^{-p}$ permise)

Arithmétique naïve en précision machine

Réaliste : algorithme en temps $C\,K_{\kappa,n}\,n^2$ avec C petit

Arithmétique rapide en précision multiple

Nécessite une précision d'au moins $p \geqslant n$
Réaliste : algorithme en temps $C\,K_{\kappa,n}\,\mathsf{I}((p+n)\,n)\log^{O(1)} n$, avec C pas trop grand

Théorème. (Schönhage, Gourdon) *Pour $P \in \mathbb{Z}[z]\,2^{-p}$ avec $\|P\| \leqslant 1$, on peut calculer en temps $\mathcal{O}(\mathsf{I}((p+n\log n)\,n)\,n)$ des nombres $a_k, b_k \in \mathbb{Z}\,2^{-p}$ avec*

$$\|P - (a_1 + b_1\,z)\cdots(a_n + b_n\,z)\| \;\leqslant\; 2^{-p}$$

Évaluation multipoint rapide

Arithmétique naïve en précision machine

n fois Horner : $\mathsf{E}(n,p) = \mathcal{O}(\mathsf{I}(p)\, n^2)$

Arithmétique rapide en précision multiple

$\mathsf{E}(n,p) = \mathcal{O}(\mathsf{I}((p+n)\, n) \log n)$

Algorithme intermédiaire

$\mathsf{E}(n,p) = \mathcal{O}(\mathsf{I}(n^{3/2}\, p^{3/2} \log^3 n))$ (meilleur si $p \ll \sqrt[3]{n}$)

Question ouverte

Peut-on faire mieux pour $p = o(n)$?

$$f\colon \mathbb{C}^n \to \mathbb{C}^n, \qquad \mathcal{B}(z,r) \in \mathcal{B}(\mathbb{C}^n, \mathbb{R}^n), \qquad V \approx J_f(z)^{-1}$$
$$K(\mathcal{B}(z,r)) \;=\; z - Vf(z) + (1 - VJ_f(\mathcal{B}(z,r)))\,\mathcal{B}(0,r)$$

Théorème. *Si* $K(\mathcal{B}(z,r)) \subseteq \mathcal{B}(z,r)$, *alors* $f(u) = 0$ *pour un certain* $u \in \mathcal{B}(z,r)$.

Démonstration. Soit $g(z) = z - Vf(z)$. Pour $u \in \mathcal{B}(z,r)$, on a

$$\begin{aligned} g(u) &= g(z) + \int_0^1 J_g(z + (u-z)\,t)\,(u-z)\,\mathrm{d}t \\ &\subseteq g(z) + J_g(\mathcal{B}(z,r))\,\mathcal{B}(0,r), \end{aligned}$$

puisque $J_g(\mathcal{B}(z,r))$ est convexe. Donc

$$g(\mathcal{B}(z,r)) \;\subseteq\; g(z) + J_g(\mathcal{B}(z,r))\,\mathcal{B}(0,r) \;\subseteq\; \mathcal{B}(z,r),$$

donc g admet un point fixe, grace au théorème de Brouwer. □

Certification par la méthode de Krawczyk/Rump

$$f\colon \mathbb{C}^n \to \mathbb{C}^n, \qquad \mathcal{B}(z,r) \in \mathcal{B}(\mathbb{C}^n, \mathbb{R}^n), \qquad V \approx J_f(z)^{-1}$$

$$K(\mathcal{B}(z,r)) \;=\; z - Vf(z) + (1 - VJ_f(\mathcal{B}(z,r)))\,\mathcal{B}(0,r)$$

Théorème. *Si* $K(\mathcal{B}(z,r)) \subseteq \mathcal{B}(z,r)$, *alors* $f(u) = 0$ *pour un certain* $u \in \mathcal{B}(z,r)$.

Théorème. *Si* $K(\mathcal{B}(z,r)) \subseteq \operatorname{int} \mathcal{B}(z,r)$, *alors* $f(u) = 0$ *pour un unique* $u \in \mathcal{B}(z,r)$.

Certification par la méthode de Krawczyk/Rump

$$f\colon \mathbb{C}^n \to \mathbb{C}^n, \qquad \mathcal{B}(z,r) \in \mathcal{B}(\mathbb{C}^n, \mathbb{R}^n), \qquad V \approx J_f(z)^{-1}$$

$$K(\mathcal{B}(z,r)) \;=\; z - Vf(z) + (1 - VJ_f(\mathcal{B}(z,r)))\,\mathcal{B}(0,r)$$

Théorème. *Si* $K(\mathcal{B}(z,r)) \subseteq \mathcal{B}(z,r)$, *alors* $f(u) = 0$ *pour un certain* $u \in \mathcal{B}(z,r)$.

Théorème. *Si* $K(\mathcal{B}(z,r)) \subseteq \operatorname{int} \mathcal{B}(z,r)$, *alors* $f(u) = 0$ *pour un unique* $u \in \mathcal{B}(z,r)$.

Pour trouver r, faire

$$\begin{aligned} r_0 &= 0 \\ r_{k+1} &= (1+\varepsilon) \max\left(r_k, \operatorname{rad} K(z, r_k)\right) \end{aligned}$$

Problème

$$P(\sigma) \;\approx\; (z-\sigma)^{\mu} + P_{\mu+1}\,(z-\sigma)^{\mu+1} + \cdots + P_n\,(z-\sigma)^n$$

Comment montrer que P admet exactement μ racines sur $\mathcal{B}(\sigma, r)$?

Réponse *via* les modèles de Taylor

Prendre $\boldsymbol{u} = \mathcal{B}_r(\sigma + z, 0) \in \mathcal{B}_r(\mathbb{C}[z]_{\leqslant \nu}, \mathbb{R})$ pour $\nu \geqslant \mu$ et évaluer

$$\boldsymbol{v} \;=\; P(\boldsymbol{u}) = \mathcal{B}_r(Q_0 + \cdots + Q_\nu\, z^\nu, \varepsilon).$$

Montrer que tout $\tilde{P} \in \boldsymbol{v}$ admet μ racines dans $\mathcal{B}(0, r)$.

Par exemple

$\varepsilon + |Q_0| + \cdots + |Q_{\mu-1}|\, r^{\mu-1} + |Q_{\mu-1}|\, r^{\mu+1} + \cdots + |Q_\nu|\, r^\nu < |Q_\mu|\, r^\mu$ et Rouché

$$P(x,y) \quad \begin{cases} x^2+2\,x\,y-y^2-3\,x+5\,y+8=0 \\ 3\,x^2-x\,y+y^2+8\,x-2\,y+7=0 \end{cases}$$

$$\text{Fastoche}(x,y) \quad \begin{cases} x^2-1=0 \\ y^2-1=0 \end{cases}$$

$$H(x,y,t) \quad \begin{cases} (x^2-1)\,t+(x^2+2\,x\,y-y^2-3\,x+5\,y+8)\,(1-t)=0 \\ (y^2-1)\,t+(3\,x^2-x\,y+y^2+8\,x-2\,y+7)\,(1-t)=0 \end{cases}$$

Références

Numérique : Drexler 77, Morgan 87, Verschelde 96, Sommese-Wampler 05, etc.
Théorique : Shub-Smale, Pardo, Dedieu, etc.
Algébrique : Giusti-Heintz-Morais-Pardo 95, Lecerf 01, Durvye 08

$$P(x,y) \quad \begin{cases} x^2+2\,x\,y-y^2-3\,x+5\,y+8=0 \\ 3\,x^2-x\,y+y^2+8\,x-2\,y+7=0 \end{cases}$$

$$\text{Fastoche}(x,y) \quad \begin{cases} x^2-1=0 \\ y^2-1=0 \end{cases}$$

$$H(x,y,t) \quad \begin{cases} (x^2-1)\,t+(x^2+2\,x\,y-y^2-3\,x+5\,y+8)\,(1-t)=0 \\ (y^2-1)\,t+(3\,x^2-x\,y+y^2+8\,x-2\,y+7)\,(1-t)=0 \end{cases}$$

Exemples...

Solutions à l'infini

$$\begin{aligned} P_1 &= x^2 - 2\,x \\ P_2 &= x\,y - 2 \end{aligned}$$

$$\begin{aligned} P_1 &= x^2 - 2\,x\,z \\ P_2 &= x\,y - 2\,z^2 \\ P_3 &= 3\,x - 5\,y + 7\,z - 10 \end{aligned}$$

Solutions multiples

$$x_t, y_t, z_t \in \mathbb{C}\left(\left(t^{1/\kappa}\right)\right)$$

Méthode « préducteur-correcteur »

$$
\begin{aligned}
H(z,t) &\approx 0 \\
H(z+\mathrm{d}z, t+\mathrm{d}t) &\approx 0 \\
\mathrm{d}z &= -\frac{\partial H}{\partial z}(z,t)^{-1}\left(H(z,t)+\frac{\partial H}{\partial t}(z,t)\,\mathrm{d}t\right) && \text{(prédiction)} \\
\mathrm{d}z &\mathrel{+}= -\frac{\partial H}{\partial z}(z,t)^{-1}\,H(z+\mathrm{d}z, t+\mathrm{d}t) && \text{(correction)}
\end{aligned}
$$

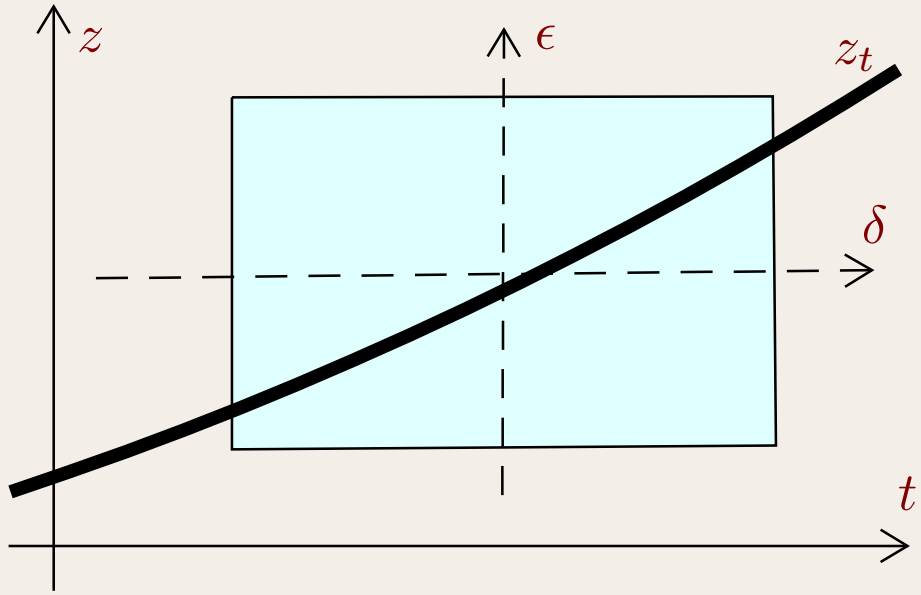
Contrôle de pas

$$
\begin{aligned}
\mathrm{d}t &:= \lambda\,\mathrm{d}t \ \ (\lambda>1), \text{ si pas accepté} \\
\mathrm{d}t &:= \alpha\,\mathrm{d}t, \text{ sinon}
\end{aligned}
$$

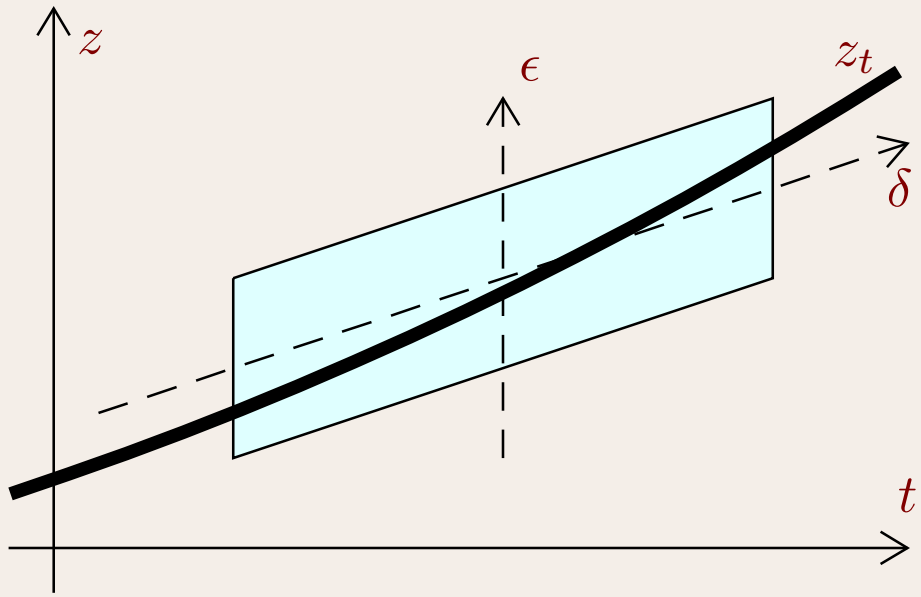
Critère numérique d'acceptation

$$
\left\| \frac{\partial H}{\partial z}(z,t)^{-1}\,\frac{\partial H}{\partial z}(z+\mathrm{d}z, t+\mathrm{d}t) - 1 \right\| \leqslant \text{seuil}
$$

Krawczyk-Rump uniforme



Modèles de Taylor (ordre $\leqslant 1$ en z et t)



Racines multiples

Idée : prendre un paquet de chemins « conjugués »

$$\begin{aligned} z_t^k &= \varphi\big(\mathrm{e}^{2\pi \mathrm{i} k/\kappa}\, t\big) \\ \varphi &\in \mathbb{C}\big(\big(t^{1/\kappa}\big)\big)^n. \end{aligned}$$

Considérer $\mathcal{Z}_t = \{z_t^1, \ldots, z_t^\kappa\}$ comme « chemin » avec idéal $\mathfrak{I}_t$

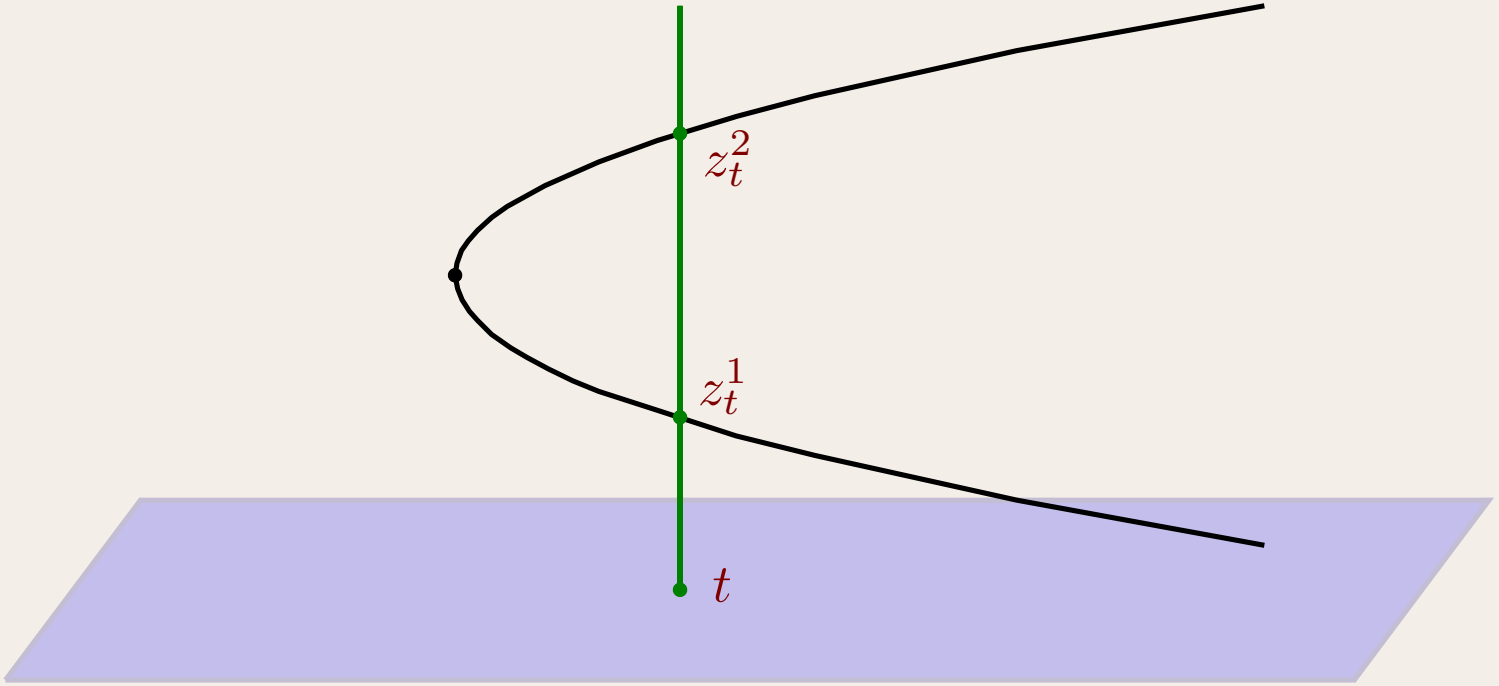
Représentation de $\mathfrak{I}_t$ (en position générale)

$$\begin{cases} (z_{t,1})^\kappa - U_{t,1}(z_{t,1}) = (z_{t,1} - z_{t,1}^1) \cdots (z_{t,1} - z_{t,1}^\kappa) \\ z_{t,2} - U_{t,2}(z_{t,1}) \\ \vdots \\ z_{t,n} - U_{t,n}(z_{t,1}) \end{cases}$$

Remonter l'homotopie H

Évaluer H en $(u, U_{t,2}(u), \ldots, U_{t,n}, t) \in \mathbb{A}^n \times \mathbb{C}$ avec $\mathbb{A} = \mathbb{C}[u]/(u^r - U_{t,1}(u))$

Exemple



$$
\begin{aligned}
P(z,t) &= 0 \\
\mathbb{A}_{\alpha,\beta} &= \mathbb{C}[u]/((u-\alpha)(u-\beta)) \\
P(u,t) &\in \mathbb{A}_{\alpha,\beta} \\
P(u,t)=0 &\Leftrightarrow P(\alpha,t)=0 \wedge P(\beta,t)=0
\end{aligned}
$$