Multiplication rapide I

Joris van der Hoeven

CNRS, École polytechnique

JNCF, Luminy

28 février, 2022

Motivation I

La multiplication comme brique de base pour implanter d'autres opérations

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une série formelle

$$f = 1 + f_1 z + \cdots + f_{n-1} z^{n-1} + O(z^n)$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une série formelle

$$f = 1 + f_1 z + \cdots + f_{m-1} z^{m-1} + f_m z^m + \cdots + f_{n-1} z^{n-1} + O(z^n), \qquad m = \left\lceil \frac{n}{2} \right\rceil$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une série formelle

$$\begin{aligned} f &= 1 + f_1 z + \cdots + f_{m-1} z^{m-1} + f_m z^m + \cdots + f_{n-1} z^{n-1} + O(z^n), \qquad m = \left\lceil \frac{n}{2} \right\rceil \\ g &= f^{-1} + O(z^m) \\ h = fg &= 1 \qquad\qquad + h_m z^m + \cdots + h_{n-1} z^{n-1} + O(z^n) \end{aligned}$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une série formelle

$$
\begin{aligned}
f &= 1 + f_1 z + \cdots + f_{m-1} z^{m-1} + f_m z^m + \cdots + f_{n-1} z^{n-1} + O(z^n), \qquad m = \left\lceil \frac{n}{2} \right\rceil \\
g &= f^{-1} + O(z^m) \\
h = fg &= 1 + h_m z^m + \cdots + h_{n-1} z^{n-1} + O(z^n) \\
h^{-1} &= 1 - h_m z^m - \cdots - h_{n-1} z^{n-1} + O(z^n) \\
f^{-1} &= g h^{-1} + O(z^n)
\end{aligned}
$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une série formelle

$$f = 1 + f_1 z + \cdots + f_{m-1} z^{m-1} + f_m z^m + \cdots + f_{n-1} z^{n-1} + O(z^n), \qquad m = \left\lceil \frac{n}{2} \right\rceil$$

$$g = f^{-1} + O(z^m)$$

$$\begin{aligned} h = fg &= 1 + h_m z^m + \cdots + h_{n-1} z^{n-1} + O(z^n) \\ h^{-1} &= 1 - h_m z^m - \cdots - h_{n-1} z^{n-1} + O(z^n) \end{aligned}$$

$$f^{-1} = g h^{-1} + O(z^n)$$

$\mathsf{M}(n)$: coût de multiplication de deux polynômes de degré n

$$\mathsf{T}(n) \leqslant \mathsf{T}(m) + 2\,\mathsf{M}(n) + O(n)$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une série formelle

$$f = 1 + f_1 z + \cdots + f_{m-1} z^{m-1} + f_m z^m + \cdots + f_{n-1} z^{n-1} + O(z^n), \qquad m = \left\lceil \frac{n}{2} \right\rceil$$

$$g = f^{-1} + O(z^m)$$

$$h = fg = 1 + h_m z^m + \cdots + h_{n-1} z^{n-1} + O(z^n)$$

$$h^{-1} = 1 - h_m z^m - \cdots - h_{n-1} z^{n-1} + O(z^n)$$

$$f^{-1} = g h^{-1} + O(z^n)$$

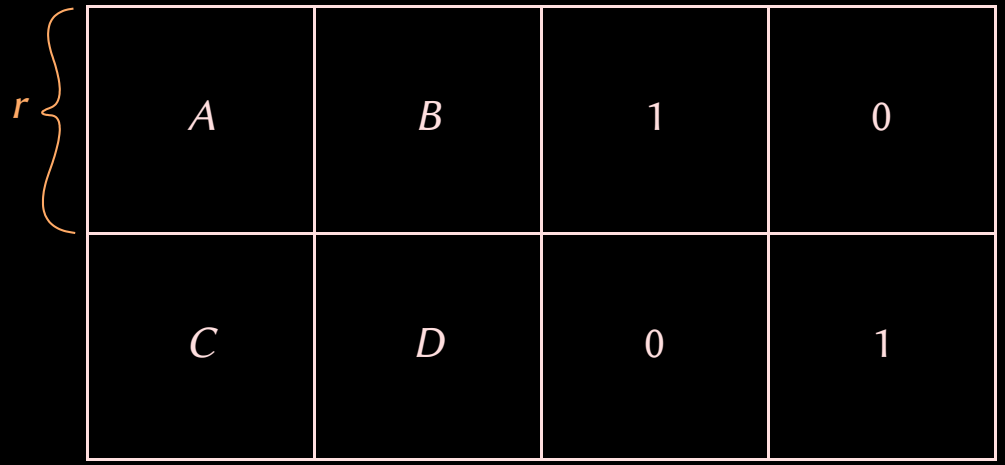
$\mathrm{M}(n)$: coût de multiplication de deux polynômes de degré n

$$\mathrm{T}(n) \leqslant \mathrm{T}(m) + 2\,\mathrm{M}(n) + O(n)$$

$$\mathrm{T}(n) = O(\mathrm{M}(n))$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice



$\Omega(r)$: coût pour multiplier deux matrices $r \times r$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

$A^{-1}A$	$A^{-1}B$	A^{-1}	0
C	D	0	1

$$\mathsf{T}(r) + \Omega(r)$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	$\tilde{B}$	A^{-1}	0
C	D	0	1

$\mathsf{T}(r) + \Omega(r)$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	$\tilde{B}$	A^{-1}	0
$C - C1$	$D - C\tilde{B}$	CA^{-1}	1

$$\mathsf{T}(r) + 3\,\Omega(r)$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	$\tilde{B}$	A^{-1}	0
0	$\tilde{D}$	CA^{-1}	1

$\mathsf{T}(r) + 3\,\Omega(r)$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	$\tilde{B}$	A^{-1}	0
0	$\tilde{D}^{-1}\tilde{D}$	$\tilde{D}^{-1}CA^{-1}$	$\tilde{D}^{-1}$

$$2\,\mathsf{T}(r) + 4\,\Omega(r)$$

Motivation I

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	$\tilde{B}$	A^{-1}	0
0	1	U	$\tilde{D}^{-1}$

$$2\,\mathsf{T}(r) + 4\,\Omega(r)$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	$\tilde{B} - \tilde{B}\,1$	$A^{-1} - \tilde{B}\,U$	$-\tilde{B}\,\tilde{D}^{-1}$
0	1	U	$\tilde{D}^{-1}$

$$2\,\mathsf{T}(r) + 6\,\Omega(r)$$

Motivation I

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	0	$A^{-1} - \tilde{B}\,U$	$-\tilde{B}\,\tilde{D}^{-1}$
0	1	U	$\tilde{D}^{-1}$

$$\mathsf{T}(2\,r) \;=\; 2\,\mathsf{T}(r) + 6\,\Omega(r) + O(r^2)$$

La multiplication comme brique de base pour implanter d'autres opérations

Inversion d'une matrice

1	0	$A^{-1} - \tilde{B}\,U$	$-\tilde{B}\,\tilde{D}^{-1}$
0	1	U	$\tilde{D}^{-1}$

$$\mathsf{T}(r) = O(\Omega(r)\log r)$$

Motivation II

La multiplication comme étalon pour la complexité

Motivation II

La multiplication comme étalon pour la complexité

Complexités fondamentales

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires
$\mathsf{M}(n)$: coût pour multiplier deux polynômes de degré n
$\Omega(r)$: coût pour multiplier deux matrices $r \times r$

La multiplication comme étalon pour la complexité

Complexités fondamentales

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires
$\mathsf{M}_{\mathbb{K}}(n)$: coût pour multiplier deux polynômes de degré n dans $\mathbb{K}[x]$
$\Omega_{\mathbb{K}}(r)$: coût pour multiplier deux matrices dans $\mathbb{K}^{r\times r}$

Motivation II

La multiplication comme étalon pour la complexité

Complexités fondamentales

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires
$\mathsf{M}_{\mathbb{K}}(n)$: coût pour multiplier deux polynômes de degré n dans $\mathbb{K}[x]$
$\Omega_{\mathbb{K}}(r)$: coût pour multiplier deux matrices dans $\mathbb{K}^{r\times r}$

Régularité : $\mathsf{I}(N)/N$, $\mathsf{M}_{\mathbb{K}}(n)/n$ et $\Omega_{\mathbb{K}}(r)/r^2$ croissantes

Motivation II

La multiplication comme étalon pour la complexité

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim \frac{4}{3}\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, …	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(n\,b))$
b $\log n$ bits	

Motivation II

La multiplication comme étalon pour la complexité

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim \frac{4}{3}\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, …	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(n\,b))$
b $\log n$ bits	

Motivation II

La multiplication comme étalon pour la complexité

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim \frac{4}{3}\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, ...	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(n\,b))$
b $\log n$ bits	

Motivation II

La multiplication comme étalon pour la complexité

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim \frac{4}{3}\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, ...	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(n\,b))$
b $\log n$ bits	

Motivation II

La multiplication comme étalon pour la complexité

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim \frac{4}{3}\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, …	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(nb))$
b log n bits	

Motivation II

La multiplication comme étalon pour la complexité

$\mathsf{I}(N)$: coût pour multiplier deux entiers de N chiffres binaires

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim \frac{4}{3}\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, …	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(n\,b))$
$b \geqslant \log n$ bits	

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

$\mathbb{A}$: « nouvelle » algèbre (séries, opérateurs différentiels, nombres flottants, ...)

Complexité d'un problème sur $\mathbb{A}$ (division, factorisation, simplification, ...)

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

$\mathbb{A}$: « nouvelle » algèbre (séries, opérateurs différentiels, nombres flottants, ...)

Complexité d'un problème sur $\mathbb{A}$ (division, factorisation, simplification, ...)

- Illuminant d'étudier la complexité de la multiplication dans $\mathbb{A}$

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

$\mathbb{A}$: « nouvelle » algèbre (séries, opérateurs différentiels, nombres flottants, ...)

Complexité d'un problème sur $\mathbb{A}$ (division, factorisation, simplification, ...)

- Illuminant d'étudier la complexité de la multiplication dans $\mathbb{A}$
- $\longrightarrow$ représentations alternatives des objets dans $\mathbb{A}$

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

$\mathbb{A}$: « nouvelle » algèbre (séries, opérateurs différentiels, nombres flottants, ...)

Complexité d'un problème sur $\mathbb{A}$ (division, factorisation, simplification, ...)

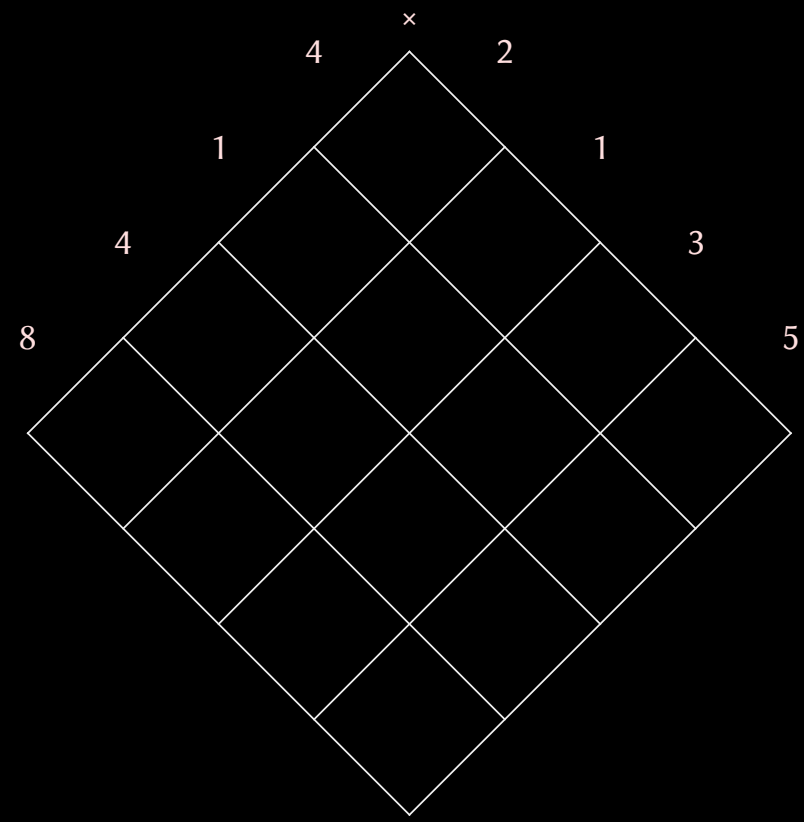
- Illuminant d'étudier la complexité de la multiplication dans $\mathbb{A}$
- $\longrightarrow$ représentations alternatives des objets dans $\mathbb{A}$
- $\longrightarrow$ techniques développées plus généralement utiles

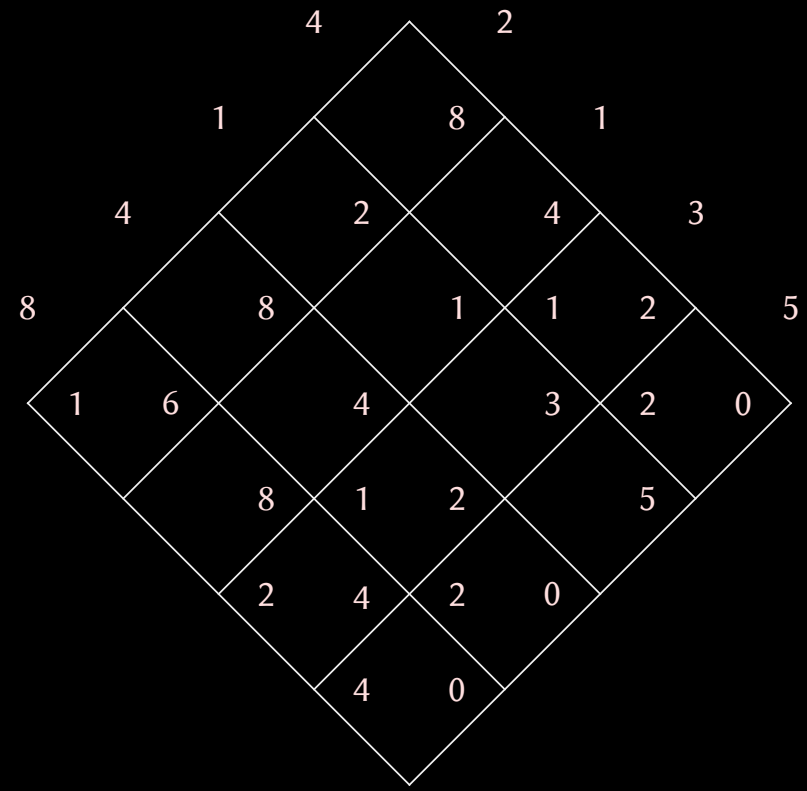
Plan

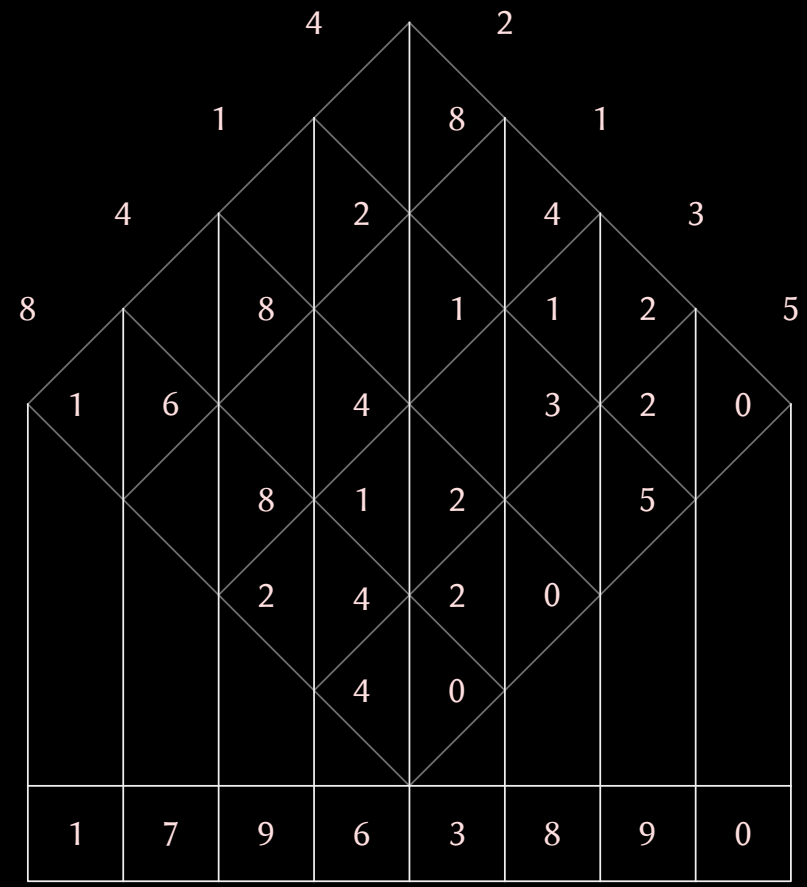
PARTIE I

Multiplication des entiers jusqu'à 1971

8 4 1 4 × 2 1 3 5

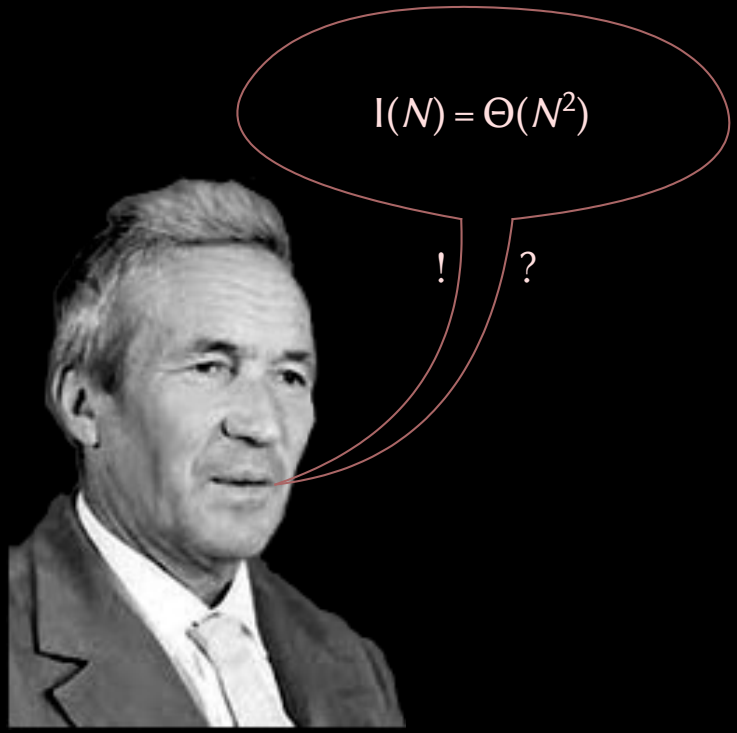

×
4
2
1
1
4
3
8
5


4 2
1 8 1
4 2 4 3
8 8 1 1 2 5
1 6 4 3 2 0
8 1 2 5
2 4 2 0
4 0

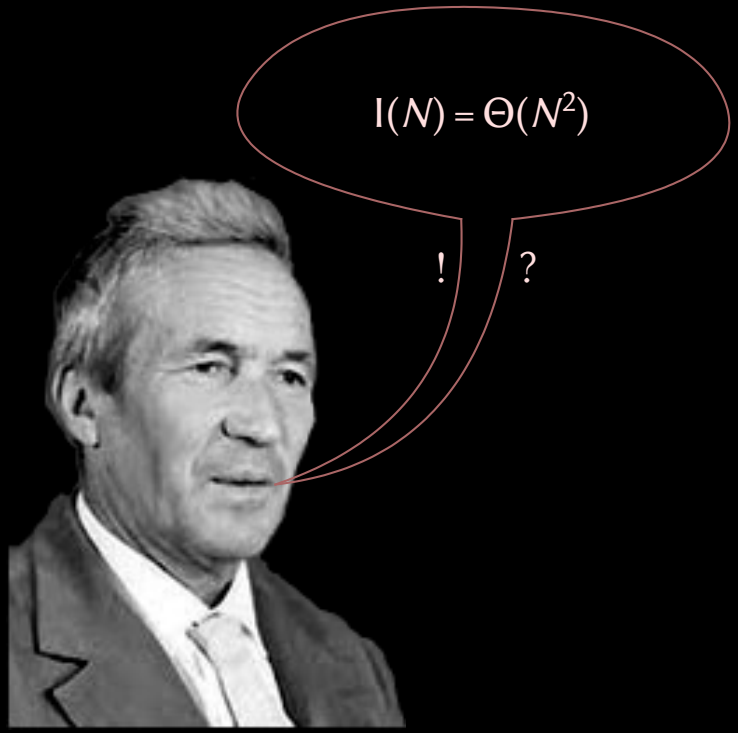

4 2
1 8 1
4 2 4 3
8 8 1 1 2 5
1 6 4 3 2 0
8 1 2 5
2 4 2 0
4 0
1 7 9 6 3 8 9 0

Peut-on faire mieux ?

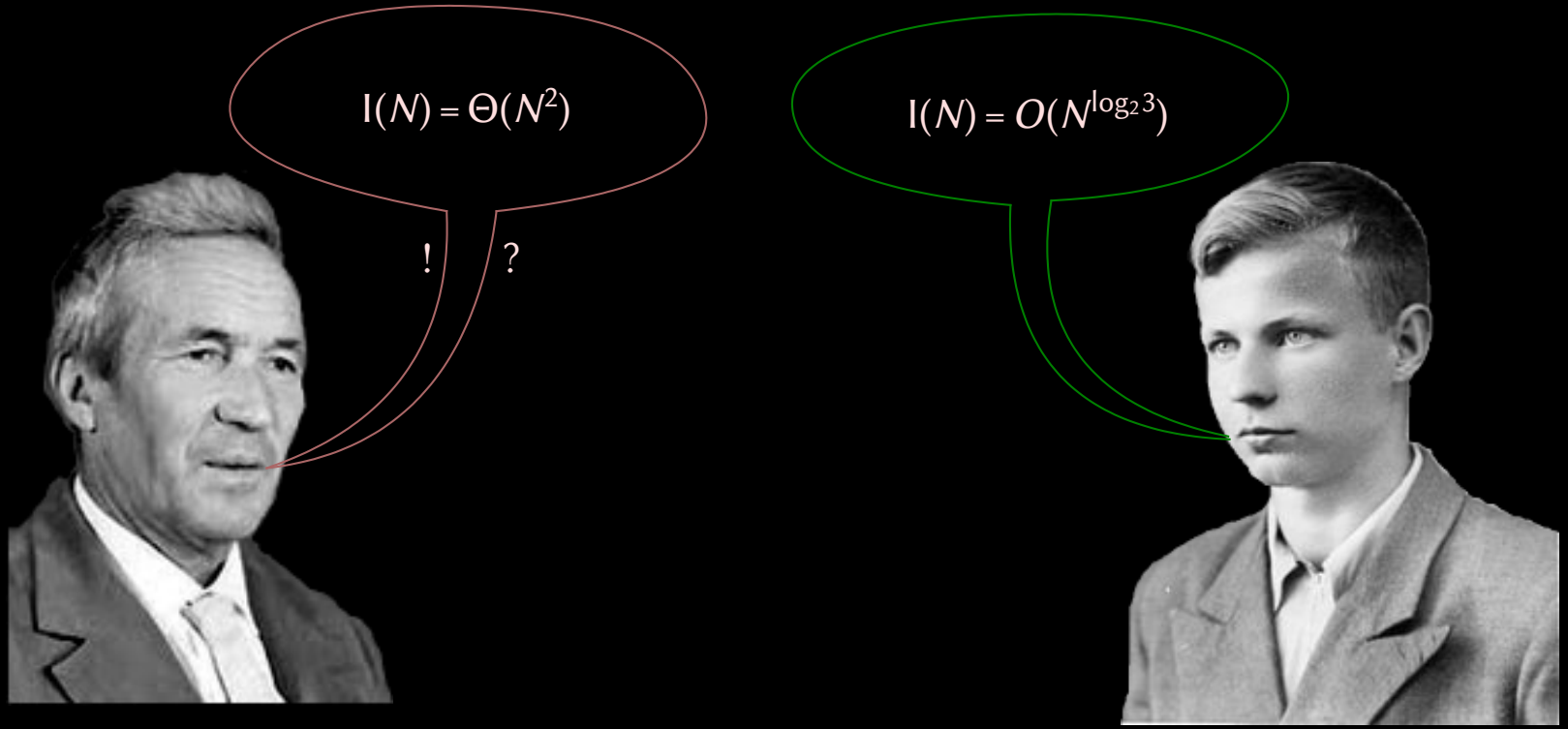
Peut-on faire mieux ?



Peut-on faire mieux ?



Peut-on faire mieux ?



1962

Historique

1962	Karatsuba	$O(N^{\log 3/\log 2})$
1963	Toom	$O\left(N 2^{5\sqrt{\log N/\log 2}}\right)$
1966	Schönhage	$O\left(N 2^{\sqrt{2\log N/\log 2}} (\log N)^{3/2}\right)$
1969	Knuth	$O\left(N 2^{\sqrt{2\log N/\log 2}} \log N\right)$
1971	Pollard	$O(N \log N \log\log N \log\log\log N \cdots)$
1971	Schönhage-Strassen	$O(N \log N \log\log N)$
2007	Fürer	$O(N \log N 2^{O(\log^* N)})$
2014	Harvey-vdH-Lecerf	$O(N \log N 8^{\log^* N})$
2017	Harvey	$O(N \log N 6^{\log^* N})$
2017	Harvey-vdH	$O(N \log N (4\sqrt{2})^{\log^* N})$
2018	Harvey-vdH	$O(N \log N 4^{\log^* N})$
2019	Harvey-vdH	$O(N \log N)$

Multiplication de Karatsuba

$$13022020 \times 31415926$$

Multiplication de Karatsuba

$$1302\ \ 2020 \times 3141\ \ 5926$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) =$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2+(a\cdot d+b\cdot c)\,x+b\cdot d$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexité

$$\mathrm{I}(N) \leqslant 3\,\mathrm{I}(N/2) + CN$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexité

$$\begin{aligned} I(N) &\leqslant 3\,I(N/2) + CN \\ &\leqslant 9\,I(N/4) + \tfrac{5}{2}CN \end{aligned}$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexité

$$\begin{aligned} \mathrm{I}(N) &\leqslant 3\,\mathrm{I}(N/2) + CN \\ &\leqslant 9\,\mathrm{I}(N/4) + \tfrac{5}{2}CN \\ &\leqslant 27\,\mathrm{I}(N/8) + \tfrac{19}{4}CN \end{aligned}$$

Multiplication de Karatsuba

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexité

$$\begin{aligned} \mathrm{I}(N) &\leqslant 3\,\mathrm{I}(N/2) + CN \\ &\leqslant 9\,\mathrm{I}(N/4) + \tfrac{5}{2}CN \\ &\leqslant 27\,\mathrm{I}(N/8) + \tfrac{19}{4}CN \\ &\leqslant \cdots \\ &\leqslant O\left(N^{\frac{\log 3}{\log 2}}\right) \end{aligned}$$

Segmentation de Kronecker

$$4627579679788114 \times 4519170871966234$$

$$\wr$$

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \times (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

Entiers *versus* polynômes

Segmentation de Kronecker

$$\begin{array}{rcl} 4627579679788114 & \times & 4519170871966234 \\ & \wr & \\ (4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) & \times & (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234) \end{array}$$

Substitution de Kronecker

$$\begin{array}{rcl} (4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) & \times & (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234) \\ & \wr & \\ 46270000057960000079780000008114 & \times & 45190000017080000071960000006234 \end{array}$$

Entiers *versus* polynômes

Segmentation de Kronecker

$$4627579679788114 \times 4519170871966234$$

$$\wr$$

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \times (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

Substitution de Kronecker

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \times (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

$$\wr$$

$$46270000057960000079780000008114 \times 45190000017080000071960000006234$$

$$1004003 \times 2001005 = 2009015023015$$

Polynômes cycliques

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

$\mathbb{K}[x]/(x^n - 1)$: anneau des polynômes cycliques de longueur n

Polynômes cycliques

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

$\mathbb{K}[x]/(x^n - 1)$: anneau des polynômes cycliques de longueur n

$$P \in \mathbb{K}[x], \quad \deg P < n \quad \overset{\text{bijection}}{\longleftrightarrow} \quad \bar{P} \in \mathbb{K}[x]/(x^n - 1)$$

Polynômes cycliques

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

$\mathbb{K}[x]/(x^n - 1)$: anneau des polynômes cycliques de longueur n

$$P \in \mathbb{K}[x], \quad \deg P < n \quad \overset{\text{bijection}}{\longleftrightarrow} \quad \bar{P} \in \mathbb{K}[x]/(x^n - 1)$$

$$P, Q \in \mathbb{K}[x], \quad \deg(PQ) < n, \qquad \text{Calculer } PQ \iff \text{Calculer } \bar{P}\bar{Q}$$

Polynômes cycliques

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

$\mathbb{K}[x]/(x^n - 1)$: anneau des polynômes cycliques de longueur n

$$P \in \mathbb{K}[x], \quad \deg P < n \quad \overset{\text{bijection}}{\longleftrightarrow} \quad \bar{P} \in \mathbb{K}[x]/(x^n - 1)$$

$$P, Q \in \mathbb{K}[x], \quad \deg(PQ) < n, \qquad \text{Calculer } PQ \iff \text{Calculer } \bar{P}\bar{Q}$$

Résumé jusqu'à présent

$$\mathbb{Z} \xrightarrow{\text{Kronecker}} \mathbb{K}[x] \xrightarrow{\text{Encode}} \mathbb{K}[x]/(x^n - 1)$$

Transformation de Fourier discrète (DFT)

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

ω : racine n-ième primitive de l'unité dans $\mathbb{K}$, comme $\omega = e^{\frac{2\pi i}{n}}$ si $\mathbb{K} = \mathbb{C}$

Transformation de Fourier discrète (DFT)

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

ω : racine n-ième primitive de l'unité dans $\mathbb{K}$, comme $\omega = e^{\frac{2\pi i}{n}}$ si $\mathbb{K} = \mathbb{C}$

Théorème des restes chinois

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

Transformation de Fourier discrète (DFT)

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

ω : racine n-ième primitive de l'unité dans $\mathbb{K}$, comme $\omega = e^{\frac{2\pi i}{n}}$ si $\mathbb{K} = \mathbb{C}$

Théorème des restes chinois

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

Transformation de Fourier discrète (DFT)

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

ω : racine n-ième primitive de l'unité dans $\mathbb{K}$, comme $\omega = e^{\frac{2\pi i}{n}}$ si $\mathbb{K} = \mathbb{C}$

Théorème des restes chinois

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

Transformation de Fourier discrète (DFT)

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

ω : racine n-ième primitive de l'unité dans $\mathbb{K}$, comme $\omega = e^{\frac{2\pi i}{n}}$ si $\mathbb{K} = \mathbb{C}$

Théorème des restes chinois

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

Transformation de Fourier discrète

$$\mathbb{K}[x]/(x^n - 1) \underset{\mathrm{DFT}_\omega^{-1}}{\overset{\mathrm{DFT}_\omega}{\rightleftharpoons}} \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

Transformation de Fourier discrète (DFT)

$\mathbb{K}$: un corps (ou un anneau convenable)

n : longueur de cycle

ω : racine n-ième primitive de l'unité dans $\mathbb{K}$, comme $\omega = e^{\frac{2\pi i}{n}}$ si $\mathbb{K} = \mathbb{C}$

Théorème des restes chinois

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

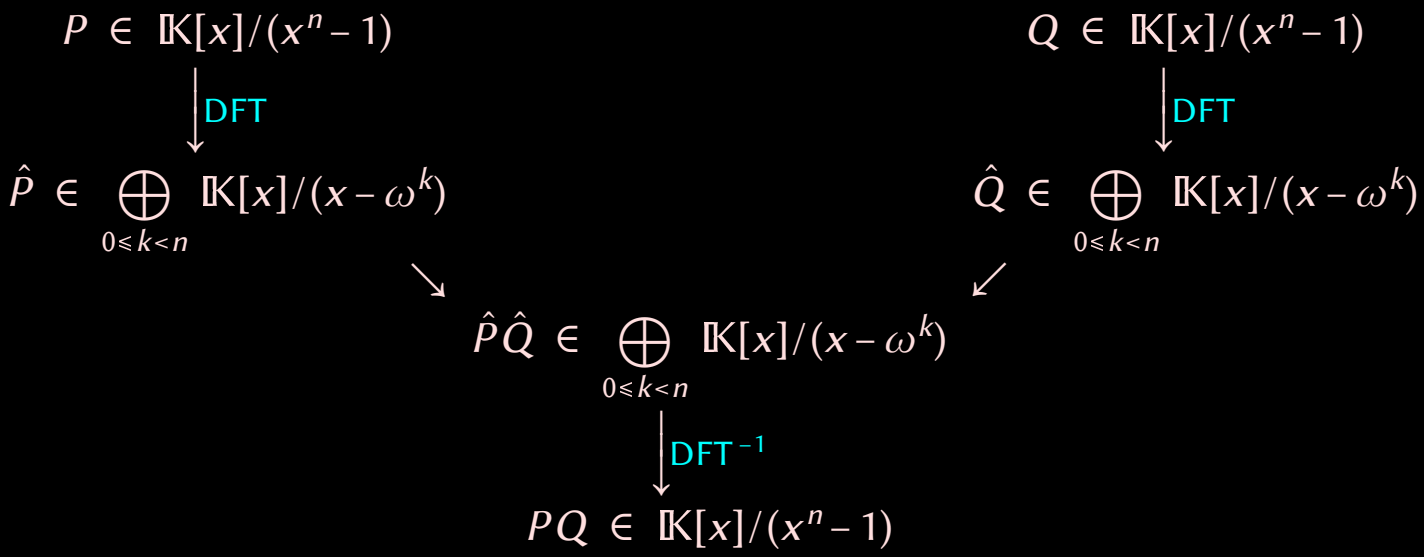
$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

Transformation de Fourier discrète

$$\mathbb{K}[x]/(x^n - 1) \underset{\mathrm{DFT}_\omega^{-1}}{\overset{\mathrm{DFT}_\omega}{\rightleftharpoons}} \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\mathrm{DFT}_\omega^{-1} \quad \leftrightsquigarrow \quad \frac{1}{n}\mathrm{DFT}_{\omega^{-1}}$$

Application à la multiplication



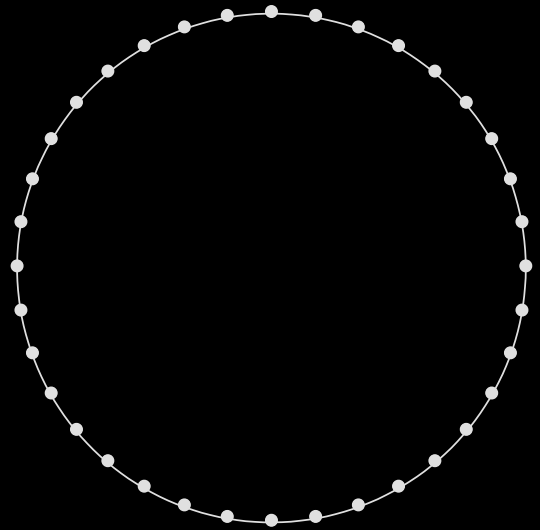
Application à la multiplication

$$
\begin{array}{ccc}
P \in \mathbb{K}[x]/(x^n-1) & & Q \in \mathbb{K}[x]/(x^n-1) \\
\downarrow \text{DFT} & & \downarrow \text{DFT} \\
\hat{P} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x-\omega^k) & & \hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x-\omega^k) \\
& \searrow \quad \swarrow & \\
& \hat{P}\hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x-\omega^k) & \\
& \downarrow \text{DFT}^{-1} & \\
& PQ \in \mathbb{K}[x]/(x^n-1) &
\end{array}
$$

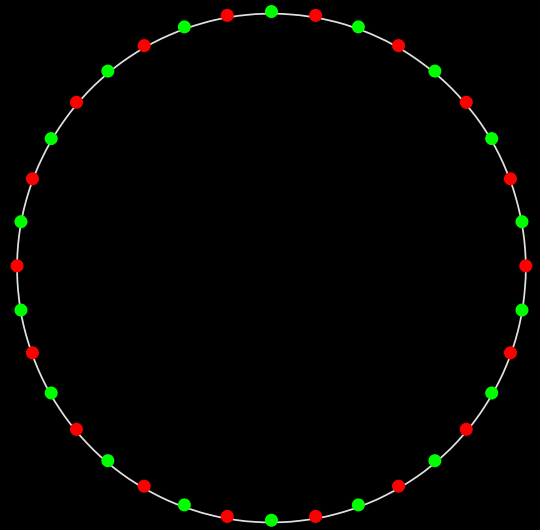
Résumé jusqu'à présent

$$
\mathbb{Z} \xrightarrow{\text{Kronecker}} \mathbb{K}[x] \xrightarrow{\text{Encode}} \mathbb{K}[x]/(x^n-1) \xrightarrow{\text{DFT}} \mathbb{K}^n
$$

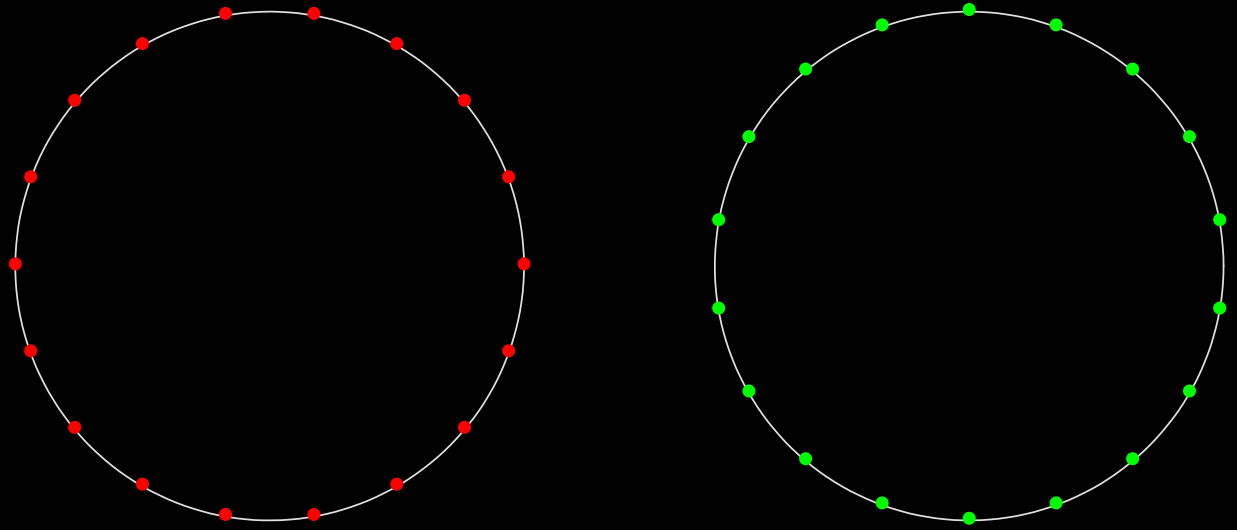
Rendre les DFTs efficaces : FFT



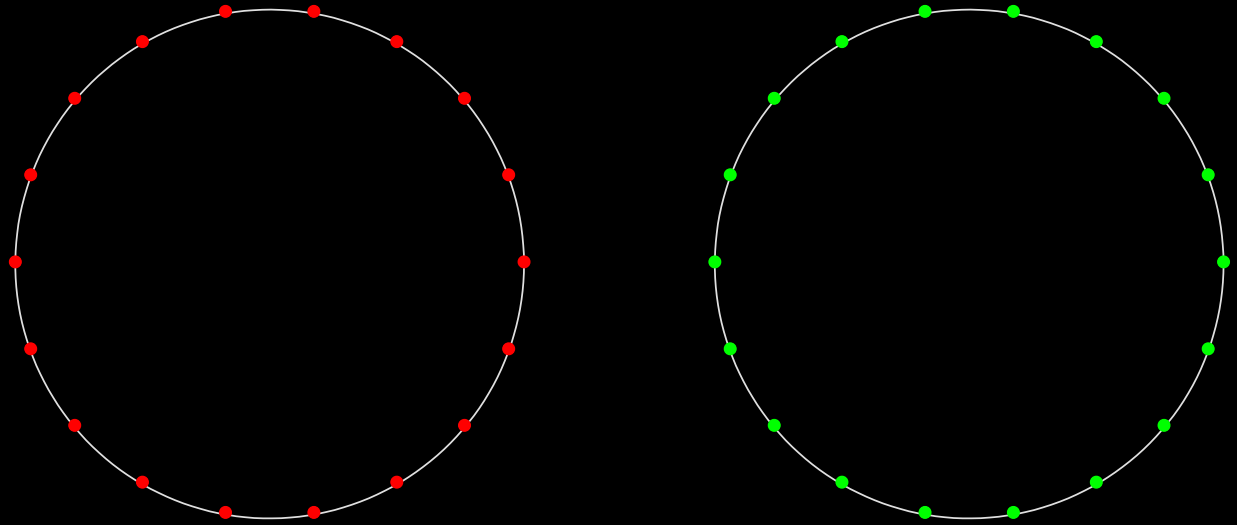
Rendre les DFTs efficaces : FFT



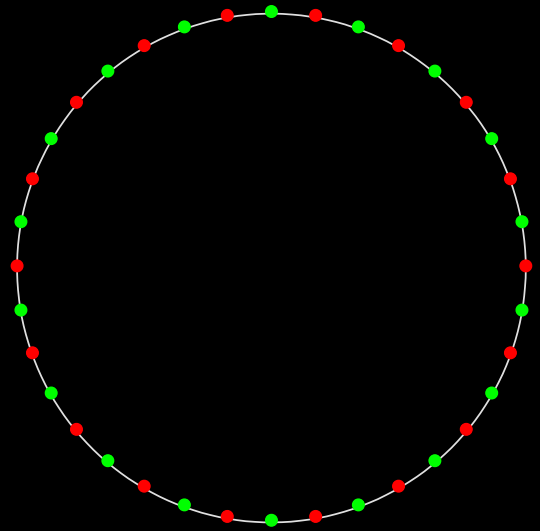
Rendre les DFTs efficaces : FFT



Rendre les DFTs efficaces : FFT

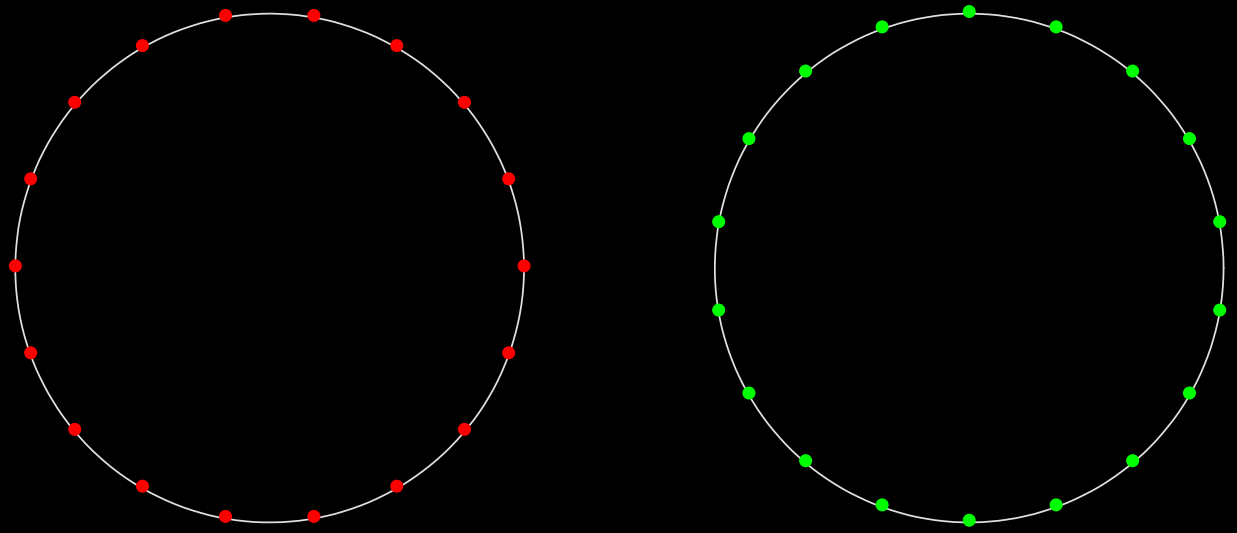


Rendre les DFTs efficaces : FFT



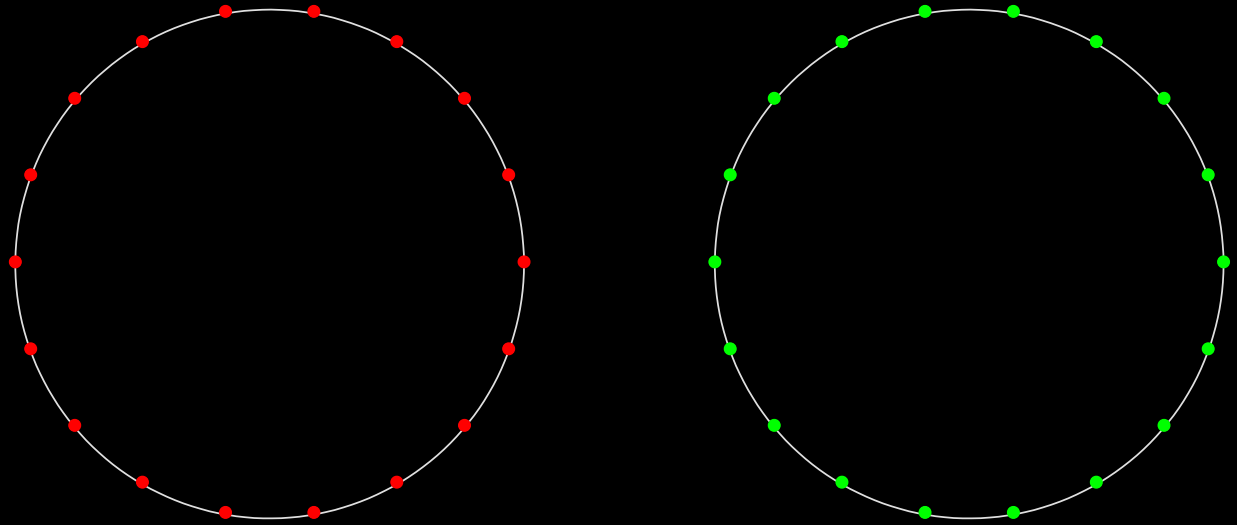
$\mathbb{K}[x]/(x^{2n}-1)$

Rendre les DFTs efficaces : FFT



$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$

Rendre les DFTs efficaces : FFT



$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$
$$\cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(\tilde{x}^n-1)$$
$$\tilde{x} = \omega x$$
$$\omega^n = -1$$

Analyse de complexité

$$\mathrm{F}_{\mathbb{K}}(2\,n) \;\leqslant\; 2\,\mathrm{F}_{\mathbb{K}}(n) + n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}} + n\,\mathrm{mul}_{\omega^{\mathbb{N}}}$$

Analyse de complexité

$$\mathsf{F}_{\mathbb{K}}(2\,n) \;\leqslant\; 2\,\mathsf{F}_{\mathbb{K}}(n) + \underbrace{n\,\mathsf{add}_{\mathbb{K}} + n\,\mathsf{sub}_{\mathbb{K}}} + n\,\mathsf{mul}_{\omega^{\mathbb{N}}}$$

$$\mathbb{K}[x]/(x^{2n}-1)$$

$$\cong$$

$$\mathbb{K}[x]/(x^{n}-1) \oplus \mathbb{K}[x]/(x^{n}+1)$$

Analyse de complexité

$$\mathrm{F}_{\mathbb{K}}(2\,n) \;\leqslant\; 2\,\mathrm{F}_{\mathbb{K}}(n) + \underbrace{n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}}} + \underbrace{n\,\mathrm{mul}_{\omega^{\mathbb{N}}}}$$

$$\mathbb{K}[x]/(x^{2n}-1)$$

$$\cong$$

$$\mathbb{K}[x]/(x^{n}-1) \oplus \mathbb{K}[x]/(x^{n}+1)$$

$$\mathbb{K}[x]/(x^{n}+1)$$

$$\cong$$

$$\mathbb{K}[x]/(\tilde{x}^{n}-1)$$

Analyse de complexité

$$\mathrm{F}_{\mathbb{K}}(2\,n) \;\leqslant\; 2\,\mathrm{F}_{\mathbb{K}}(n) + \underbrace{n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}}} + \underbrace{n\,\mathrm{mul}_{\omega^{\mathbb{N}}}}$$

$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$

$$\mathbb{K}[x]/(x^n+1) \cong \mathbb{K}[x]/(\tilde{x}^n-1)$$

$$n = 2^{\lg n} \Longrightarrow \mathrm{F}_{\mathbb{K}}(n) \leqslant n \lg n \left(\mathrm{add}_{\mathbb{K}} + \frac{1}{2}\mathrm{mul}_{\omega^{\mathbb{N}}}\right)$$

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ avec $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω existe…

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ avec $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω existe…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}$ avec $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ avec $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω existe…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}$ avec $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Analyse de complexité

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ avec $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω existe…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}$ avec $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Analyse de complexité

I. $\mathsf{I}(N) = O(N\,\mathsf{I}(\log N))$ $\qquad$ $\mathsf{I}(N) = O(N \log N \log\log N \cdots)$

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ avec $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω existe…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}$ avec $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Analyse de complexité

I. $\mathsf{I}(N) = O(N\,\mathsf{I}(\log N))$ $\qquad$ $\mathsf{I}(N) = O(N \log N \log\log N \cdots)$

II. $\mathsf{I}(N) = O(N\,\mathsf{I}(\log N))$ $\qquad$ $\mathsf{I}(N) = O(N \log N \log\log N \cdots)$

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ avec $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ avec $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω existe…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}$ avec $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Analyse de complexité

I. $\mathsf{I}(N) = O(N\,\mathsf{I}(\log N))$ $\qquad$ $\mathsf{I}(N) = O(N \log N \log\log N \cdots)$

II. $\mathsf{I}(N) = O(N\,\mathsf{I}(\log N))$ $\qquad$ $\mathsf{I}(N) = O(N \log N \log\log N \cdots)$

III. $\mathsf{I}^{\ominus}(N) \leqslant 2\sqrt{N}\,\mathsf{I}^{\ominus}\left(\sqrt{N}\right) + O(N \log N)$ $\qquad$ $\mathsf{I}(N) = O(N \log N \log\log N)$

$\mathsf{I}^{\ominus}(N)$: coût de la multiplication dans $\mathbb{Z}/(2^N + 1)\mathbb{Z}$

PARTIE II

Boîte à outils pour les FFTs

FFT de Cooley–Tukey généralisée

$$n = n_1 n_2, \qquad \omega^n = 1, \qquad \vartheta := \omega^{n_2}, \qquad \vartheta^{n_1} = 1$$

$$\mathbb{K}[x]/(x^n - 1) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - \vartheta^k) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - 1) \cong \mathbb{K}^n$$

FFT de Cooley–Tukey généralisée

$$n = n_1 n_2, \qquad \omega^n = 1, \qquad \vartheta := \omega^{n_2}, \qquad \vartheta^{n_1} = 1$$

$$\mathbb{K}[x]/(x^n - 1) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - \vartheta^k) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - 1) \cong \mathbb{K}^n$$

n_2 DFTs de longueur n_1

$$\mathbb{K}[x]/(x^n - 1) = (\mathbb{K} + \cdots + \mathbb{K}\, x^{n_2-1})[x^{n_1}]/((x^{n_1})^{n_2} - 1)$$

FFT de Cooley–Tukey généralisée

$$n = n_1 n_2, \qquad \omega^n = 1, \qquad \vartheta := \omega^{n_2}, \qquad \vartheta^{n_1} = 1$$

$$\mathbb{K}[x]/(x^n - 1) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - \vartheta^k) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - 1) \cong \mathbb{K}^n$$

n_2 DFTs de longueur n_1

n multiplications par des puissances de ω

FFT de Cooley–Tukey généralisée

$$n = n_1 n_2, \qquad \omega^n = 1, \qquad \vartheta := \omega^{n_2}, \qquad \vartheta^{n_1} = 1$$

$$\mathbb{K}[x]/(x^n - 1) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - \vartheta^k) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - 1) \cong \mathbb{K}^n$$

n_2 DFTs de longueur n_1

n multiplications par des puissances de ω

n_1 DFTs de longueur n_2

FFT de Cooley–Tukey généralisée

$$n = n_1 n_2, \qquad \omega^n = 1, \qquad \vartheta := \omega^{n_2}, \qquad \vartheta^{n_1} = 1$$

$$\mathbb{K}[x]/(x^n - 1) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - \vartheta^k) \cong \prod_{k=0}^{n_1-1} \mathbb{K}[x]/(x^{n_2} - 1) \cong \mathbb{K}^n$$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n_2\,\mathsf{F}_{\mathbb{K}}(n_1) + n \cdot \mathsf{mul}_{\omega^{\mathbb{N}}} + n_1\,\mathsf{F}_{\mathbb{K}}(n_2)$$

FFT de Good

$$n = n_1 n_2, \qquad n_1 \wedge n_2 = 1$$

$$n = n_1 n_2, \qquad n_1 \wedge n_2 = 1$$

$$\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}/n_1\mathbb{Z} + \mathbb{Z}/n_2\mathbb{Z}$$

FFT de Good

$$n = n_1 n_2, \qquad n_1 \wedge n_2 = 1$$

$$\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}/n_1\mathbb{Z} + \mathbb{Z}/n_2\mathbb{Z}$$

$$x^{\mathbb{Z}/(n\mathbb{Z})} \cong x_1^{\mathbb{Z}/n_1\mathbb{Z}} \times x_2^{\mathbb{Z}/n_2\mathbb{Z}}$$

FFT de Good

$$n = n_1 n_2, \qquad n_1 \wedge n_2 = 1$$

$$\mathbb{Z}/(n_1 n_2 \mathbb{Z}) \cong \mathbb{Z}/n_1\mathbb{Z} + \mathbb{Z}/n_2\mathbb{Z}$$

$$x^{\mathbb{Z}/(n\mathbb{Z})} \cong x_1^{\mathbb{Z}/n_1\mathbb{Z}} \times x_2^{\mathbb{Z}/n_2\mathbb{Z}}$$

$$\begin{aligned}\mathbb{K}[x]/(x^n-1) &\cong \mathbb{K}[x_1]/(x_1^{n_1}-1) \otimes \mathbb{K}[x_2]/(x_2^{n_2}-1)\\ &\cong \mathbb{K}[x_1,x_2]/(x_1^{n_1}-1, x_2^{n_2}-1)\end{aligned}$$

FFT de Good

$$n = n_1 n_2, \qquad n_1 \wedge n_2 = 1$$

$$\mathbb{Z}/(n_1 n_2 \mathbb{Z}) \cong \mathbb{Z}/n_1\mathbb{Z} + \mathbb{Z}/n_2\mathbb{Z}$$

$$x^{\mathbb{Z}/(n\mathbb{Z})} \cong x_1^{\mathbb{Z}/n_1\mathbb{Z}} \times x_2^{\mathbb{Z}/n_2\mathbb{Z}}$$

$$\begin{aligned}
\mathbb{K}[x]/(x^n - 1) &\cong \mathbb{K}[x_1]/(x_1^{n_1} - 1) \otimes \mathbb{K}[x_2]/(x_2^{n_2} - 1) \\
&\cong \mathbb{K}[x_1, x_2]/(x_1^{n_1} - 1, x_2^{n_2} - 1) \\
&\cong \mathbb{K}^{n_1}[x_2]/(x_2^{n_2} - 1) \\
&\cong (\mathbb{K}^{n_1})^{n_2}
\end{aligned}$$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n_2 \mathsf{F}_{\mathbb{K}}(n_1) + n_1 \mathsf{F}_{\mathbb{K}}(n_2)$$

FFT de Good

$$n = n_1 n_2, \qquad n_1 \wedge n_2 = 1$$

$$\mathbb{Z}/(n_1 n_2 \mathbb{Z}) \cong \mathbb{Z}/n_1\mathbb{Z} + \mathbb{Z}/n_2\mathbb{Z}$$

$$x^{\mathbb{Z}/(n\mathbb{Z})} \cong x_1^{\mathbb{Z}/n_1\mathbb{Z}} \times x_2^{\mathbb{Z}/n_2\mathbb{Z}}$$

$$\begin{aligned}
\mathbb{K}[x]/(x^n - 1) &\cong \mathbb{K}[x_1]/(x_1^{n_1} - 1) \otimes \mathbb{K}[x_2]/(x_2^{n_2} - 1) \\
&\cong \mathbb{K}[x_1, x_2]/(x_1^{n_1} - 1, x_2^{n_2} - 1) \\
&\cong \mathbb{K}^{n_1}[x_2]/(x_2^{n_2} - 1) \\
&\cong (\mathbb{K}^{n_1})^{n_2}
\end{aligned}$$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n_2 \mathsf{F}_{\mathbb{K}}(n_1) + n_1 \mathsf{F}_{\mathbb{K}}(n_2)$$

La base 12 ou 24 est mieux pour les FFTs que la base 2 !

Réduction de Rader

DFT de longueur $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \\ A(\omega^4) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \in \mathbb{K}[x]/(x^5 - 1)$$

DFT de longueur $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \\ A(\omega^4) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^1 & \omega^3 \\ 1 & \omega^3 & \omega^1 & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \in \mathbb{K}[x]/(x^5 - 1)$$

Réduction de Rader

DFT de longueur $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^{2^0}) \\ A(\omega^{2^1}) \\ A(\omega^{2^3}) \\ A(\omega^{2^2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{2^0} & \omega^{2^1} & \omega^{2^3} & \omega^{2^2} \\ 1 & \omega^{2^1} & \omega^{2^2} & \omega^{2^4} & \omega^{2^3} \\ 1 & \omega^{2^3} & \omega^{2^4} & \omega^{2^6} & \omega^{2^5} \\ 1 & \omega^{2^2} & \omega^{2^3} & \omega^{2^5} & \omega^{2^4} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

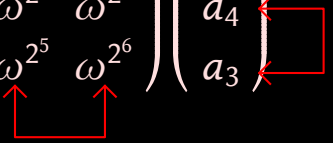
$$1 = 2^0, \qquad 2 = 2^1, \qquad 3 = 2^3, \qquad 4 = 2^2 \qquad (\mathrm{mod}\, 5)$$

DFT de longueur $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^{2^0}) \\ A(\omega^{2^1}) \\ A(\omega^{2^2}) \\ A(\omega^{2^3}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{2^0} & \omega^{2^1} & \omega^{2^3} & \omega^{2^2} \\ 1 & \omega^{2^1} & \omega^{2^2} & \omega^{2^4} & \omega^{2^3} \\ 1 & \omega^{2^2} & \omega^{2^3} & \omega^{2^5} & \omega^{2^4} \\ 1 & \omega^{2^3} & \omega^{2^4} & \omega^{2^6} & \omega^{2^5} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

DFT de longueur $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^{2^0}) \\ A(\omega^{2^1}) \\ A(\omega^{2^2}) \\ A(\omega^{2^3}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{2^0} & \omega^{2^1} & \omega^{2^2} & \omega^{2^3} \\ 1 & \omega^{2^1} & \omega^{2^2} & \omega^{2^3} & \omega^{2^4} \\ 1 & \omega^{2^2} & \omega^{2^3} & \omega^{2^4} & \omega^{2^5} \\ 1 & \omega^{2^3} & \omega^{2^4} & \omega^{2^5} & \omega^{2^6} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_4 \\ a_3 \end{pmatrix}$$



DFT de longueur $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^4) \\ A(\omega^3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ 1 & \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ 1 & \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_4 \\ a_3 \end{pmatrix}$$

DFT de longueur $p = 5$

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$\Updownarrow$$

$$v_0 + v_1 x + v_2 x^2 + v_3 x^3 = (\omega^1 + \omega^2 x + \omega^4 x^2 + \omega^3 x^3)(u_0 + u_1 x + u_2 x^2 + u_3 x^3)$$

modulo $x^4 - 1$

Réduction de Rader

DFT de longueur $p = 5$

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$\Updownarrow$$

$$v_0 + v_1 x + v_2 x^2 + v_3 x^3 = (\omega^1 + \omega^2 x + \omega^4 x^2 + \omega^3 x^3)(u_0 + u_1 x + u_2 x^2 + u_3 x^3) \text{ modulo } x^4 - 1$$

$$\mathrm{F}(p) \leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(p-1) + 2p \cdot \mathrm{add}_{\mathbb{K}}$$

$\mathrm{M}^{\circ}_{\mathbb{K}}(n)$: coût de la multiplication dans $\mathbb{K}[x]/(x^n - 1)$
$\mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(n)$: quand un argument est fixe

Réduction de Rader

DFT de longueur $p = 5$

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$\Updownarrow$$

$$v_0 + v_1 x + v_2 x^2 + v_3 x^3 = (\omega^1 + \omega^2 x + \omega^4 x^2 + \omega^3 x^3)(u_0 + u_1 x + u_2 x^2 + u_3 x^3) \text{ modulo } x^4 - 1$$

$$\begin{aligned} \mathsf{F}_{\mathbb{K}}(p) &\leqslant \mathsf{M}^{\circ}_{\mathbb{K},\text{fixe}}(p-1) + 2p \cdot \mathrm{add}_{\mathbb{K}} \\ &\leqslant 2\,\mathsf{F}_{\mathbb{K}}(p-1) + 2p \cdot \mathrm{add}_{\mathbb{K}} \end{aligned}$$

$\mathsf{M}^{\circ}_{\mathbb{K}}(n)$: coût de la multiplication dans $\mathbb{K}[x]/(x^n - 1)$
$\mathsf{M}^{\circ}_{\mathbb{K},\text{fixe}}(n)$: quand un argument est fixe

Réduction de Bluestein

$$n \in 2\mathbb{N}^{>}, \qquad \eta^{2n} = 1, \qquad \omega = \eta^{2}$$

Réduction de Bluestein

$$n \in 2\mathbb{N}^{>}, \qquad \eta^{2n} = 1, \qquad \omega = \eta^2$$

$$f_i := \eta^{i^2}, \quad g_i := \eta^{-i^2}$$

Réduction de Bluestein

$$n \in 2\mathbb{N}^{>}, \qquad \eta^{2n} = 1, \qquad \omega = \eta^2$$

$$f_i := \eta^{i^2}, \quad g_i := \eta^{-i^2}$$

$$g_{i+n} = \eta^{-(i+n)^2} = \eta^{-i^2-n^2-2ni} = \eta^{-i^2}\,\omega^{-\left(\frac{n}{2}+i\right)n} = g_i$$

Réduction de Bluestein

$$n \in 2\mathbb{N}^{>}, \qquad \eta^{2n} = 1, \qquad \omega = \eta^2$$

$$f_i := \eta^{i^2}, \quad g_i := \eta^{-i^2}$$

$$g_{i+n} = \eta^{-(i+n)^2} = \eta^{-i^2-n^2-2ni} = \eta^{-i^2}\,\omega^{-\left(\frac{n}{2}+i\right)n} = g_i$$

$$f_i\, f_j\, g_{i-j} = \eta^{i^2+j^2-(i-j)^2} = \eta^{2ij} = \omega^{ij}$$

Réduction de Bluestein

$$n \in 2\mathbb{N}^{>}, \qquad \eta^{2n} = 1, \qquad \omega = \eta^2$$

$$f_i := \eta^{i^2}, \quad g_i := \eta^{-i^2}$$

$$g_{i+n} = \eta^{-(i+n)^2} = \eta^{-i^2-n^2-2ni} = \eta^{-i^2}\,\omega^{-\left(\frac{n}{2}+i\right)n} = g_i$$

$$f_i\, f_j\, g_{i-j} = \eta^{i^2+j^2-(i-j)^2} = \eta^{2ij} = \omega^{ij}$$

Pour $a_0, \ldots, a_{n-1} \in \mathbb{K}$,

$$\hat{a}_i := \sum_{j=0}^{n-1} a_j \omega^{ij} = f_i \sum_{j=0}^{n-1} (a_j f_j)\, g_{i-j}$$

Réduction de Bluestein

$$n \in 2\mathbb{N}^{>}, \qquad \eta^{2n} = 1, \qquad \omega = \eta^2$$

$$f_i := \eta^{i^2}, \quad g_i := \eta^{-i^2}$$

$$g_{i+n} = \eta^{-(i+n)^2} = \eta^{-i^2-n^2-2ni} = \eta^{-i^2}\,\omega^{-\left(\frac{n}{2}+i\right)n} = g_i$$

$$f_i\, f_j\, g_{i-j} = \eta^{i^2+j^2-(i-j)^2} = \eta^{2ij} = \omega^{ij}$$

Pour $a_0, \ldots, a_{n-1} \in \mathbb{K}$,

$$\hat{a}_i := \underbrace{\sum_{j=0}^{n-1} a_j\, \omega^{ij}}_{\text{DFT}} = f_i \underbrace{\sum_{j=0}^{n-1} (a_j\, f_j)\, g_{i-j}}_{\text{produit cyclique}}$$

Résumé

$$\mathrm{M}^{\circ}_{\mathbb{K}}(n) \leqslant 3\,\mathrm{F}_{\mathbb{K}}(n) + n\,\mathrm{mul}_{\mathbb{K}} \qquad \text{(multiplication FFT)}$$

$$\mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(n) \leqslant 2\,\mathrm{F}_{\mathbb{K}}(n) + n\,\mathrm{mul}_{\mathbb{K}}$$

$$\mathrm{F}_{\mathbb{K}}(n) \leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(n) + 2\,n\,\mathrm{mul}_{\mathbb{K}} \qquad \text{(Bluestein)}$$

$$\mathrm{F}_{\mathbb{K}}(p) \leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(p-1) + 2\,n\,\mathrm{add}_{\mathbb{K}} \qquad \text{(Rader)}$$

Multiplication dans $\mathbb{F}_2[x]$

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

Multiplication dans $\mathbb{F}_2[x]$

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \qquad n = 30\,k$$

$$\underbrace{a_0 + a_1 x + \cdots + a_{29} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}} + (\underbrace{a_{30} + \cdots + a_{59} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}}) x^{30} + \cdots + (\underbrace{a_{n-30} + \cdots + a_{n-1} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}}) x^{30(k-1)}$$

Multiplication dans $\mathbb{F}_2[x]$

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \qquad n = 30\,k$$

$$\underbrace{a_0 + a_1 x + \cdots + a_{29} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}} + (\underbrace{a_{30} + \cdots + a_{59} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}}) x^{30} + \cdots + (\underbrace{a_{n-30} + \cdots + a_{n-1} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}}) x^{30(k-1)}$$

Pourquoi $\mathbb{F}_{2^{60}}$?

$$2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

Multiplication dans $\mathbb{F}_2[x]$

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \qquad n = 30\,k$$

$$\underbrace{a_0 + a_1 x + \cdots + a_{29} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}} + (\underbrace{a_{30} + \cdots + a_{59} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}}) x^{30} + \cdots + (\underbrace{a_{n-30} + \cdots + a_{n-1} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}}) x^{30(k-1)}$$

Pourquoi $\mathbb{F}_{2^{60}}$?

$$2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

Rader

$$2 \quad 2^2 \quad 2 \cdot 3 \quad 2 \cdot 5 \quad 2^2 \cdot 3 \quad 2 \cdot 3 \cdot 5 \quad 2^3 \cdot 5 \quad 2^2 \cdot 3 \cdot 5 \quad 2 \cdot 3 \cdot 5^2 \quad \cdots$$

Multiplication dans $\mathbb{F}_2[x]$

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \qquad n = 30\,k$$

$$\underbrace{a_0 + a_1 x + \cdots + a_{29} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}} + \underbrace{(a_{30} + \cdots + a_{59} x^{29})}_{\hookrightarrow \mathbb{F}_{2^{60}}} x^{30} + \cdots + \underbrace{(a_{n-30} + \cdots + a_{n-1} x^{29})}_{\hookrightarrow \mathbb{F}_{2^{60}}} x^{30(k-1)}$$

Pourquoi $\mathbb{F}_{2^{60}}$?

$$2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

Rader

$$2 \quad 2^2 \quad 2\cdot 3 \quad 2\cdot 5 \quad 2^2\cdot 3 \quad 2\cdot 3\cdot 5 \quad 2^3\cdot 5 \quad 2^2\cdot 3\cdot 5 \quad 2\cdot 3\cdot 5^2 \quad \cdots$$

$$2 \quad 2^2 \quad 2 \quad 2 \quad 2^2 \quad 2^2 \quad 2 \quad 2^2 \quad 2 \quad 2^2$$

Multiplication dans $\mathbb{F}_2[x]$

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \qquad n \;=\; 30\,k$$

$$\underbrace{a_0 + a_1 x + \cdots + a_{29} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}} + (\underbrace{a_{30} + \cdots + a_{59} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}})\, x^{30} + \cdots + (\underbrace{a_{n-30} + \cdots + a_{n-1} x^{29}}_{\hookrightarrow \mathbb{F}_{2^{60}}})\, x^{30(k-1)}$$

Pourquoi $\mathbb{F}_{2^{60}}$?

$$2^{60} - 1 \;=\; 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

Rader

$$2 \quad 2^2 \quad 2\cdot 3 \quad 2\cdot 5 \quad 2^2\cdot 3 \quad 2\cdot 3\cdot 5 \quad 2^3\cdot 5 \quad 2^2\cdot 3\cdot 5 \quad 2\cdot 3\cdot 5^2 \quad \cdots$$

$$2 \quad 2^2 \quad 2 \quad 2 \quad 2^2 \quad 2^2 \quad 2 \quad 2^2 \quad 2 \quad 2^2$$

$\dfrac{x^{61}-1}{x-1}$ est irreductible $\Longrightarrow$ $\mathbb{F}_{2^{60}} \times \mathbb{F}_2 \;\cong\; \mathbb{F}[x]/(x^{61}-1)$

FFT « de Frobenius »

$$A = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_2[x]$$

FFT « de Frobenius »

$$A = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_2[x]$$

$A \in \mathbb{F}_{2^k}[x]$, $l \mid (2^k - 1)$, $\omega^l = 1$, $l \geqslant n$, calculer $\mathrm{DFT}_\omega(A)$?

FFT « de Frobenius »

$$A = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_2[x]$$

$A \in \mathbb{F}_{2^k}[x]$, $l \mid (2^k - 1)$, $\omega^l = 1$, $l \geqslant n$, calculer $\mathrm{DFT}_\omega(A)$?

$i = 0, \ldots, l-1$, $v \mid k$ minimal avec $A(\omega^i) \in \mathbb{F}_{2^v}$

$$A(\omega^i) = A(\omega^i), \quad A((\omega^i)^2) = A(\omega^i)^2, \quad \ldots, \quad A((\omega^i)^{2^{v-1}}) = A(\omega^i)^{2^{v-1}}$$

FFT « de Frobenius »

$$A = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_2[x]$$

$A \in \mathbb{F}_{2^k}[x]$, $l \mid (2^k - 1)$, $\omega^l = 1$, $l \geqslant n$, calculer $\mathrm{DFT}_\omega(A)$?

$i = 0, \ldots, l-1$, $v \mid k$ minimal avec $A(\omega^i) \in \mathbb{F}_{2^v}$

$$A(\omega^i) = A(\omega^i), \quad A((\omega^i)^2) = A(\omega^i)^2, \quad \ldots, \quad A((\omega^i)^{2^{v-1}}) = A(\omega^i)^{2^{v-1}}$$

v fois plus de coefficients, mais v fois moins de valeurs à calculer

FFT « de Frobenius »

$$A = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_2[x]$$

$A \in \mathbb{F}_{2^k}[x]$, $l \mid (2^k - 1)$, $\omega^l = 1$, $l \geqslant n$, calculer $\mathrm{DFT}_\omega(A)$?

$i = 0, \ldots, l-1$, $v \mid k$ minimal avec $A(\omega^i) \in \mathbb{F}_{2^v}$

$$A(\omega^i) = A(\omega^i), \quad A((\omega^i)^2) = A(\omega^i)^2, \quad \ldots, \quad A((\omega^i)^{2^{v-1}}) = A(\omega^i)^{2^{v-1}}$$

v fois plus de coefficients, mais v fois moins de valeurs à calculer

Au final, on gagne un facteur 2

PARTIE III

Multiplication en temps $O(n \log n)$

Une construction soigneuse donne

$$\mathrm{I}^{\ominus}(n) \leqslant C\,n\log n + 2\,n^{1/2}\,\mathrm{I}^{\ominus}(n^{1/2})$$

Une construction soigneuse donne

$$\begin{aligned} \mathsf{I}^{\ominus}(n) &\leqslant C\,n\log n + 2\,n^{1/2}\,\mathsf{I}^{\ominus}(n^{1/2}) \\ &\leqslant C\,n\log n + C\,n\log n + 4\,n^{3/4}\,\mathsf{I}^{\ominus}(n^{1/4}) \end{aligned}$$

Une construction soigneuse donne

$$\begin{aligned} \mathsf{I}^{\ominus}(n) &\leqslant C\,n\log n + 2\,n^{1/2}\,\mathsf{I}^{\ominus}(n^{1/2}) \\ &\leqslant C\,n\log n + C\,n\log n + 4\,n^{3/4}\,\mathsf{I}^{\ominus}(n^{1/4}) \\ &\leqslant C\,n\log n + C\,n\log n + C\,n\log n + 8\,n^{7/8}\,\mathsf{I}^{\ominus}(n^{1/8}) \end{aligned}$$

Une construction soigneuse donne

$$\begin{aligned}
\mathsf{I}^{\ominus}(n) &\leqslant C\,n\log n + 2\,n^{1/2}\,\mathsf{I}^{\ominus}(n^{1/2}) \\
&\leqslant C\,n\log n + C\,n\log n + 4\,n^{3/4}\,\mathsf{I}^{\ominus}(n^{1/4}) \\
&\leqslant C\,n\log n + C\,n\log n + C\,n\log n + 8\,n^{7/8}\,\mathsf{I}^{\ominus}(n^{1/8}) \\
&\vdots \\
&\leqslant C\,n\log n + \overset{\log\log n\ \times}{\cdots} + C\,n\log n + C\,n\log n + O(n\log n)
\end{aligned}$$

Et si…

$$\mathrm{I}^{\ominus}(n) \leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathrm{I}^{\ominus}(n^{1/2})$$

Et si…

$$\begin{aligned} \mathrm{I}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathrm{I}^{\ominus}(n^{1/2}) \\ &\leqslant C\,n\log n + 0.99\,C\,n\log n + 1.98^2\,n^{3/4}\,\mathrm{I}^{\ominus}(n^{1/4}) \end{aligned}$$

Et si…

$$\begin{aligned} \mathsf{I}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathsf{I}^{\ominus}(n^{1/2}) \\ &\leqslant C\,n\log n + 0.99C\,n\log n + 1.98^2\,n^{3/4}\,\mathsf{I}^{\ominus}(n^{1/4}) \\ &\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,\mathsf{I}^{\ominus}(n^{1/8}) \end{aligned}$$

Et si…

$$\begin{aligned}
\mathrm{I}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathrm{I}^{\ominus}(n^{1/2}) \\
&\leqslant C\,n\log n + 0.99C\,n\log n + 1.98^2\,n^{3/4}\,\mathrm{I}^{\ominus}(n^{1/4}) \\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,\mathrm{I}^{\ominus}(n^{1/8}) \\
&\vdots \\
&\leqslant O(n\log n)
\end{aligned}$$

Et si…

$$\begin{aligned} \mathsf{I}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathsf{I}^{\ominus}(n^{1/2}) \\ &\leqslant C\,n\log n + 0.99\,C\,n\log n + 1.98^2\,n^{3/4}\,\mathsf{I}^{\ominus}(n^{1/4}) \\ &\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,\mathsf{I}^{\ominus}(n^{1/8}) \\ &\vdots \\ &\leqslant O(n\log n) \end{aligned}$$

Objectif suivant :

$$\mathsf{I}(n) \leqslant C\,n\log n + (d-\epsilon)\,n^{1-1/d}\,\mathsf{I}(n^{1/d})$$

Et si…

$$\begin{aligned}
\mathsf{I}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathsf{I}^{\ominus}(n^{1/2}) \\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 1.98^2\,n^{3/4}\,\mathsf{I}^{\ominus}(n^{1/4}) \\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,\mathsf{I}^{\ominus}(n^{1/8}) \\
&\vdots \\
&\leqslant O(n\log n)
\end{aligned}$$

Objectif suivant :

$$\begin{aligned}
\mathsf{I}(n) &\leqslant C\,n\log n + (d-\epsilon)\,n^{1-1/d}\,\mathsf{I}(n^{1/d}) \quad \text{ou} \\
\mathsf{I}\left(\frac{n^d}{d-\epsilon}\right) &\leqslant C\,n^d\log n + n^{d-1}\,\mathsf{I}(n)
\end{aligned}$$

Transformations polynomiales de Nussbaumer

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

Schönhage–Strassen

$$\mathbb{L}[x]/(x^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^n$$

$$\mathsf{mul}_{\mathbb{L}[x]/(x^n-1)} \leqslant n\,\mathsf{mul}_{\mathbb{L}} + O(n^2 \log n)$$

Transformations polynomiales de Nussbaumer

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

Schönhage–Strassen

$$\mathbb{L}[x]/(x^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^n$$

$$\mathsf{mul}_{\mathbb{L}[x]/(x^n-1)} \leqslant n\,\mathsf{mul}_{\mathbb{L}} + O(n^2 \log n)$$

Nussbaumer

$$\mathbb{L}[u_2, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^{n^{d-1}}$$

$$\mathsf{mul}_{\mathbb{L}[u_2,\ldots,u_d]/(u_2^n-1,\ldots,u_d^n-1)} \leqslant n^{d-1}\,\mathsf{mul}_{\mathbb{L}} + O(n^d \log n)$$

Transformations polynomiales de Nussbaumer

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

Schönhage–Strassen

$$\mathbb{L}[x]/(x^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^n$$

$$\mathsf{mul}_{\mathbb{L}[x]/(x^n-1)} \leqslant n\,\mathsf{mul}_{\mathbb{L}} + O(n^2 \log n)$$

Nussbaumer

$$\mathbb{L}[u_2, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^{n^{d-1}}$$

$$\mathsf{mul}_{\mathbb{L}[u_2,\ldots,u_d]/(u_2^n-1,\ldots,u_d^n-1)} \leqslant n^{d-1}\,\mathsf{mul}_{\mathbb{L}} + O(n^d \log n)$$

Objectif suivant :

$$\mathbb{K}[x]/(x^{n^d/(d-\epsilon)} - 1) \overset{?}{\longrightarrow} \mathbb{K}[u_1, \ldots, u_d]/(u_1^n - 1, \ldots, u_d^n - 1)$$

Restes chinois à la Good

$s_1, \ldots, s_d$ deux à deux premiers entres eux

Restes chinois à la Good

$s_1, \ldots, s_d$ deux à deux premiers entres eux

FFT de Good

$$\mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) \;\cong\; \mathbb{K}[u_1, \ldots, u_d]/(u_1^{s_1} - 1, \ldots, u_d^{s_d} - 1)$$

Restes chinois à la Good

$s_1, \dots, s_d$ deux à deux premiers entres eux

FFT de Good

$$\mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) \;\cong\; \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1)$$

Cadre

- d fixé une fois pour toute (suffisamment grand)
- $s_1 = 2^l$
- $s_k = (1 - o(1))\, 2^l$ ou $s_k = (1 - o(1))\, 2^{l-1}$, $\qquad k = 2, \dots, d$

Restes chinois à la Good

$s_1, \dots, s_d$ deux à deux premiers entres eux

FFT de Good

$$\mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) \;\cong\; \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1)$$

Cadre

- d fixé une fois pour toute (suffisamment grand)
- $s_1 = 2^l$
- $s_k = (1 - o(1))\, 2^l$ ou $s_k = (1 - o(1))\, 2^{l-1}$, $\qquad k = 2, \dots, d$

$$\mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1) \xrightarrow{\;?\;} \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_1} - 1)$$

Première approche par Rader

$$\mathbb{K}[u_1,\ldots,u_d]/(u_1^{s_1}-1,\ldots,u_d^{s_d}-1) \xrightarrow{?} \mathbb{K}[u_1,\ldots,u_d]/(u_1^{s_1}-1,\ldots,u_d^{s_1}-1)$$

Première approche par Rader

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_d}-1) \xrightarrow{?} \mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_1}-1)$$

$$\searrow$$

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,u_2^{\epsilon_2 s_1+1}-1,\dots,u_d^{\epsilon_d s_1+1}-1)$$

Première approche par Rader

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_d}-1) \xrightarrow{?} \mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_1}-1)$$

$$\searrow$$

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1, u_2^{\epsilon_2 s_1+1}-1,\dots,u_d^{\epsilon_d s_1+1}-1)$$

Exemple

$$s_1 = 2^8, \qquad s_2 = 2^8+1, \qquad s_3 = 3\cdot 2^8+1, \qquad s_4 = 13\cdot 2^8+1$$

Première approche par Rader

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_d}-1) \xrightarrow{?} \mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_1}-1)$$

$$\searrow$$

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1, u_2^{\epsilon_2 s_1+1}-1,\dots,u_d^{\epsilon_d s_1+1}-1)$$

Exemple

$$s_1 = 2^8, \qquad s_2 = 2^8+1, \qquad s_3 = 3\cdot 2^8+1, \qquad s_4 = 13\cdot 2^8+1$$

Constante de Linnik

$$\begin{aligned} P(a,k) &:= \min\{ck+a : c\in\mathbb{N}, ck+a \text{ est premier}\} \\ P(k) &:= \max\{P(a,k) : 0<a<k, a\wedge k = 1\} \\ L \text{ constante de Linnik} &:\Longleftrightarrow P(k) = O(k^L) \end{aligned}$$

Première approche par Rader

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_d}-1) \xrightarrow{?} \mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,\dots,u_d^{s_1}-1)$$

$$\searrow$$

$$\mathbb{K}[u_1,\dots,u_d]/(u_1^{s_1}-1,u_2^{\epsilon_2 s_1+1}-1,\dots,u_d^{\epsilon_d s_1+1}-1)$$

Exemple

$$s_1 = 2^8, \qquad s_2 = 2^8+1, \qquad s_3 = 3\cdot 2^8+1, \qquad s_4 = 13\cdot 2^8+1$$

Constante de Linnik

$$\begin{aligned} P(a,k) &:= \min\{ck+a : c\in\mathbb{N}, ck+a \text{ est premier}\} \\ P(k) &:= \max\{P(a,k) : 0<a<k, a\wedge k=1\} \\ L \text{ constante de Linnik} &:\Longleftrightarrow P(k) = O(k^L) \end{aligned}$$

Empiriquement : $P(k) = O(k\log^2 k)$

Constante de Linnik

$$\begin{aligned} P(a,k) &:= \min\{ck+a : c\in\mathbb{N}, ck+a \text{ est premier}\} \\ P(k) &:= \max\{P(a,k) : 0<a<k, a\wedge k = 1\} \\ L \text{ constante de Linnik} &:\Longleftrightarrow P(k) = O(k^L) \end{aligned}$$

Théorème

S'il existe une constante de Linnik $L < 1 + \frac{1}{303}$, alors

$$I(N) = O(N \log N).$$

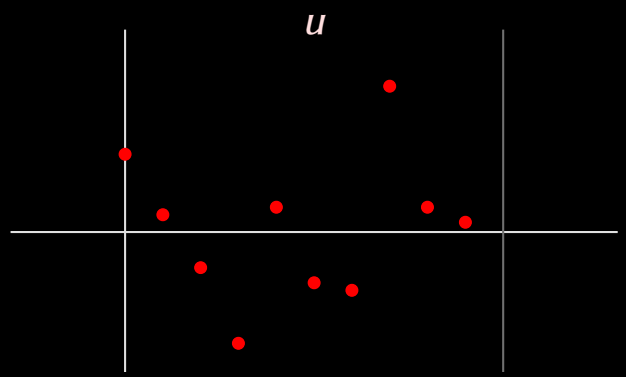
Théorème

S'il existe une constante de Linnik $L < 1 + 2^{-1162}$, alors

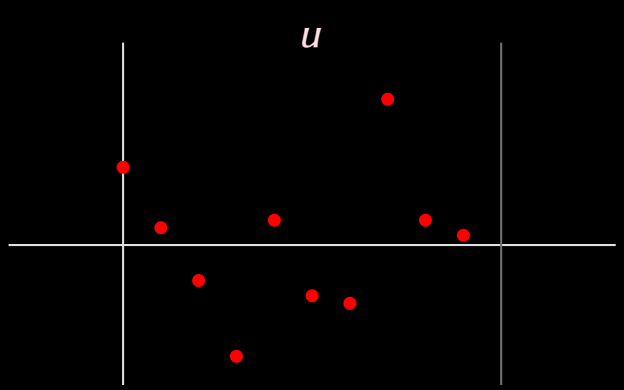
$$M_{\mathbb{F}_q}(n) = O(n \log q \log(n \log q)),$$

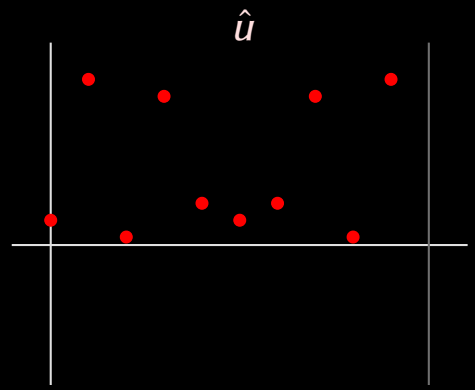
uniformément en q.

Rééchantillonage gaussien

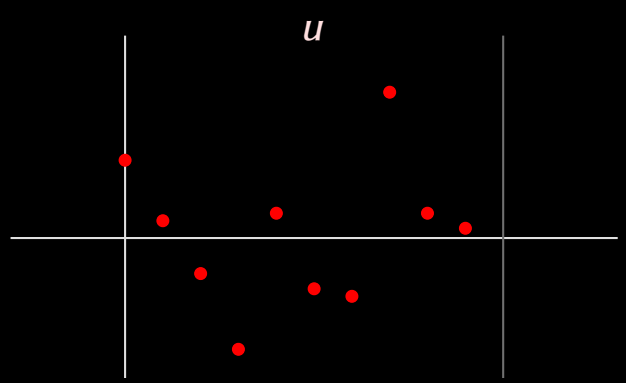


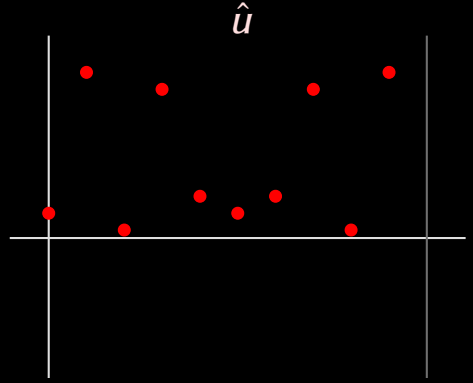
Rééchantillonage gaussien

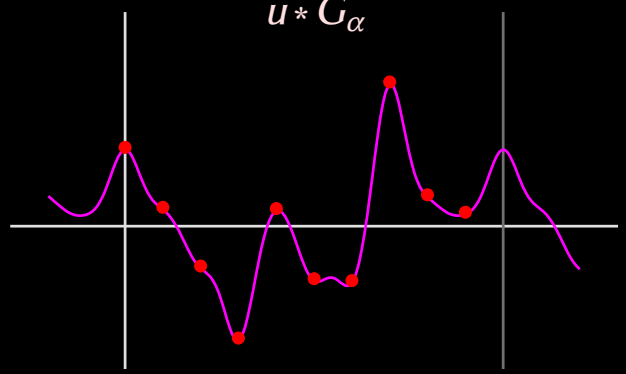




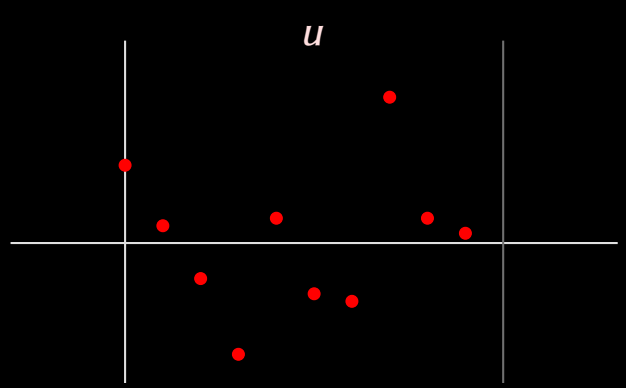
Rééchantillonage gaussien

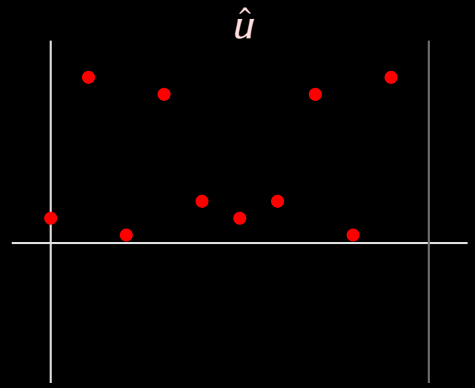


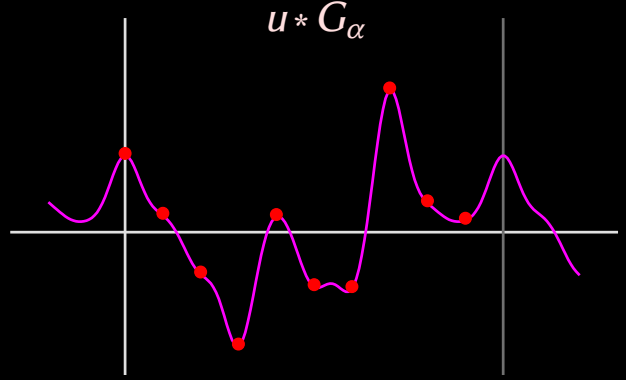


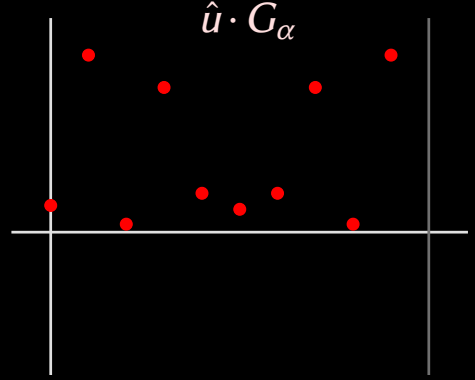


Rééchantillonage gaussien

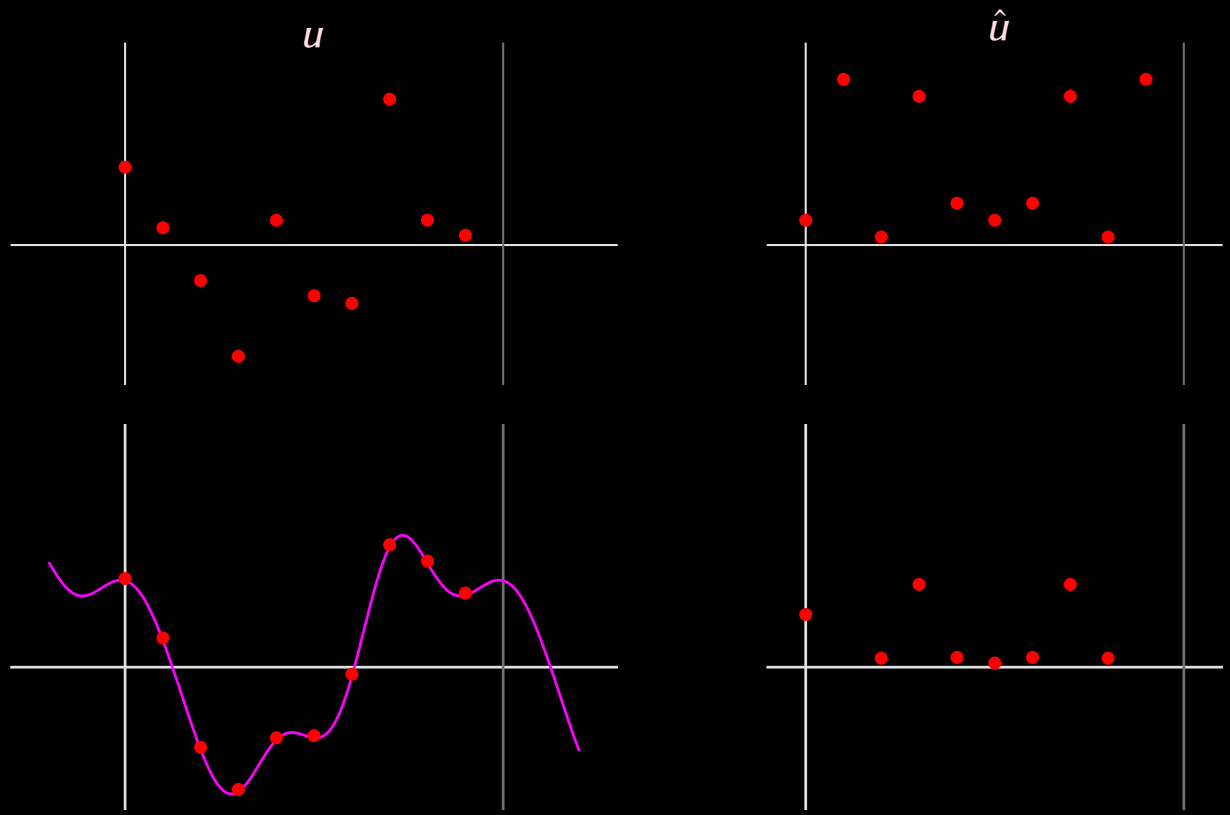




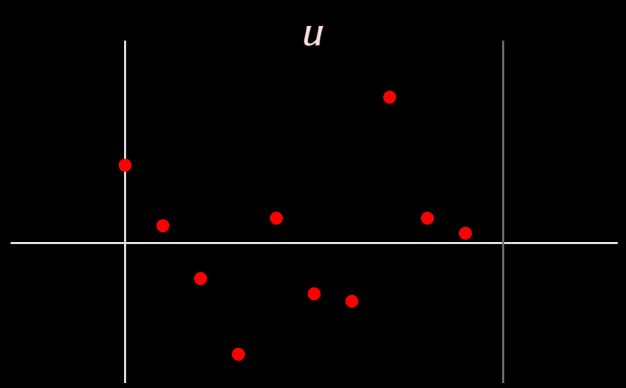


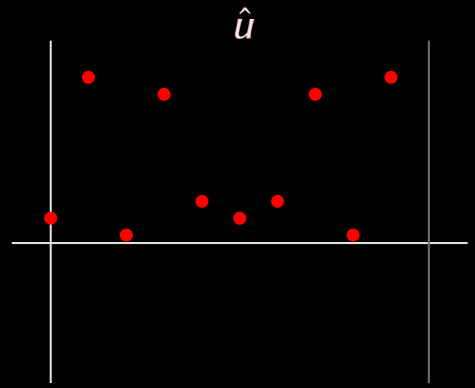


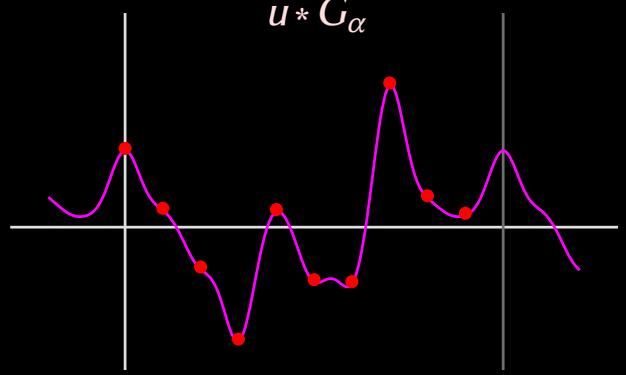
Rééchantillonage gaussien

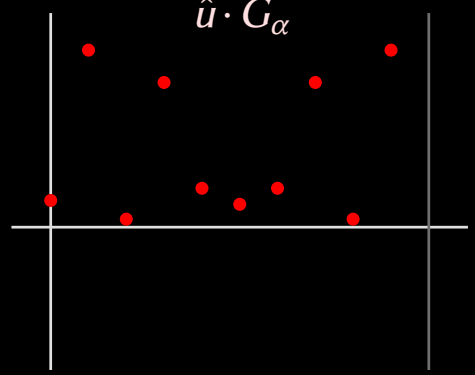


Rééchantillonage gaussien

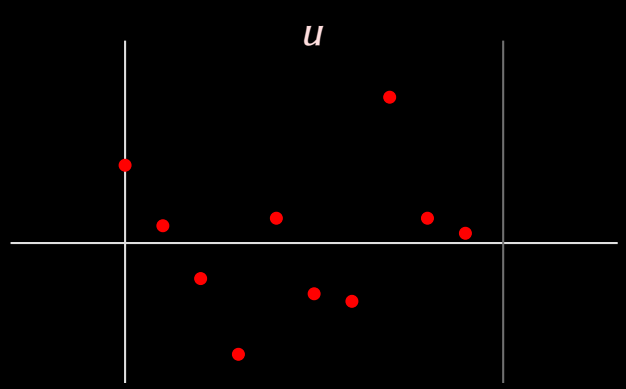


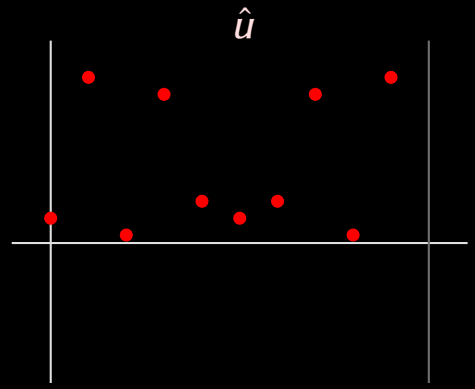


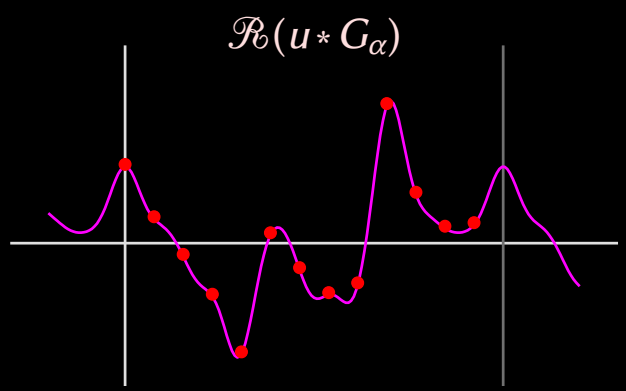


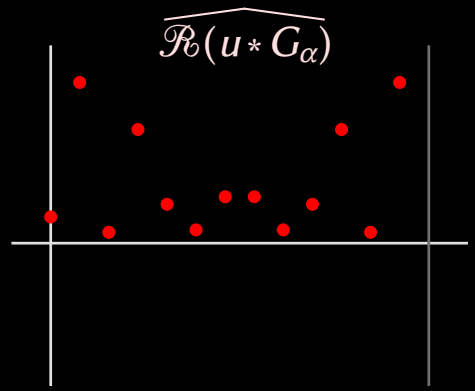


Rééchantillonage gaussien





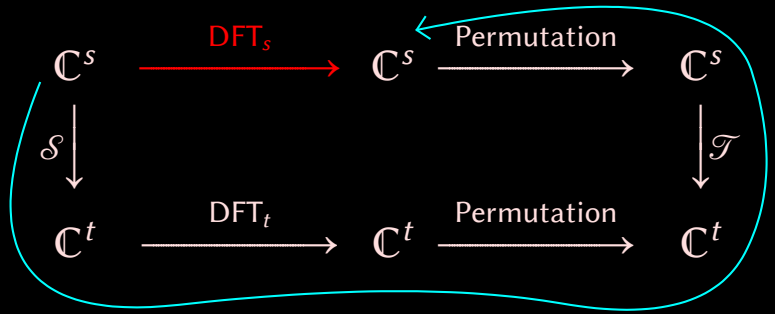




$$\begin{array}{ccccc}
\mathbb{C}^s & \xrightarrow{\mathrm{DFT}_s} & \mathbb{C}^s & \xrightarrow{\text{Permutation}} & \mathbb{C}^s \\
\Big\downarrow{\scriptstyle \mathcal{S}} & & & & \Big\downarrow{\scriptstyle \mathcal{T}} \\
\mathbb{C}^t & \xrightarrow{\mathrm{DFT}_t} & \mathbb{C}^t & \xrightarrow{\text{Permutation}} & \mathbb{C}^t
\end{array}$$

$$\begin{aligned}
(\mathcal{S}\,u)_k &:= \alpha^{-1} \sum_{j\in\mathbb{Z}} \mathrm{e}^{-\pi\alpha^{-2}s^2(\frac{k}{t}-\frac{j}{s})^2}\, u_j \\
(\mathcal{T}\,u)_k &:= \sum_{j\in\mathbb{Z}} \mathrm{e}^{-\pi\alpha^{2}t^2(\frac{k}{t}-\frac{j}{s})^2}\, u_j
\end{aligned}$$

Rééchantillonage gaussien



$$(\mathcal{S}\,u)_k := \alpha^{-1} \sum_{j\in\mathbb{Z}} \mathrm{e}^{-\pi\alpha^{-2}s^2(\frac{k}{t}-\frac{j}{s})^2}\, u_j$$

$$(\mathcal{T}\,u)_k := \sum_{j\in\mathbb{Z}} \mathrm{e}^{-\pi\alpha^{2}t^2(\frac{k}{t}-\frac{j}{s})^2}\, u_j$$

Matrice pour $\mathcal{S}$ quand $s = 10$, $t = 13$ et $\alpha = 2$

$$\begin{bmatrix}
0.5000 & 0.2280 & 0.0216 & 4.2e\text{-}4 & 1.7e\text{-}6 & 2.9e\text{-}9 & 1.7e\text{-}6 & 4.2e\text{-}4 & 0.0216 & 0.2280 \\
0.3142 & 0.4795 & 0.1522 & 0.0100 & 1.3e\text{-}4 & 3.9e\text{-}7 & 8.9e\text{-}9 & 7.1e\text{-}6 & 0.0012 & 0.0428 \\
0.0779 & 0.3982 & 0.4230 & 0.0934 & 0.0043 & 4.0e\text{-}5 & 8.1e\text{-}8 & 4.7e\text{-}8 & 2.6e\text{-}5 & 0.0032 \\
0.0076 & 0.1305 & 0.4642 & 0.3432 & 0.0527 & 0.0017 & 1.1e\text{-}5 & 1.5e\text{-}8 & 2.3e\text{-}7 & 9.2e\text{-}5 \\
2.9e\text{-}4 & 0.0169 & 0.2011 & 0.4977 & 0.2561 & 0.0274 & 6.0e\text{-}4 & 2.8e\text{-}6 & 3.5e\text{-}9 & 1.0e\text{-}6 \\
4.4e\text{-}6 & 8.6e\text{-}4 & 0.0344 & 0.2849 & 0.4908 & 0.1757 & 0.0131 & 2.0e\text{-}4 & 6.5e\text{-}7 & 5.3e\text{-}9 \\
2.7e\text{-}8 & 1.7e\text{-}5 & 0.0023 & 0.0644 & 0.3714 & 0.4452 & 0.1109 & 0.0057 & 6.1e\text{-}5 & 1.3e\text{-}7 \\
2.7e\text{-}8 & 1.3e\text{-}7 & 6.1e\text{-}5 & 0.0057 & 0.1109 & 0.4452 & 0.3714 & 0.0644 & 0.0023 & 1.7e\text{-}5 \\
4.4e\text{-}6 & 5.3e\text{-}9 & 6.5e\text{-}7 & 2.0e\text{-}4 & 0.0131 & 0.1757 & 0.4908 & 0.2849 & 0.0344 & 8.6e\text{-}4 \\
2.9e\text{-}4 & 1.0e\text{-}6 & 3.5e\text{-}9 & 2.8e\text{-}6 & 6.0e\text{-}4 & 0.0274 & 0.2561 & 0.4977 & 0.2011 & 0.0169 \\
0.0076 & 9.2e\text{-}5 & 2.3e\text{-}7 & 1.5e\text{-}8 & 1.1e\text{-}5 & 0.0017 & 0.0527 & 0.3432 & 0.4642 & 0.1305 \\
0.0779 & 0.0032 & 2.6e\text{-}5 & 4.7e\text{-}8 & 8.1e\text{-}8 & 4.0e\text{-}5 & 0.0043 & 0.0934 & 0.4230 & 0.3982 \\
0.3142 & 0.0428 & 0.0012 & 7.1e\text{-}6 & 8.9e\text{-}9 & 3.9e\text{-}7 & 1.3e\text{-}4 & 0.0100 & 0.1522 & 0.4795
\end{bmatrix}$$

Matrice pour $\mathscr{T}$ quand $s = 10$, $t = 13$ et $\alpha = 2$

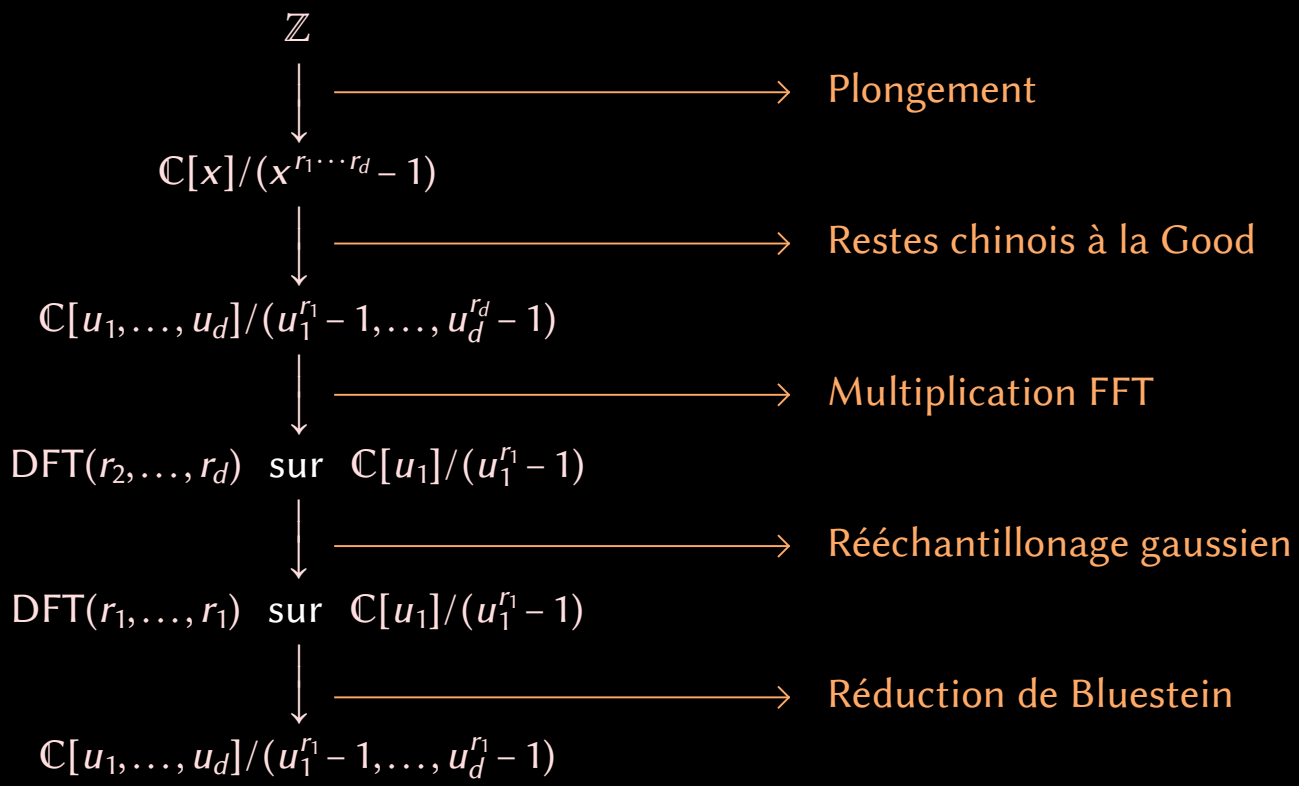
$$\begin{bmatrix}
1.0000 & 5.9e\text{-}10 & 1.2e\text{-}37 & 9.8e\text{-}84 & 2.6e\text{-}148 & 5.2e\text{-}231 & 2.6e\text{-}148 & 9.8e\text{-}84 & 1.2e\text{-}37 & 5.9e\text{-}10 \\
3.4e\text{-}6 & 0.3227 & 1.0e\text{-}14 & 1.2e\text{-}46 & 5.3e\text{-}97 & 8.1e\text{-}166 & 1.6e\text{-}210 & 9.2e\text{-}132 & 1.8e\text{-}71 & 1.3e\text{-}29 \\
1.4e\text{-}22 & 0.0021 & 0.0108 & 1.9e\text{-}20 & 1.3e\text{-}56 & 3.0e\text{-}111 & 2.5e\text{-}184 & 1.0e\text{-}190 & 3.3e\text{-}116 & 3.6e\text{-}60 \\
7.6e\text{-}50 & 1.6e\text{-}16 & 0.1339 & 3.7e\text{-}5 & 3.8e\text{-}27 & 1.3e\text{-}67 & 1.8e\text{-}126 & 8.4e\text{-}204 & 7.1e\text{-}172 & 1.2e\text{-}101 \\
4.7e\text{-}88 & 1.6e\text{-}40 & 2.0e\text{-}11 & 0.8819 & 1.3e\text{-}8 & 7.7e\text{-}35 & 1.5e\text{-}79 & 1.1e\text{-}142 & 2.8e\text{-}224 & 4.9e\text{-}154 \\
3.6e\text{-}137 & 1.9e\text{-}75 & 3.6e\text{-}32 & 2.4e\text{-}7 & 0.6049 & 5.2e\text{-}13 & 1.6e\text{-}43 & 1.8e\text{-}92 & 7.2e\text{-}160 & 2.4e\text{-}217 \\
3.3e\text{-}197 & 2.7e\text{-}121 & 8.1e\text{-}64 & 8.5e\text{-}25 & 3.2e\text{-}4 & 0.0432 & 2.0e\text{-}18 & 3.5e\text{-}53 & 2.2e\text{-}106 & 4.8e\text{-}178 \\
3.3e\text{-}197 & 4.8e\text{-}178 & 2.2e\text{-}106 & 3.5e\text{-}53 & 2.0e\text{-}18 & 0.0432 & 3.2e\text{-}4 & 8.5e\text{-}25 & 8.1e\text{-}64 & 2.7e\text{-}121 \\
3.6e\text{-}137 & 2.4e\text{-}217 & 7.2e\text{-}160 & 1.8e\text{-}92 & 1.6e\text{-}43 & 5.2e\text{-}13 & 0.6049 & 2.4e\text{-}7 & 3.6e\text{-}32 & 1.9e\text{-}75 \\
4.7e\text{-}88 & 4.9e\text{-}154 & 2.8e\text{-}224 & 1.1e\text{-}142 & 1.5e\text{-}79 & 7.7e\text{-}35 & 1.3e\text{-}8 & 0.8819 & 2.0e\text{-}11 & 1.6e\text{-}40 \\
7.6e\text{-}50 & 1.2e\text{-}101 & 7.1e\text{-}172 & 8.4e\text{-}204 & 1.8e\text{-}126 & 1.3e\text{-}67 & 3.8e\text{-}27 & 3.7e\text{-}5 & 0.1339 & 1.6e\text{-}16 \\
1.4e\text{-}22 & 3.6e\text{-}60 & 3.3e\text{-}116 & 1.0e\text{-}190 & 2.5e\text{-}184 & 3.0e\text{-}111 & 1.3e\text{-}56 & 1.9e\text{-}20 & 0.0108 & 0.0021 \\
3.4e\text{-}6 & 1.3e\text{-}29 & 1.8e\text{-}71 & 9.2e\text{-}132 & 1.6e\text{-}210 & 8.1e\text{-}166 & 5.3e\text{-}97 & 1.2e\text{-}46 & 1.0e\text{-}14 & 0.3227
\end{bmatrix}$$

Matrice pour $\mathscr{T}$ quand $s = 10$, $t = 13$ et $\alpha = 2$

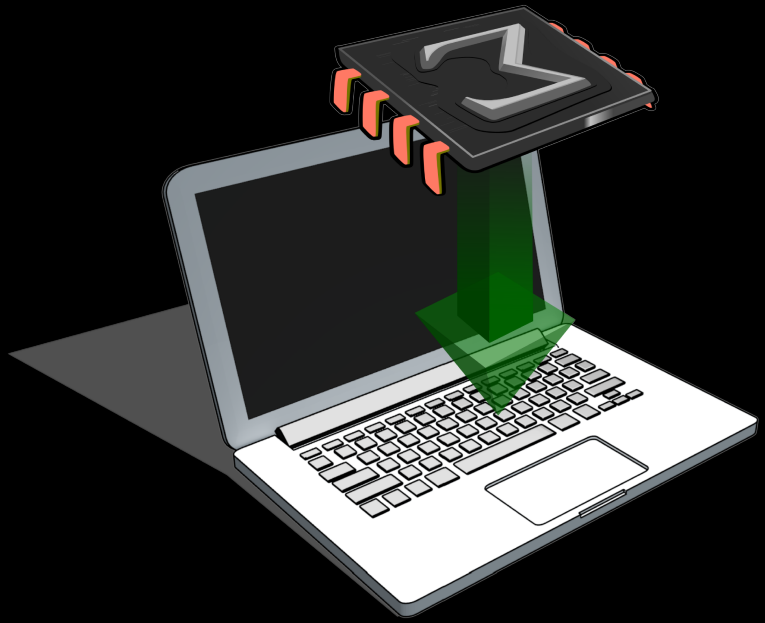
$$\begin{bmatrix}
1.0000 & 5.9e\text{-}10 & 1.2e\text{-}37 & 9.8e\text{-}84 & 2.6e\text{-}148 & 5.2e\text{-}231 & 2.6e\text{-}148 & 9.8e\text{-}84 & 1.2e\text{-}37 & 5.9e\text{-}10 \\
3.4e\text{-}6 & 0.3227 & 1.0e\text{-}14 & 1.2e\text{-}46 & 5.3e\text{-}97 & 8.1e\text{-}166 & 1.6e\text{-}210 & 9.2e\text{-}132 & 1.8e\text{-}71 & 1.3e\text{-}29 \\
1.4e\text{-}22 & 0.0021 & 0.0108 & 1.9e\text{-}20 & 1.3e\text{-}56 & 3.0e\text{-}111 & 2.5e\text{-}184 & 1.0e\text{-}190 & 3.3e\text{-}116 & 3.6e\text{-}60 \\
7.6e\text{-}50 & 1.6e\text{-}16 & 0.1339 & 3.7e\text{-}5 & 3.8e\text{-}27 & 1.3e\text{-}67 & 1.8e\text{-}126 & 8.4e\text{-}204 & 7.1e\text{-}172 & 1.2e\text{-}101 \\
4.7e\text{-}88 & 1.6e\text{-}40 & 2.0e\text{-}11 & 0.8819 & 1.3e\text{-}8 & 7.7e\text{-}35 & 1.5e\text{-}79 & 1.1e\text{-}142 & 2.8e\text{-}224 & 4.9e\text{-}154 \\
3.6e\text{-}137 & 1.9e\text{-}75 & 3.6e\text{-}32 & 2.4e\text{-}7 & 0.6049 & 5.2e\text{-}13 & 1.6e\text{-}43 & 1.8e\text{-}92 & 7.2e\text{-}160 & 2.4e\text{-}217 \\
3.3e\text{-}197 & 2.7e\text{-}121 & 8.1e\text{-}64 & 8.5e\text{-}25 & 3.2e\text{-}4 & 0.0432 & 2.0e\text{-}18 & 3.5e\text{-}53 & 2.2e\text{-}106 & 4.8e\text{-}178 \\
3.3e\text{-}197 & 4.8e\text{-}178 & 2.2e\text{-}106 & 3.5e\text{-}53 & 2.0e\text{-}18 & 0.0432 & 3.2e\text{-}4 & 8.5e\text{-}25 & 8.1e\text{-}64 & 2.7e\text{-}121 \\
3.6e\text{-}137 & 2.4e\text{-}217 & 7.2e\text{-}160 & 1.8e\text{-}92 & 1.6e\text{-}43 & 5.2e\text{-}13 & 0.6049 & 2.4e\text{-}7 & 3.6e\text{-}32 & 1.9e\text{-}75 \\
4.7e\text{-}88 & 4.9e\text{-}154 & 2.8e\text{-}224 & 1.1e\text{-}142 & 1.5e\text{-}79 & 7.7e\text{-}35 & 1.3e\text{-}8 & 0.8819 & 2.0e\text{-}11 & 1.6e\text{-}40 \\
7.6e\text{-}50 & 1.2e\text{-}101 & 7.1e\text{-}172 & 8.4e\text{-}204 & 1.8e\text{-}126 & 1.3e\text{-}67 & 3.8e\text{-}27 & 3.7e\text{-}5 & 0.1339 & 1.6e\text{-}16 \\
1.4e\text{-}22 & 3.6e\text{-}60 & 3.3e\text{-}116 & 1.0e\text{-}190 & 2.5e\text{-}184 & 3.0e\text{-}111 & 1.3e\text{-}56 & 1.9e\text{-}20 & 0.0108 & 0.0021 \\
3.4e\text{-}6 & 1.3e\text{-}29 & 1.8e\text{-}71 & 9.2e\text{-}132 & 1.6e\text{-}210 & 8.1e\text{-}166 & 5.3e\text{-}97 & 1.2e\text{-}46 & 1.0e\text{-}14 & 0.3227
\end{bmatrix}$$

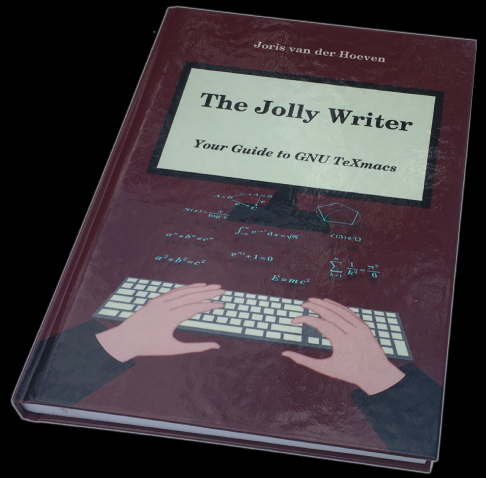
$$\frac{t}{s} \geqslant 1 + \frac{1}{\alpha^2} \Longrightarrow \mathrm{DFT}_s \text{ précise } \textit{via } \mathbb{C}^s \xrightarrow{\mathscr{S}} \mathbb{C}^t \xrightarrow{\mathrm{DFT}_t} \mathbb{C}^t \xrightarrow{\Pi} \mathbb{C}^t \xrightarrow{\mathscr{T}^{-1}} \mathbb{C}^s \xrightarrow{\Pi} \mathbb{C}^s$$

Conclusion


$\mathbb{Z}$
Plongement
$\mathbb{C}[x]/(x^{r_1\cdots r_d}-1)$
Restes chinois à la Good
$\mathbb{C}[u_1,\ldots,u_d]/(u_1^{r_1}-1,\ldots,u_d^{r_d}-1)$
Multiplication FFT
$\mathrm{DFT}(r_2,\ldots,r_d)$ sur $\mathbb{C}[u_1]/(u_1^{r_1}-1)$
Rééchantillonage gaussien
$\mathrm{DFT}(r_1,\ldots,r_1)$ sur $\mathbb{C}[u_1]/(u_1^{r_1}-1)$
Réduction de Bluestein
$\mathbb{C}[u_1,\ldots,u_d]/(u_1^{r_1}-1,\ldots,u_d^{r_1}-1)$

Merci !





http://www.TeXmacs.org

Multiplication rapide II

Joris van der Hoeven

CNRS, École polytechnique

Complexités de multiplication

b précision en chiffres binaires
d degré ou ordre
r taille d'une matrice ou ordre différentiel
s taille d'un support creux

Algèbre	Complexité	Notes	Référence
$\mathbb{Z}_p$	$\mathsf{I}(b)\,\mathrm{e}^{O\left(\sqrt{\log\log b}\right)}$	détendu	vdH
$\mathbb{K}[[z]]$	$\mathsf{M}_{\mathbb{K}}(d)\,\mathrm{e}^{O\left(\sqrt{\log\log d}\right)}$	détendu	vdH
$\mathbb{K}^{r\times r}[x]$	$O(\Omega_{\mathbb{K}}(r)\,d + r^2\,\mathsf{M}_{\mathbb{K}}(d))$	$\lvert\,\mathbb{K}\,\rvert > d$	Bostan–Schost
$\mathbb{K}[x,\partial_x]$	$O\left(\Omega_{\mathbb{K}}(r)\,{}^{d}\!/_{r} + r\,\mathsf{M}_{\mathbb{K}}(d)\log d\right)$	$d \geqslant r := \deg_\partial$	Benoit–Bostan–vdH
	$O(\Omega_{\mathbb{K}}(d)\,{}^{r}\!/_{d} + d\,\mathsf{M}_{\mathbb{K}}(r)\log r)$	$r \geqslant d := \deg_x$	
$\mathbb{L} \mid \mathbb{K}$ tower	$\mathsf{M}_{\mathbb{K}}(d)\,\mathrm{e}^{O\left(\sqrt{\log d}\right)}$	$d = [\mathbb{L}:\mathbb{K}]$	vdH–Lecerf
$\mathbb{K}[x_1,\ldots,x_n]$	$O(\mathsf{M}_{\mathbb{K}}(s))$	creux, heuristique	vdH–Lecerf, vdH

Évaluation-interpolation et opérations transposées

Évaluation multi-points : $P \in \mathbb{K}[x]$, $\deg P < d$, $\alpha_1, \ldots, \alpha_d \in \mathbb{K} \xrightarrow{?} P(\alpha_1), \ldots, P(\alpha_d)$

Évaluation-interpolation et opérations transposées

Évaluation multi-points : $P \in \mathbb{K}[x]$, $\deg P < d$, $\alpha_1, \ldots, \alpha_d \in \mathbb{K} \xrightarrow{?} P(\alpha_1), \ldots, P(\alpha_d)$

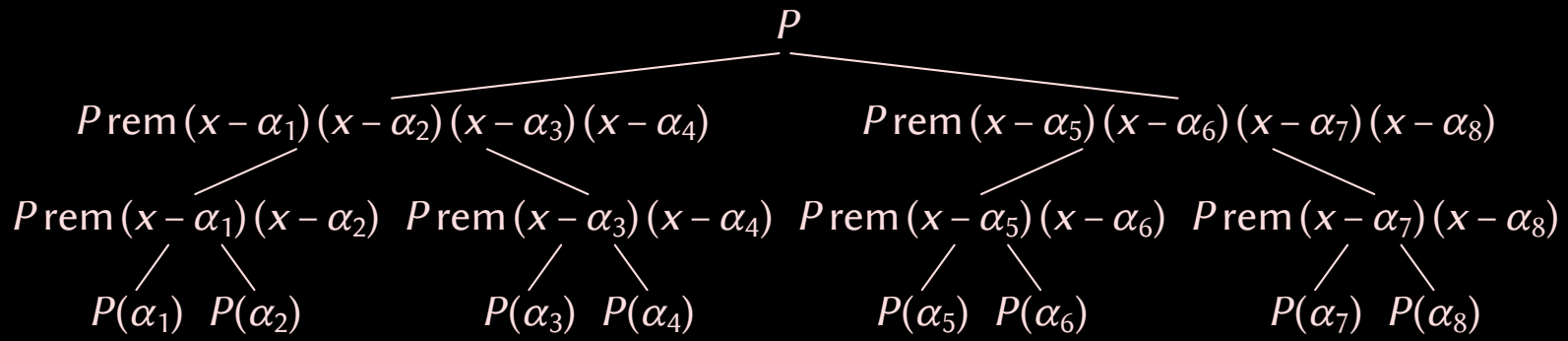
Observation : $P(\alpha_k) = P \operatorname{rem} (x - \alpha_k)$

Évaluation-interpolation et opérations transposées

Évaluation multi-points : $P \in \mathbb{K}[x]$, $\deg P < d$, $\alpha_1, \ldots, \alpha_d \in \mathbb{K} \xrightarrow{?} P(\alpha_1), \ldots, P(\alpha_d)$

Observation : $P(\alpha_k) = P \operatorname{rem} (x - \alpha_k)$

Arbre de restes

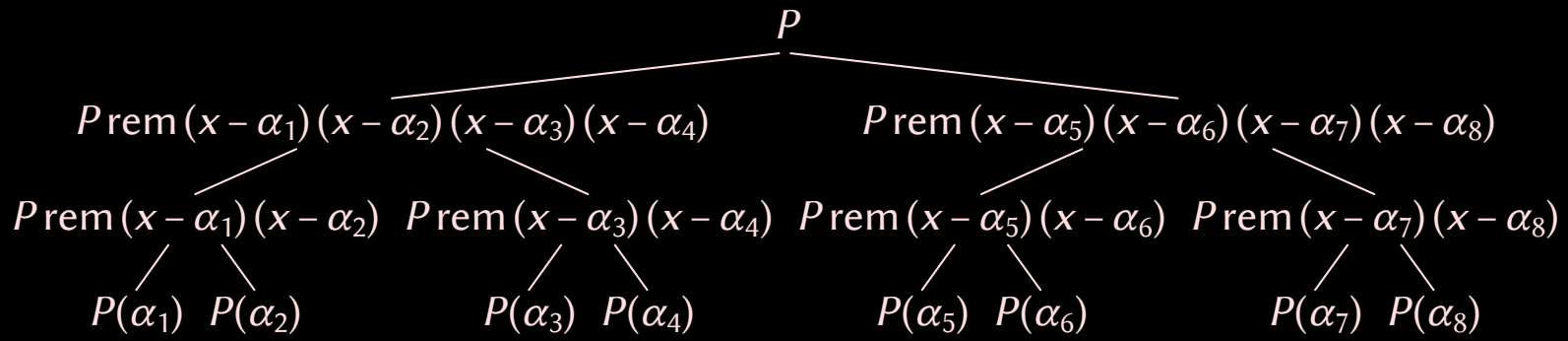


Évaluation-interpolation et opérations transposées

Évaluation multi-points : $P \in \mathbb{K}[x]$, $\deg P < d$, $\alpha_1, \ldots, \alpha_d \in \mathbb{K} \xrightarrow{?} P(\alpha_1), \ldots, P(\alpha_d)$

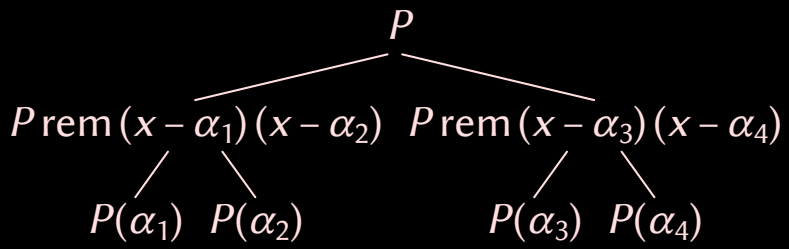
Observation : $P(\alpha_k) = P \operatorname{rem} (x - \alpha_k)$

Arbre de restes



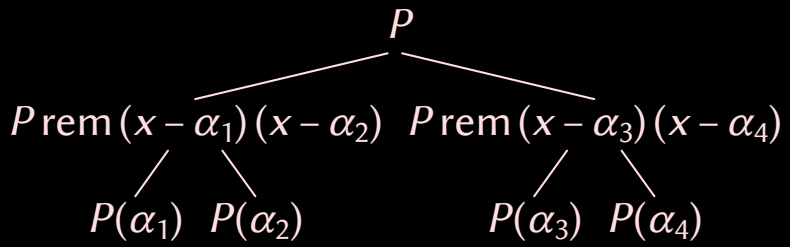
$$\mathrm{E}_{\mathbb{K}}(d) = O(2\,\mathrm{M}_{\mathbb{K}}(d/2) + 4\,\mathrm{M}_{\mathbb{K}}(d/4) + \cdots) = O(\mathrm{M}_{\mathbb{K}}(d) \log d)$$

Arbres de restes



$$\begin{aligned} \mathsf{E}_{\mathbb{K}}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \\ \mathsf{E}_{\mathbb{K}}^{-1}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \end{aligned}$$

Arbres de restes



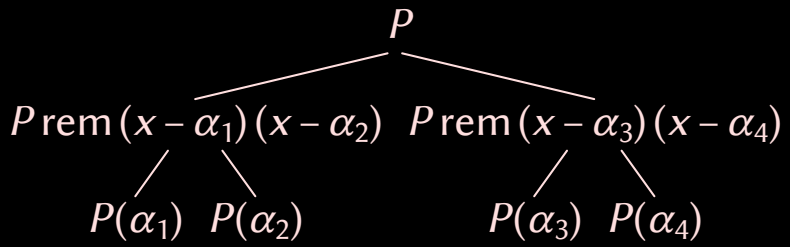
$$\begin{aligned} \mathsf{E}_{\mathbb{K}}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \\ \mathsf{E}_{\mathbb{K}}^{-1}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \end{aligned}$$

Évaluation multi-points

$$\begin{pmatrix} P(\alpha_1) \\ \vdots \\ P(\alpha_d) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} P_0 \\ \vdots \\ P_{d-1} \end{pmatrix}$$

Évaluation-interpolation et opérations transposées

Arbres de restes



$$\begin{aligned} \mathsf{E}_{\mathbb{K}}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \\ \mathsf{E}_{\mathbb{K}}^{-1}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \end{aligned}$$

Évaluation multi-points

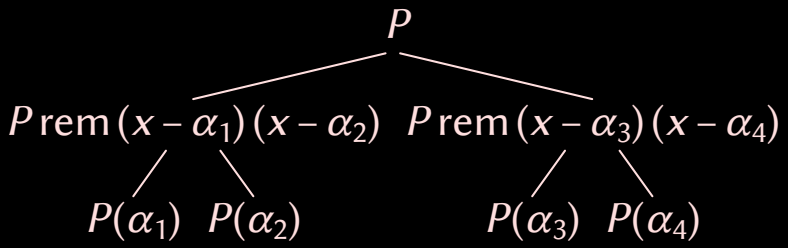
$$\begin{pmatrix} P(\alpha_1) \\ \vdots \\ P(\alpha_d) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} P_0 \\ \vdots \\ P_{d-1} \end{pmatrix}$$

Opération transposée

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_d \\ \vdots & & \vdots \\ \alpha_1^{d-1} & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{pmatrix}$$

Évaluation-interpolation et opérations transposées

Arbres de restes



$$\begin{aligned} \mathsf{E}_{\mathbb{K}}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \\ \mathsf{E}_{\mathbb{K}}^{-1}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \end{aligned}$$

$$\begin{aligned} \mathsf{E}_{\mathbb{K}}^{\top}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \\ \mathsf{E}_{\mathbb{K}}^{-1,\top}(d) &= O(\mathsf{M}_{\mathbb{K}}(d)\log d) \end{aligned}$$

Évaluation multi-points

$$\begin{pmatrix} P(\alpha_1) \\ \vdots \\ P(\alpha_d) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_1 & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} P_0 \\ \vdots \\ P_{d-1} \end{pmatrix}$$

Opération transposée

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_d \\ \vdots & & \vdots \\ \alpha_1^{d-1} & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{pmatrix}$$


$\mathbb{K}^{r\times r}[x]$

Multiplication de polynômes de matrices

Cas 1 : $2d < n, \quad n \sim 2d, \quad \omega^n = 1$

Multiplication de polynômes de matrices

Cas 1 : $2d < n, \quad n \sim 2d, \quad \omega^n = 1$

$\longrightarrow$ Multiplication FFT à coefficients dans $\mathbb{K}^{r \times r}$

Cas 1 : $2d < n$, $n \sim 2d$, $\omega^n = 1$

$\longrightarrow$ Multiplication FFT à coefficients dans $\mathbb{K}^{r\times r}$

$$\begin{aligned} \mathsf{M}_{\mathbb{K}^{r\times r}}(d) &\leqslant 3\,\mathsf{F}_{\mathbb{K}^{r\times r}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &= 3\,r^2\,\mathsf{F}_{\mathbb{K}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &\lesssim r^2\,\mathsf{M}_{\mathbb{K}}(d) + n\,\Omega_{\mathbb{K}}(r). \end{aligned}$$

Multiplication de polynômes de matrices

Cas 1 : $2d < n$, $n \sim 2d$, $\omega^n = 1$

$\longrightarrow$ Multiplication FFT à coefficients dans $\mathbb{K}^{r\times r}$

$$\begin{aligned} \mathsf{M}_{\mathbb{K}^{r\times r}}(d) &\leqslant 3\,\mathsf{F}_{\mathbb{K}^{r\times r}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &= 3\,r^2\,\mathsf{F}_{\mathbb{K}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &\lesssim r^2\,\mathsf{M}_{\mathbb{K}}(d) + n\,\Omega_{\mathbb{K}}(r). \end{aligned}$$

Cas 2 : $2d < n$, $n = O(d)$, $\omega^n = 1$

Multiplication de polynômes de matrices

Cas 1 : $2d < n, \quad n \sim 2d, \quad \omega^n = 1$

$\longrightarrow$ Multiplication FFT à coefficients dans $\mathbb{K}^{r\times r}$

$$\begin{aligned} \mathsf{M}_{\mathbb{K}^{r\times r}}(d) &\leqslant 3\,\mathsf{F}_{\mathbb{K}^{r\times r}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &= 3\,r^2\,\mathsf{F}_{\mathbb{K}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &\lesssim r^2\,\mathsf{M}_{\mathbb{K}}(d) + n\,\Omega_{\mathbb{K}}(r). \end{aligned}$$

Cas 2 : $2d < n, \quad n = O(d), \quad \omega^n = 1$

$\longrightarrow$ Multiplication TFT à coefficients dans $\mathbb{K}^{r\times r}$

Multiplication de polynômes de matrices

Cas 1 : $2d < n$, $n \sim 2d$, $\omega^n = 1$

$\longrightarrow$ Multiplication FFT à coefficients dans $\mathbb{K}^{r\times r}$

$$\begin{aligned} \mathsf{M}_{\mathbb{K}^{r\times r}}(d) &\leqslant 3\,\mathsf{F}_{\mathbb{K}^{r\times r}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &= 3\,r^2\,\mathsf{F}_{\mathbb{K}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &\lesssim r^2\,\mathsf{M}_{\mathbb{K}}(d) + n\,\Omega_{\mathbb{K}}(r). \end{aligned}$$

Cas 2 : $2d < n$, $n = O(d)$, $\omega^n = 1$

$\longrightarrow$ Multiplication TFT à coefficients dans $\mathbb{K}^{r\times r}$

Cas 3 : $|\mathbb{K}| > d$

$\longrightarrow$ Évaluation-interpolation suite géométrique de d points

Multiplication de polynômes de matrices

Cas 1 : $2d < n$, $n \sim 2d$, $\omega^n = 1$

$\longrightarrow$ Multiplication FFT à coefficients dans $\mathbb{K}^{r\times r}$

$$\begin{aligned} \mathsf{M}_{\mathbb{K}^{r\times r}}(d) &\leqslant 3\,\mathsf{F}_{\mathbb{K}^{r\times r}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &= 3\,r^2\,\mathsf{F}_{\mathbb{K}}(n) + n\,\Omega_{\mathbb{K}}(r) \\ &\lesssim r^2\,\mathsf{M}_{\mathbb{K}}(d) + n\,\Omega_{\mathbb{K}}(r). \end{aligned}$$

Cas 2 : $2d < n$, $n = O(d)$, $\omega^n = 1$

$\longrightarrow$ Multiplication TFT à coefficients dans $\mathbb{K}^{r\times r}$

Cas 3 : $|\mathbb{K}| > d$

$\longrightarrow$ Évaluation-interpolation suite géométrique de d points

$$\mathsf{M}_{\mathbb{K}^{r\times r}}(d) \leqslant O(r^2\,\mathsf{M}_{\mathbb{K}}(n)) + n\,\Omega_{\mathbb{K}}(r)$$

Inverse d'une série de matrices

$$M = 1 + M_1 z + M_2 z^2 + \cdots \in \mathbb{K}^{r \times r}[[z]]$$

Calcul de $M^{-1} + O(z^d)$ en temps $O(\mathsf{MM}(d, r))$

Inverse d'une série de matrices

$$M = 1 + M_1 z + M_2 z^2 + \cdots \in \mathbb{K}^{r\times r}[[z]]$$

Calcul de $M^{-1} + O(z^d)$ en temps $O(\mathsf{MM}(d, r))$

Padé–Hermite

$f_1, \ldots, f_r \in \mathbb{K}[[z]]$. Trouver $p_1, \ldots, p_r \in \mathbb{K}[z]$ de degré $<d$ avec

$$p_1 f_1 + \cdots + p_r f_r = O(z^{dr-1})$$

Génériquement en temps $O(\mathsf{MM}(d, r) \log d)$


$\mathbb{K}[[z]]$

Des séries comme « flots » de coefficients

$$f = f_0 + \cdots$$

Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + \cdots$$

Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + f_2 z^2 + \cdots$$

Des séries comme « flots » de coefficients

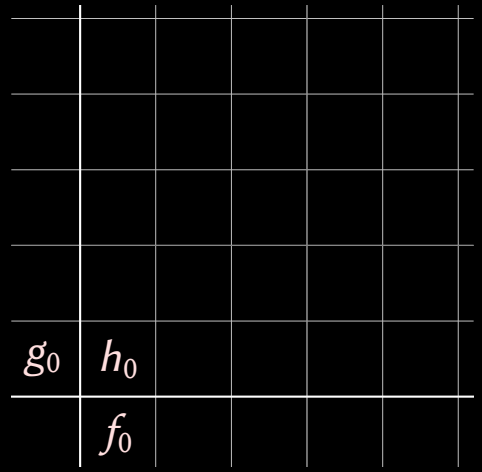
$$f = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots$$

Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots$$

Multiplication paresseuse

$$\begin{aligned} f &= f_0 + \cdots \\ g &= g_0 + \cdots \\ h = fg &= (fg)_0 + \cdots \end{aligned}$$

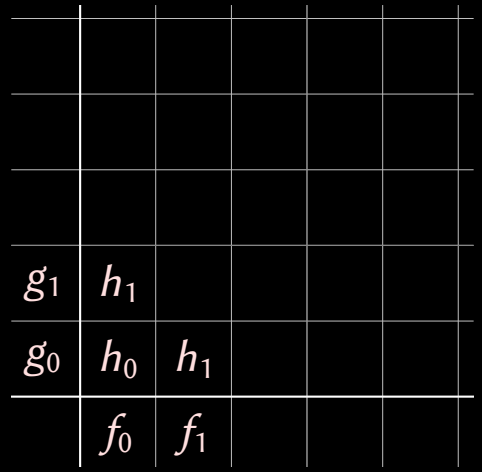


Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots$$

Multiplication paresseuse

$$\begin{aligned} f &= f_0 + f_1 z + \cdots \\ g &= g_0 + g_1 z + \cdots \\ h = fg &= (fg)_0 + (fg)_1 z + \cdots \end{aligned}$$



Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots$$

Multiplication paresseuse

$$\begin{aligned} f &= f_0 + f_1 z + f_2 z^2 + \cdots \\ g &= g_0 + g_1 z + g_2 z^2 + \cdots \\ h = fg &= (fg)_0 + (fg)_1 z + (fg)_2 z^2 + \cdots \end{aligned}$$

g_2	h_2					
g_1	h_1	h_2				
g_0	h_0	h_1	h_2			
	f_0	f_1	f_2			

Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots$$

Multiplication paresseuse

$$\begin{aligned} f &= f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots \\ g &= g_0 + g_1 z + g_2 z^2 + g_3 z^2 + \cdots \\ h = fg &= (fg)_0 + (fg)_1 z + (fg)_2 z^2 + (fg)_3 z^3 + \cdots \end{aligned}$$

g_3	h_3					
g_2	h_2	h_3				
g_1	h_1	h_2	h_3			
g_0	h_0	h_1	h_2	h_3		
	f_0	f_1	f_2	f_3		

Des séries comme « flots » de coefficients

$$f = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots$$

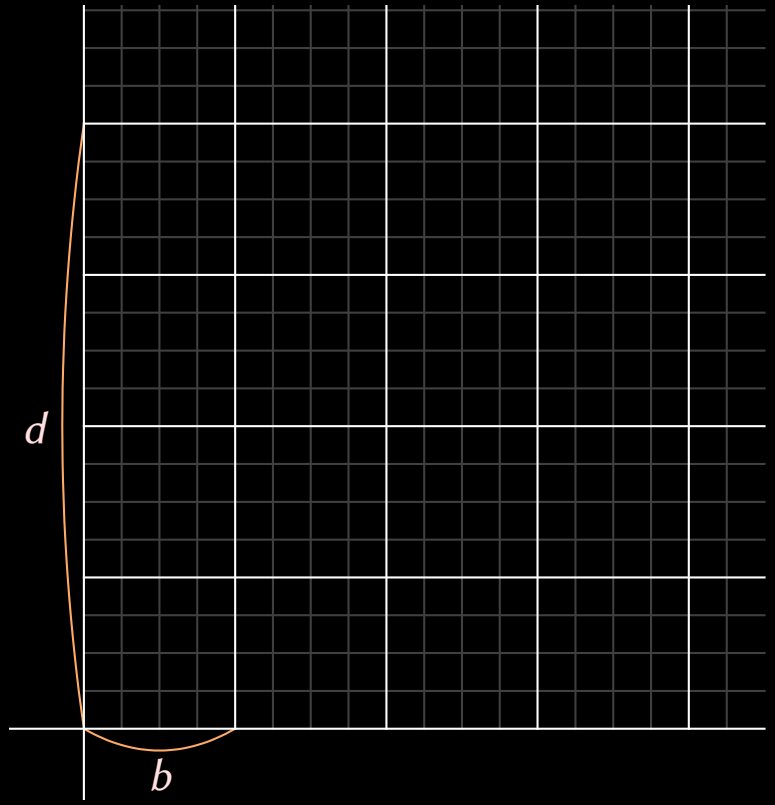
Multiplication paresseuse

$$\begin{aligned} f &= f_0 + f_1 z + f_2 z^2 + f_3 z^3 + \cdots \\ g &= g_0 + g_1 z + g_2 z^2 + g_3 z^2 + \cdots \\ h = fg &= (fg)_0 + (fg)_1 z + (fg)_2 z^2 + (fg)_3 z^3 + \cdots \end{aligned}$$

g_3	h_3					
g_2	h_2	h_3				
g_1	h_1	h_2	h_3			
g_0	h_0	h_1	h_2	h_3		
	f_0	f_1	f_2	f_3		

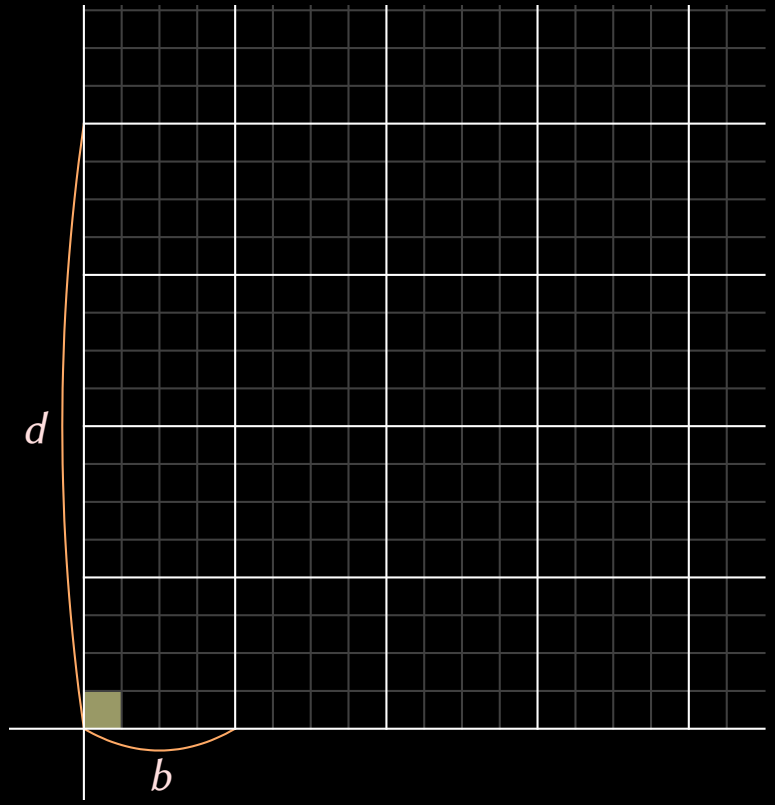
Complexité en $O(d^2)$

Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)\,?$

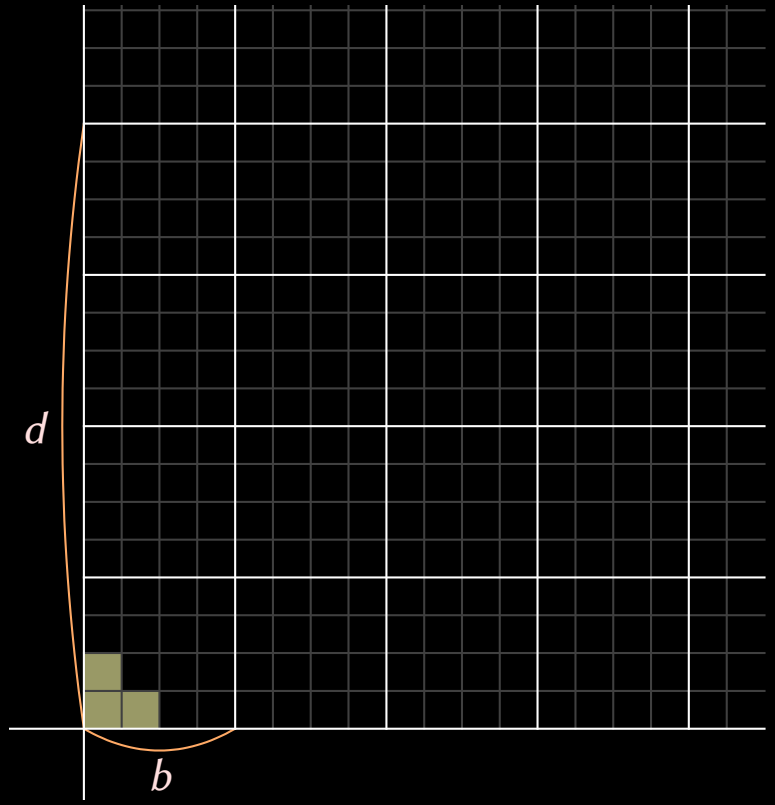
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

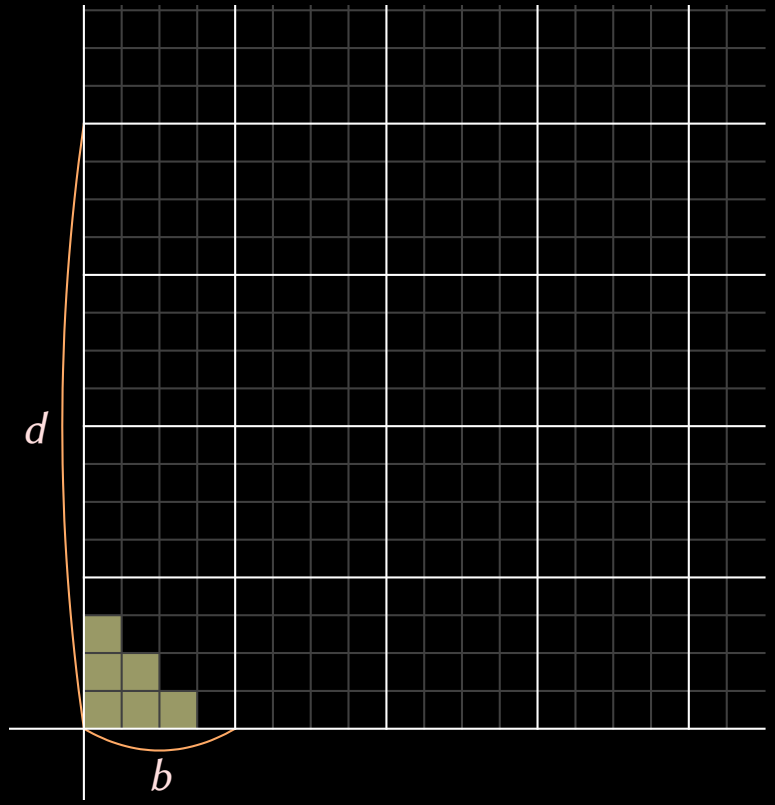
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

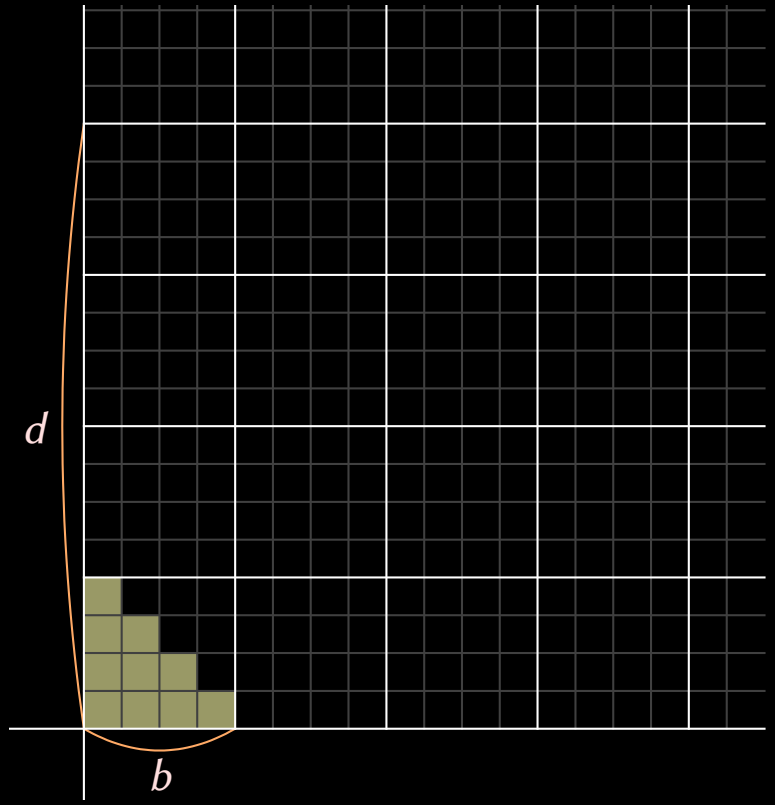
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

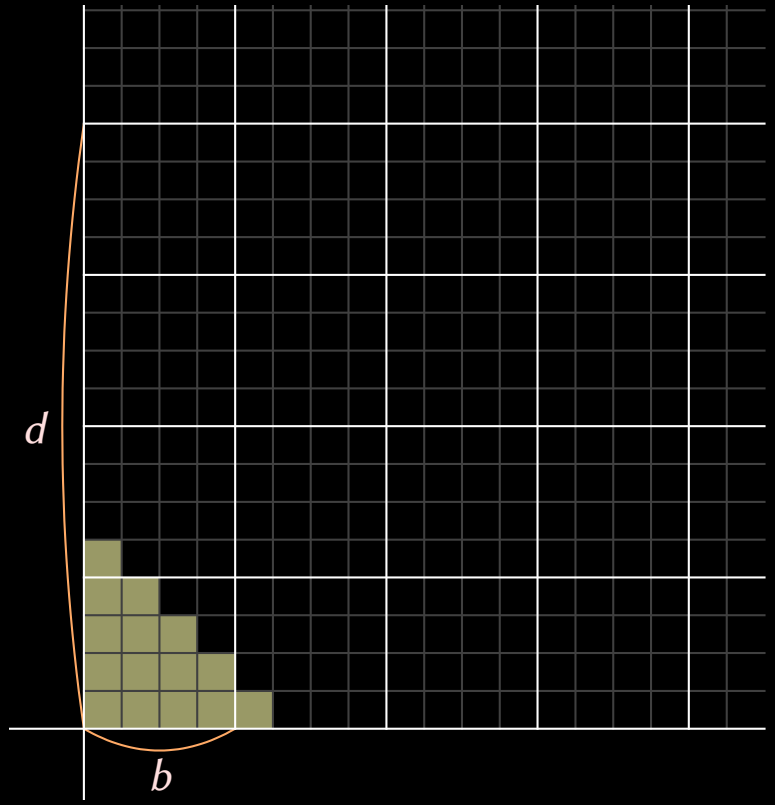
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad \mathrm{R}_{\mathbb{K}}(d)\,?$

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

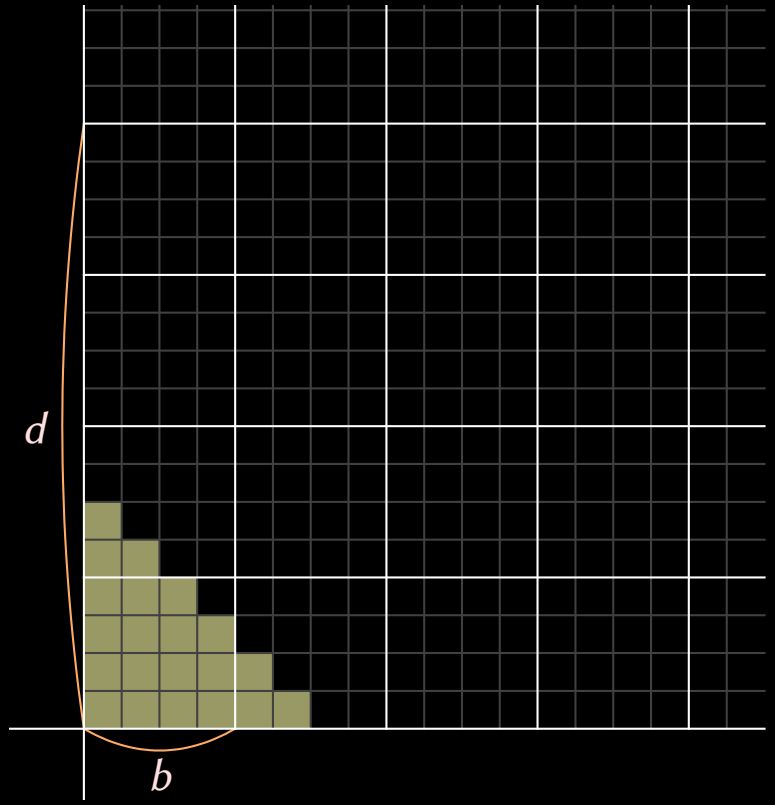
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

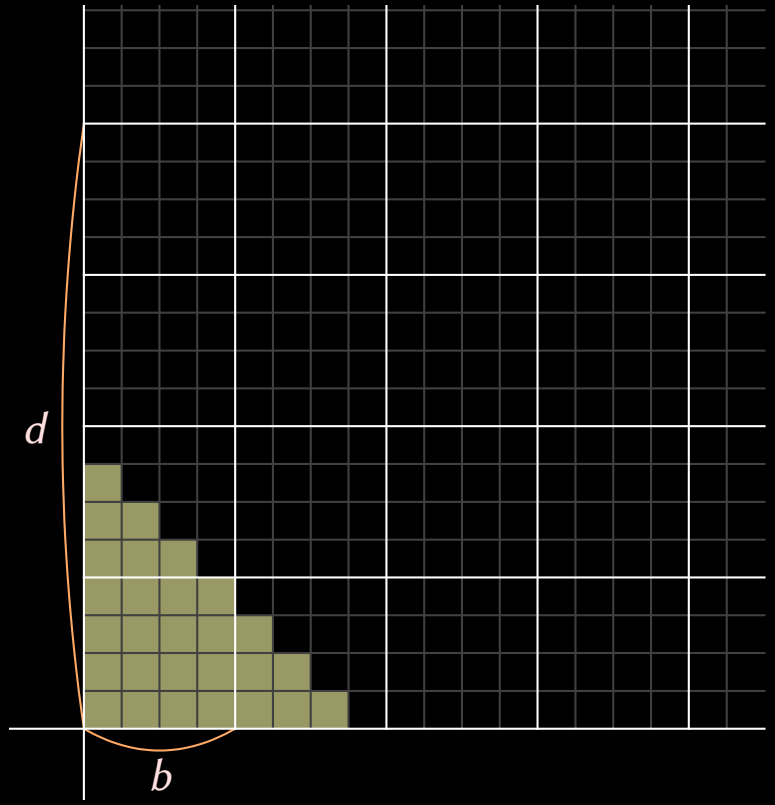
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

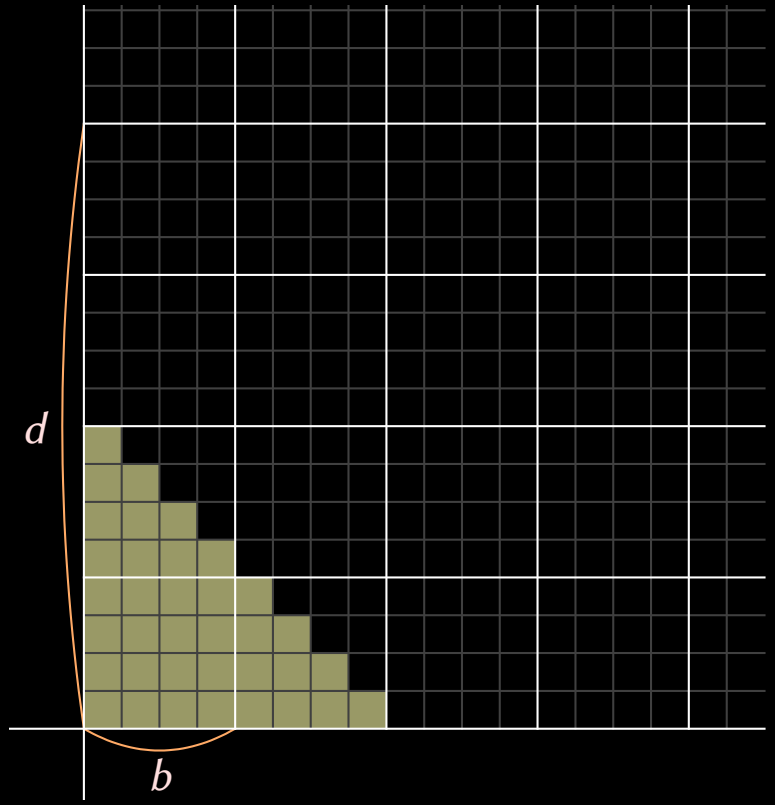
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

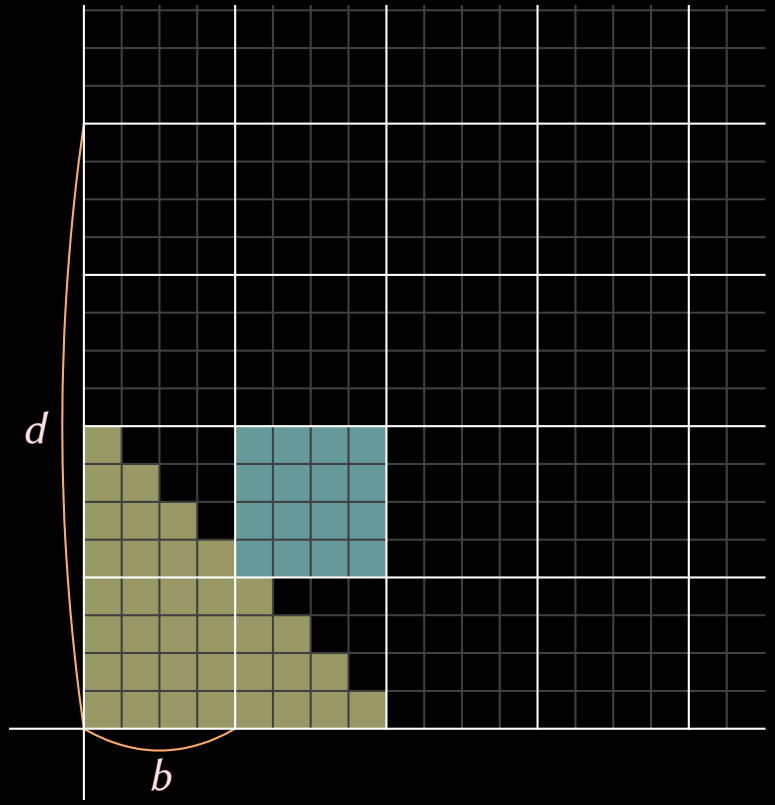
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

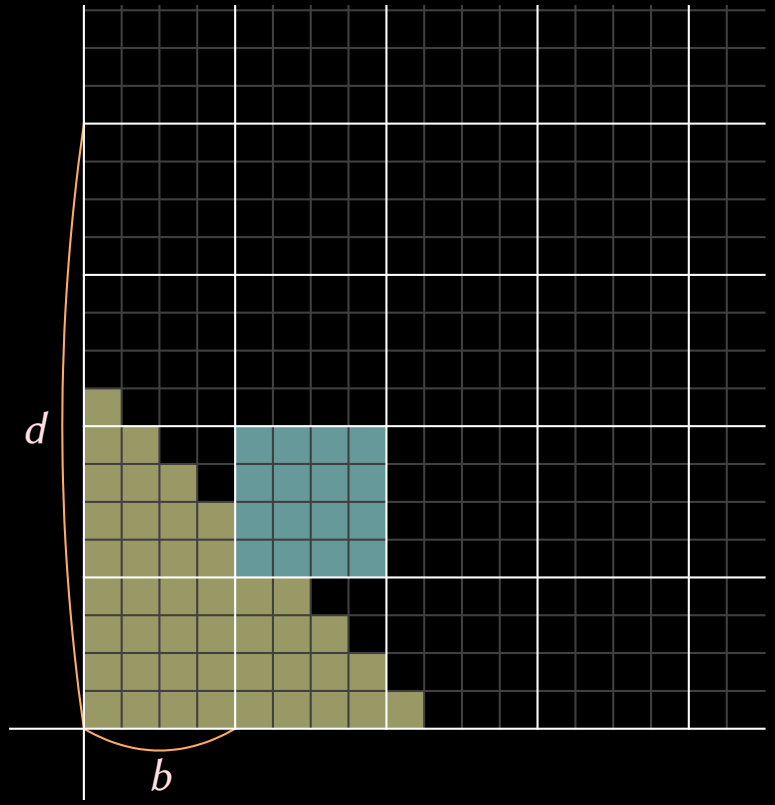
Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

$$\hat{f}_0 := \mathsf{DFT}_\omega(f_b + \cdots + f_{2b-1} z^{b-1}) \in \mathbb{K}^{2b}$$

$$\hat{g}_0 := \mathsf{DFT}_\omega(g_b + \cdots + g_{2b-1} z^{b-1}) \in \mathbb{K}^{2b}$$

$$h_{2b} + \cdots + h_{4b-1} z^{2b-1} \mathrel{+}= \mathsf{DFT}_\omega^{-1}(\hat{f}_0 \hat{g}_0)$$

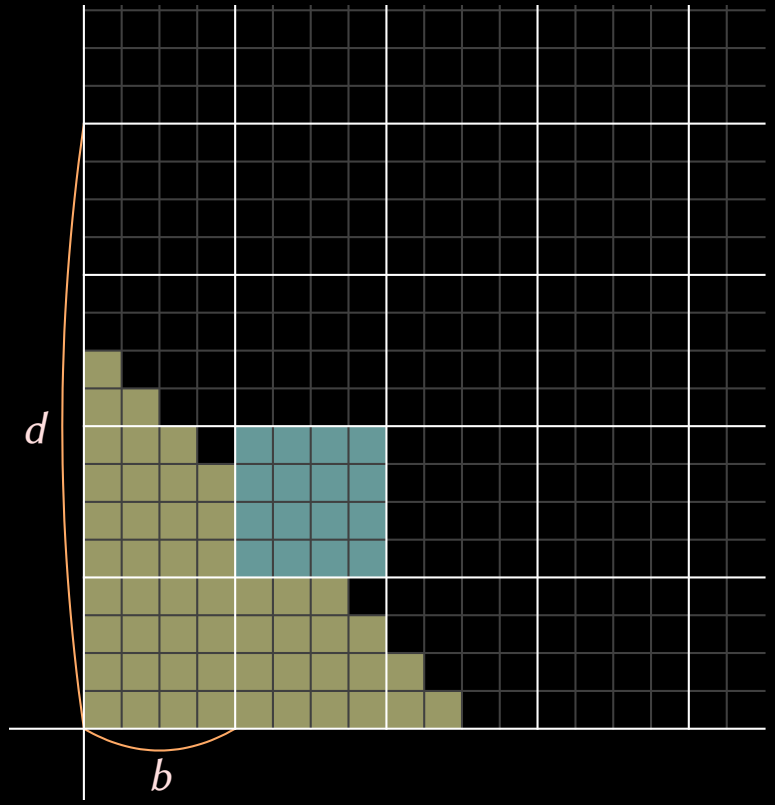
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

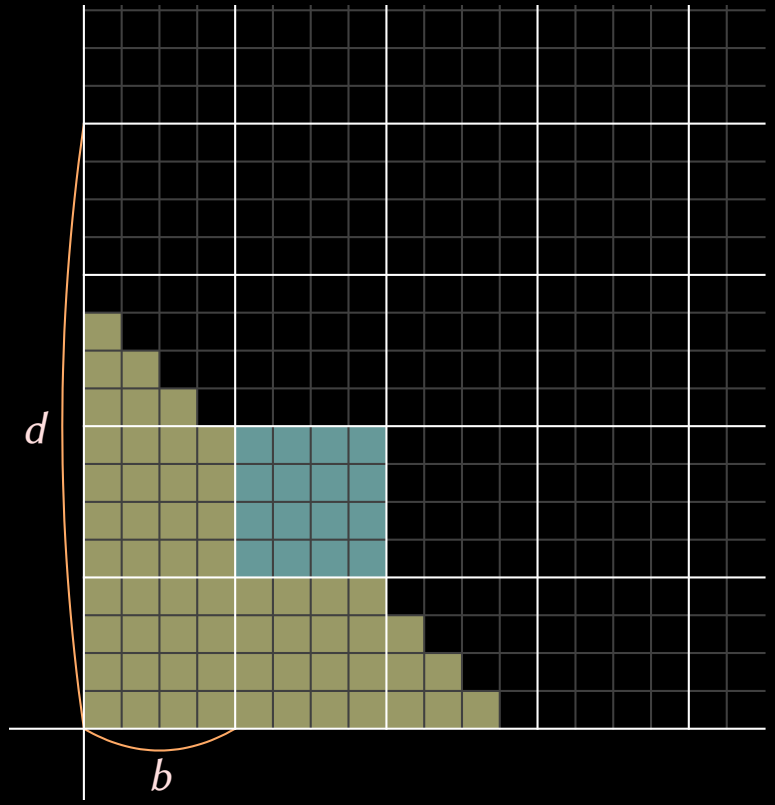
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

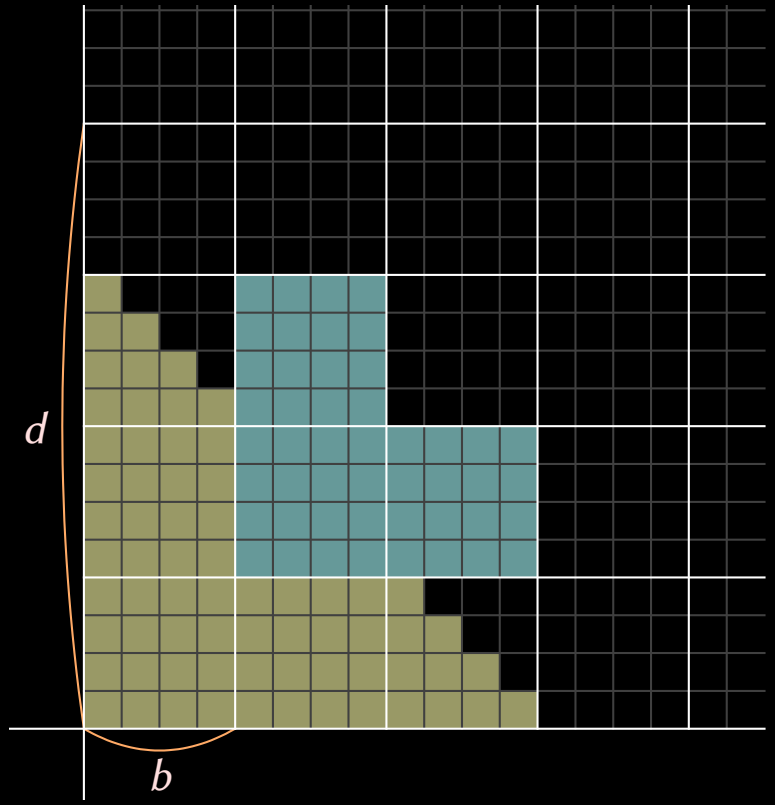
Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathsf{R}_{\mathbb{K}}(d)$?

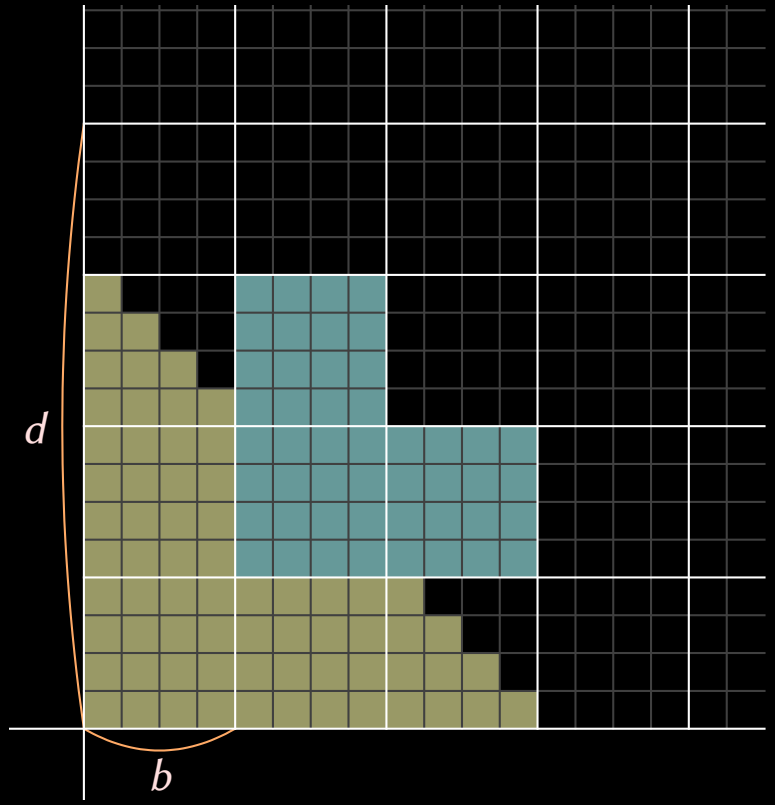
Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

$$\hat{f}_1 := \mathsf{DFT}_\omega(f_{2b} + \cdots + f_{3b-1} z^{b-1})$$

$$\hat{g}_1 := \mathsf{DFT}_\omega(g_{2b} + \cdots + g_{3b-1} z^{b-1})$$

$$h_{3b} + \cdots + h_{5b-1} z^{2b-1} \mathrel{+}= \mathsf{DFT}_\omega^{-1}(\hat{f}_0 \hat{g}_1 + \hat{f}_1 \hat{g}_0)$$

Multiplication détendue d'ordre $d = b\,l$

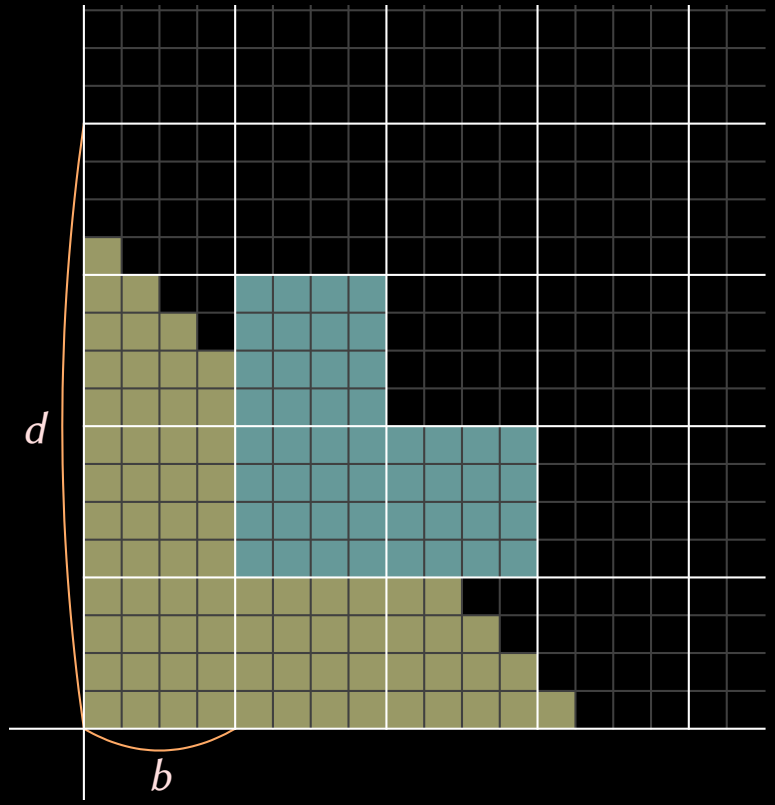


$\omega^{2b} = 1$ $\quad R_{\mathbb{K}}(d)\,?$

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

Multiplication détendue d'ordre $d = b\,l$

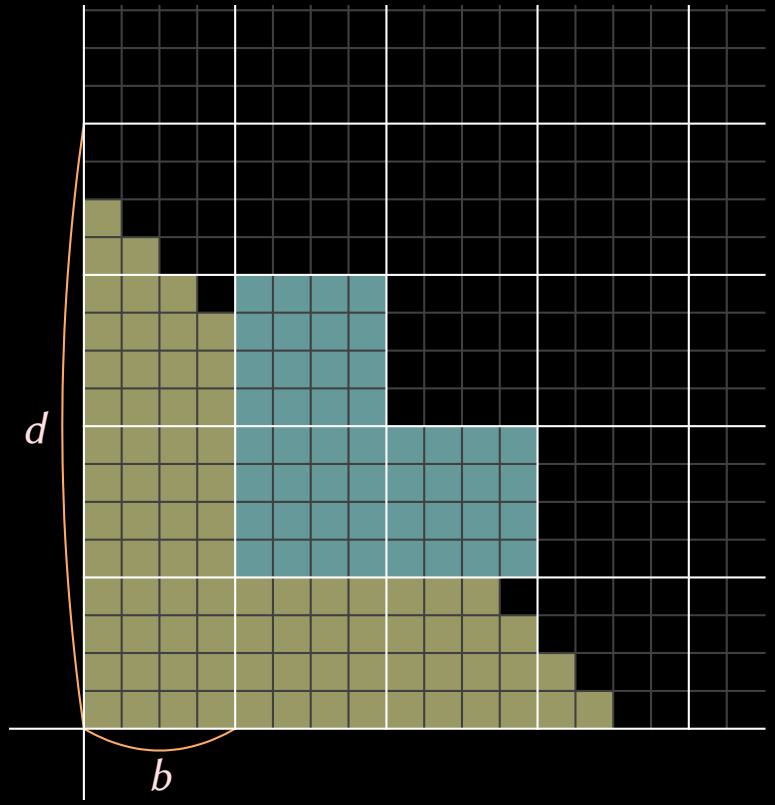


$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

Multiplication détendue d'ordre $d = b\,l$

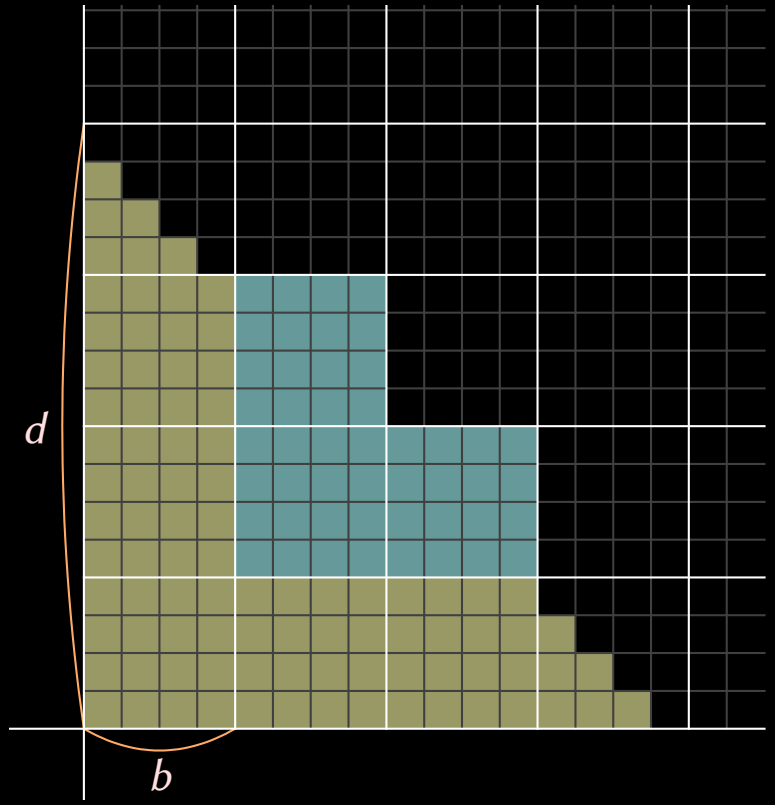


$\omega^{2b} = 1$ $\quad R_{\mathbb{K}}(d)\,?$

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

Multiplication détendue d'ordre $d = b\,l$

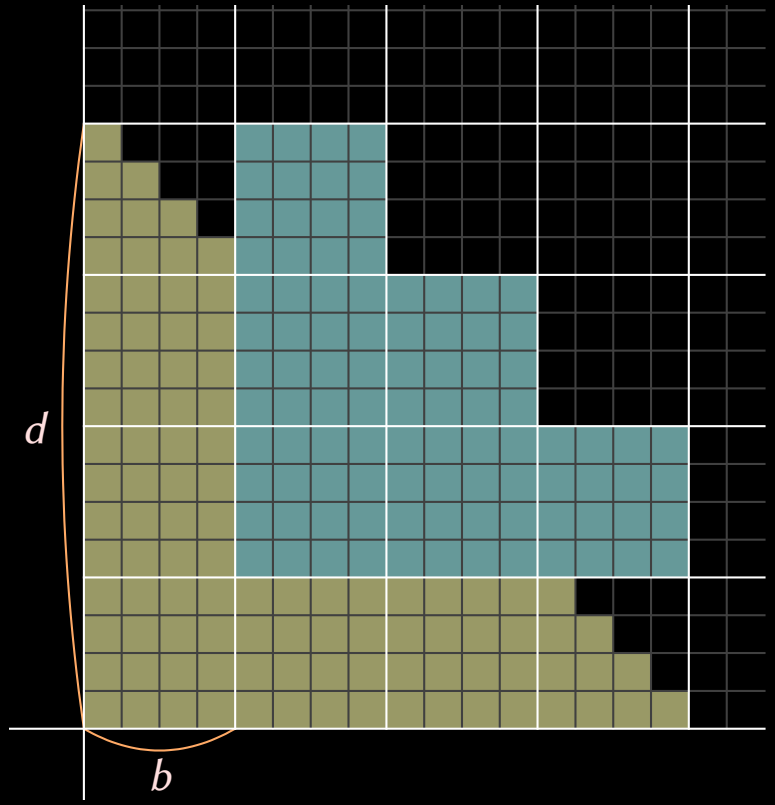


$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

Multiplication détendue d'ordre $d = b\,l$

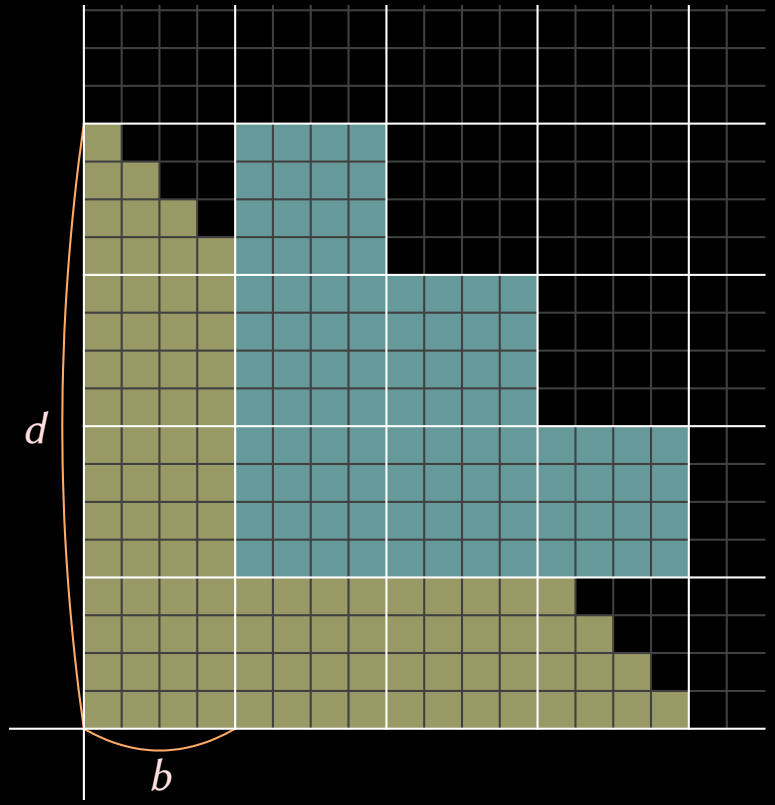


$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

Multiplication détendue d'ordre $d = b\,l$



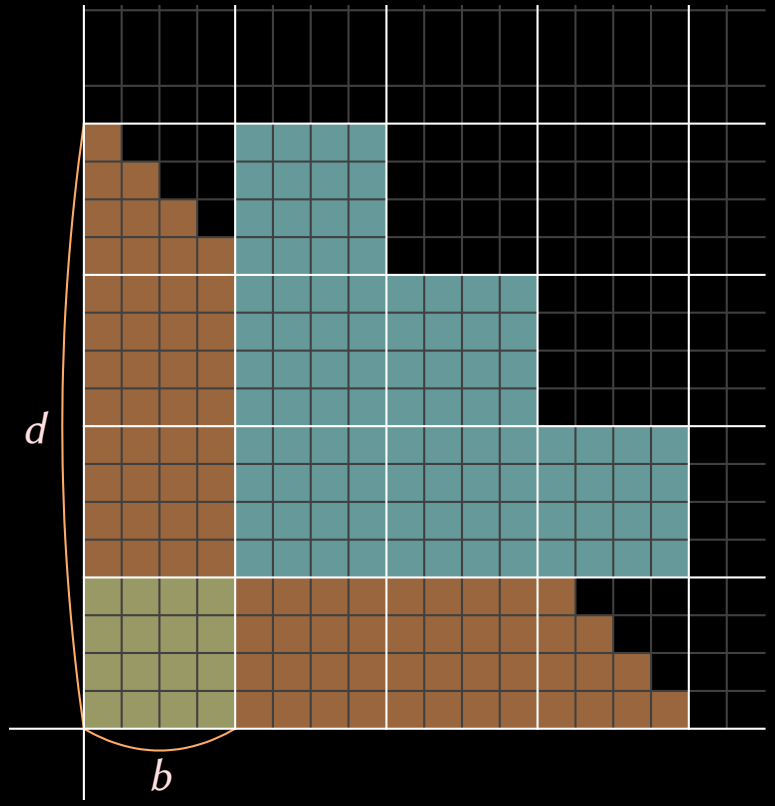
$\omega^{2b} = 1$ $\quad \mathrm{R}_{\mathbb{K}}(d)\,?$

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

$$\mathrm{R}_{\mathbb{K}}(d) \leqslant (2\,l-1)\,\mathrm{R}_{\mathbb{K}}(b) + 2\,b\,\mathrm{R}_{\mathbb{K}}(l-1) + 6\,l\,\mathrm{F}_{\mathbb{K}}(2\,b)$$

Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad$ $\mathrm{R}_{\mathbb{K}}(d)$?

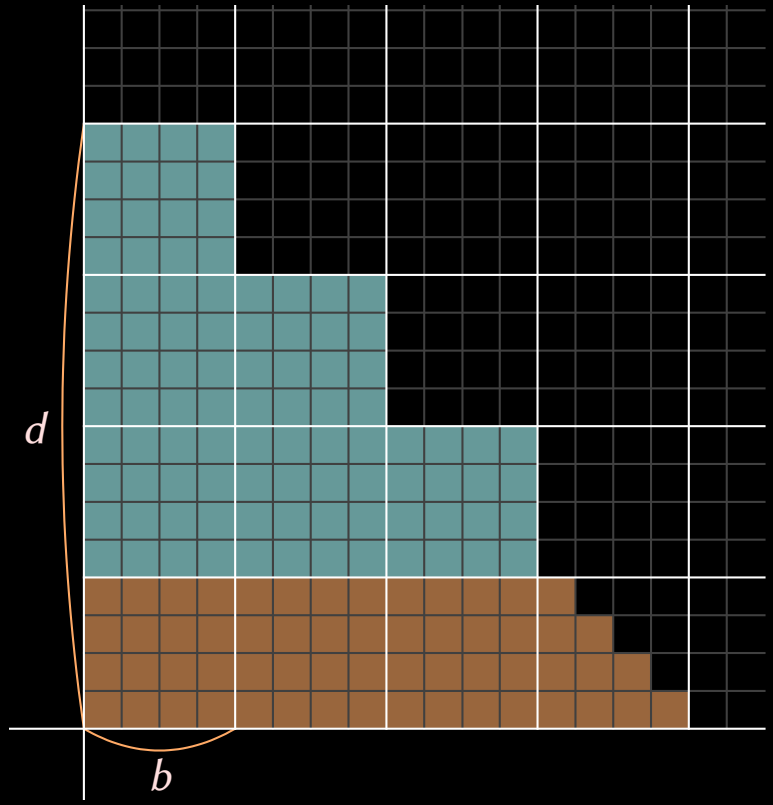
Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produits semi-détendues d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

$$\mathrm{R}_{\mathbb{K}}(d) \leqslant \mathrm{R}_{\mathbb{K}}(b) + 2\,l\,\mathrm{R}^{*}_{\mathbb{K}}(b) + 2\,b\,\mathrm{R}_{\mathbb{K}}(l) + 6\,l\,\mathrm{F}_{\mathbb{K}}(2\,b)$$

Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad \mathsf{R}_{\mathbb{K}}(d)\,?$

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

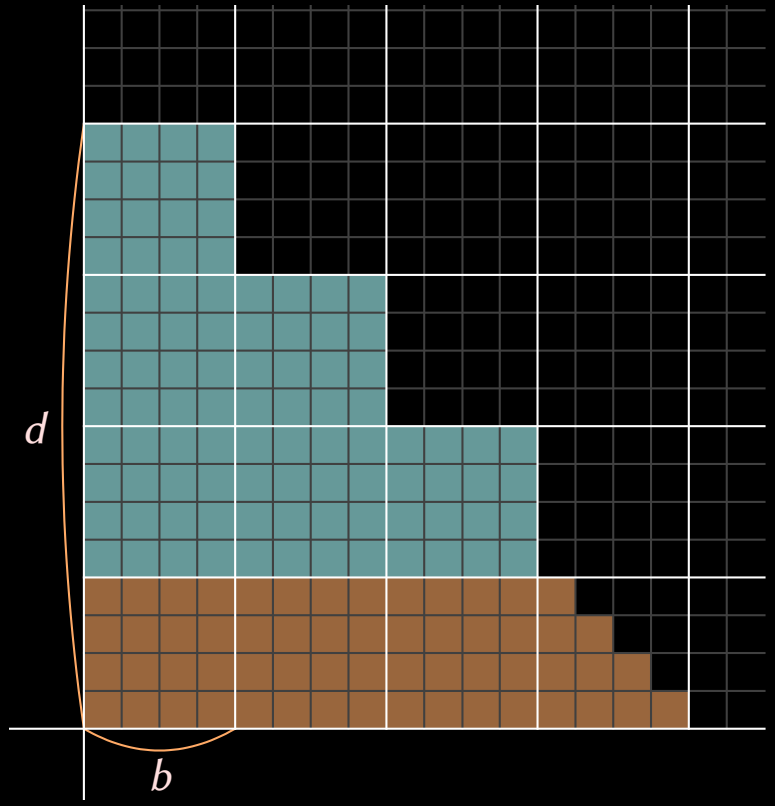
Produits semi-détendues d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

$$\mathsf{R}_{\mathbb{K}}(d) \leqslant \mathsf{R}_{\mathbb{K}}(b) + 2\,l\,\mathsf{R}^{*}_{\mathbb{K}}(b) + 2\,b\,\mathsf{R}_{\mathbb{K}}\,l + 6\,\mathsf{F}_{\mathbb{K}}(2\,b)$$

$$\mathsf{R}^{*}_{\mathbb{K}}(d) \leqslant l\,\mathsf{R}^{*}_{\mathbb{K}}(b) + 2\,b\,\mathsf{R}^{*}_{\mathbb{K}}(l) + 4\,\mathsf{F}_{\mathbb{K}}(2\,b)$$

Multiplication détendue d'ordre $d = b\,l$



$\omega^{2b} = 1$ $\quad \mathsf{R}_{\mathbb{K}}(d)\,?$ $\quad b \approx \exp \dfrac{\log d}{e^{\sqrt{2 \log 2 \log\log d}}}$

Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b

Produits semi-détendues d'ordre b

Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l - 1$

$$\mathsf{R}_{\mathbb{K}}(d) \leqslant \mathsf{R}_{\mathbb{K}}(b) + 2\,l\,\mathsf{R}^{*}_{\mathbb{K}}(b) + 2\,b\,\mathsf{R}_{\mathbb{K}}\,l + 6\,\mathsf{F}_{\mathbb{K}}(2\,b)$$

$$\mathsf{R}^{*}_{\mathbb{K}}(d) \leqslant l\,\mathsf{R}^{*}_{\mathbb{K}}(b) + 2\,b\,\mathsf{R}^{*}_{\mathbb{K}}(l) + 4\,\mathsf{F}_{\mathbb{K}}(2\,b)$$

$$\mathsf{R}_{\mathbb{K}}(d) = O(\mathsf{R}^{*}_{\mathbb{K}}(d)) = \mathsf{M}_{\mathbb{K}}(d)\,e^{O\left(\sqrt{\log\log d}\right)}$$

Calcul de l'exponentielle $g = \mathrm{e}^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$g' = f' g$$

Calcul de l'exponentielle $g = \mathrm{e}^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$\begin{aligned} g' &= f' g \\ g &= 1 + \int f' g \end{aligned}$$

Calcul de l'exponentielle $g = \mathrm{e}^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$\begin{aligned} g' &= f' g \\ g &= 1 + \int f' g \\ g_k &= \left(\int f' g \right)_k \qquad (k > 0) \end{aligned}$$

Calcul de l'exponentielle $g = e^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$\begin{aligned} g' &= f' g \\ g &= 1 + \int f' g \\ g_k &= \left(\int f' g \right)_k \\ &= \frac{1}{k} (f' g)_{k-1} \qquad (k > 0) \end{aligned}$$

Calcul de l'exponentielle $g = e^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$\begin{aligned} g' &= f' g \\ g &= 1 + \int f' g \\ g_k &= \left(\int f' g \right)_k \\ &= \frac{1}{k} (f' g)_{k-1} \\ &= \frac{1}{k} (f_1 g_{k-1} + 2 f_2 g_{k-2} + \cdots + k f_k g_0) \qquad (k > 0) \end{aligned}$$

Calcul de l'exponentielle $g = \mathrm{e}^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$\begin{aligned} g' &= f' g \\ g &= 1 + \int f' g \\ g_k &= \left(\int f' g \right)_k \\ &= \frac{1}{k} (f' g)_{k-1} \\ &= \frac{1}{k} (f_1 g_{k-1} + 2 f_2 g_{k-2} + \cdots + k f_k g_0) \qquad (k > 0) \end{aligned}$$

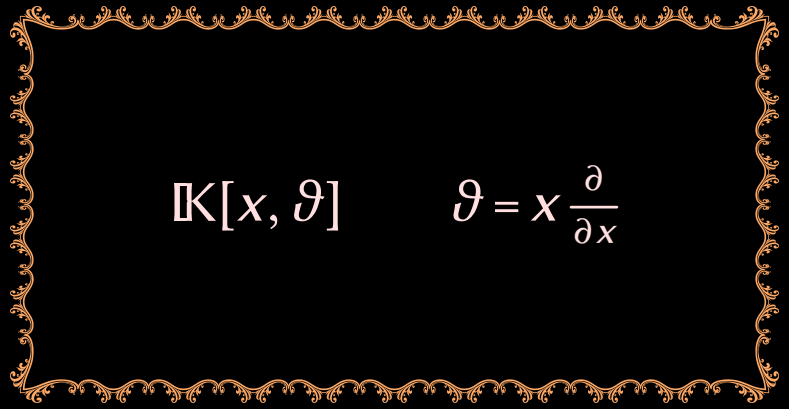
$\longrightarrow \mathsf{E}(d) \leqslant \mathsf{R}(d) + O(d)$

Calcul de l'exponentielle $g = \mathrm{e}^f, \quad f = f_1 z + f_2 z^2 + \cdots$

$$\begin{aligned} g' &= f' g \\ g &= 1 + \int f' g \\ g_k &= \left(\int f' g\right)_k \\ &= \frac{1}{k}(f' g)_{k-1} \\ &= \frac{1}{k}(f_1 g_{k-1} + 2 f_2 g_{k-2} + \cdots + k f_k g_0) \qquad (k > 0) \end{aligned}$$

$\longrightarrow \mathrm{E}(d) \leqslant \mathrm{R}(d) + O(d)$

$\longrightarrow$ Résolution d'une équation « récursive » : presque aussi vite que son évaluation


$\mathbb{K}[x, \vartheta]$
$\vartheta = x \frac{\partial}{\partial x}$

Opérateurs différentiels

$$\begin{aligned} \vartheta x &= x\vartheta + x \\ \vartheta(x^k) &= kx^k \end{aligned}$$

Opérateurs différentiels

$$\begin{aligned} \vartheta x &= x\vartheta + x \\ \vartheta(x^k) &= k x^k \end{aligned}$$

$$L = \sum_{i=0}^{d} \sum_{j=0}^{r} L_{i,j} x^i \vartheta^j$$

Opérateurs différentiels

$$\begin{aligned} \vartheta x &= x\vartheta + x \\ \vartheta(x^k) &= k x^k \end{aligned}$$

$$L = \sum_{i=0}^{d} \sum_{j=0}^{r} L_{i,j} x^i \vartheta^j$$

Multiplication par évaluation-interpolation ?

Opérateurs différentiels

$$\begin{aligned} \vartheta x &= x\vartheta + x \\ \vartheta(x^k) &= k x^k \end{aligned}$$

$$L = \sum_{i=0}^{d} \sum_{j=0}^{r} L_{i,j} x^i \vartheta^j$$

Multiplication par évaluation-interpolation ?

$$\begin{aligned} \mathbb{K}[x]_n &:= \{P \in \mathbb{K}[x] : \deg P \leqslant n\} \\ L : \mathbb{K}[x]_n &\longrightarrow \mathbb{K}[x]_{n+d} \end{aligned}$$

$$\begin{aligned} \vartheta x &= x\vartheta + x \\ \vartheta(x^k) &= k x^k \end{aligned}$$

$$L = \sum_{i=0}^{d} \sum_{j=0}^{r} L_{i,j} x^i \vartheta^j$$

Multiplication par évaluation-interpolation ?

$$\begin{aligned} \mathbb{K}[x]_n &:= \{P \in \mathbb{K}[x] : \deg P \leqslant n\} \\ L : \mathbb{K}[x]_n &\longrightarrow \mathbb{K}[x]_{n+d} \end{aligned}$$

$$L \longleftrightarrow \mathrm{Mat}_n^d(L) ? \qquad n ?$$

Opérateurs différentiels

$$L = 1$$

$$\mathrm{Mat}_n^d(L) = \overbrace{\begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ \vdots & 0 & \ddots & & \\ 0 & \vdots & \ddots & 1 & \\ 0 & 0 & & 0 & 1 \\ & 0 & \ddots & \vdots & 0 \\ & & \ddots & 0 & \vdots \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix}}^{n} \Bigg\} d$$

Opérateurs différentiels

$$L = x$$

$$\mathrm{Mat}_n^d(L) = \overbrace{\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ \vdots & 1 & \ddots & & \\ 0 & \vdots & \ddots & 0 & \\ 0 & 0 & & 1 & 0 \\ & 0 & \ddots & \vdots & 1 \\ & & \ddots & 0 & \vdots \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix}}^{n} \Big\} d$$

Opérateurs différentiels

$$L = x^k$$

$$\mathrm{Mat}_n^d(L) = \overbrace{\begin{pmatrix} 0 & & & & \\ \vdots & 0 & & & \\ 1 & & \ddots & & \\ \vdots & 1 & & 0 & \\ 0 & & \ddots & & 0 \\ & 0 & & 1 & \vdots \\ & & \ddots & & 1 \\ & & & 0 & \vdots \\ & & & & 0 \end{pmatrix}}^{n} \left.\begin{matrix} \\ k \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ d \end{matrix}\right\}$$

Opérateurs différentiels

$$L = x^k \vartheta$$

$$\mathrm{Mat}_n^d(L) = \begin{pmatrix} 0 & & & & \\ \vdots & 0 & & & \\ 0 & & \ddots & & \\ \vdots & 1 & & 0 & \\ 0 & & \ddots & & 0 \\ & 0 & & n-1 & \vdots \\ & & \ddots & & n \\ & & & 0 & \vdots \\ & & & & 0 \end{pmatrix}$$

n (top brace), k (left brace), d (right brace)

Opérateurs différentiels

$$L = x^k \vartheta^l$$

$$\mathrm{Mat}_n^d(L) = \overbrace{\begin{pmatrix} 0 & & & & & \\ \vdots & 0 & & & & \\ 0 & & \ddots & & & \\ \vdots & 1^l & & 0 & & \\ 0 & & \ddots & & 0 & \\ & 0 & & (n-1)^l & \vdots & \\ & & \ddots & & n^l & \\ & & & 0 & \vdots & \\ & & & & 0 & \end{pmatrix}}^{n} \Bigg\} k \Bigg\} d$$

Opérateurs différentiels

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix} \qquad \mathrm{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & \\ \vdots & \ddots & \\ M_{d,0} & & M_{0,n} \\ & \ddots & \vdots \\ & & M_{d,n} \end{pmatrix} \qquad M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

Opérateurs différentiels

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix} \qquad \mathrm{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & \\ \vdots & \ddots & \\ M_{d,0} & & M_{0,n} \\ & \ddots & \vdots \\ & & M_{d,n} \end{pmatrix} \qquad M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

$L \longrightarrow \mathrm{Mat}_n^d(L)$ en temps $O(d\,(n/r)\,\mathsf{M}(r)\log r)$ si $n \geqslant r$

Opérateurs différentiels

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix} \qquad \mathrm{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & \\ \vdots & \ddots & \\ M_{d,0} & & M_{0,n} \\ & \ddots & \vdots \\ & & M_{d,n} \end{pmatrix} \qquad M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

$L \longrightarrow \mathrm{Mat}_n^d(L)$ en temps $O(d\,(n/r)\,\mathsf{M}(r)\log r)$ si $n \geqslant r$

$\mathrm{Mat}_n^d(L) \longrightarrow L$ en temps $O(d\,\mathsf{M}(r)\log r)$ si $n \geqslant r$

Opérateurs différentiels

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix} \qquad \mathrm{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & \\ \vdots & \ddots & \\ M_{d,0} & & M_{0,n} \\ & \ddots & \vdots \\ & & M_{d,n} \end{pmatrix} \qquad M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

$L \longrightarrow \mathrm{Mat}_n^d(L)$ en temps $O(d\,(n/r)\,\mathrm{M}(r)\log r)$ si $n \geqslant r$

$\mathrm{Mat}_n^d(L) \longrightarrow L$ en temps $O(d\,\mathrm{M}(r)\log r)$ si $n \geqslant r$

$$\mathrm{Mat}_{2r}^{2d}(KL) = \mathrm{Mat}_{2r+d}^{d}(K)\,\mathrm{Mat}_{2r}^{d}(L)$$

Opérateurs différentiels

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix} \qquad \mathrm{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & \\ \vdots & \ddots & \\ M_{d,0} & & M_{0,n} \\ & \ddots & \vdots \\ & & M_{d,n} \end{pmatrix} \qquad M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

$L \longrightarrow \mathrm{Mat}_n^d(L)$ en temps $O(d\,(n/r)\,\mathrm{M}(r)\log r)$ si $n \geqslant r$

$\mathrm{Mat}_n^d(L) \longrightarrow L$ en temps $O(d\,\mathrm{M}(r)\log r)$ si $n \geqslant r$

$$\mathrm{Mat}_{2r}^{2d}(KL) = \mathrm{Mat}_{2r+d}^{d}(K)\,\mathrm{Mat}_{2r}^{d}(L)$$

$$\mathrm{SM}_{\mathbb{K},\vartheta}(d,r) = O\big(\Omega(r)\,{}^{d}\!/_{r} + d\,\mathrm{M}(r)\log r\big) \qquad \text{si } r \geqslant d$$

Opérateurs différentiels

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix} \qquad \mathrm{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & \\ \vdots & \ddots & \\ M_{d,0} & & M_{0,n} \\ & \ddots & \vdots \\ & & M_{d,n} \end{pmatrix} \qquad M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

$L \longrightarrow \mathrm{Mat}_n^d(L)$ en temps $O(d\,(n/r)\,\mathrm{M}(r)\log r)$ si $n \geqslant r$

$\mathrm{Mat}_n^d(L) \longrightarrow L$ en temps $O(d\,\mathrm{M}(r)\log r)$ si $n \geqslant r$

$$\mathrm{Mat}_{2r}^{2d}(KL) = \mathrm{Mat}_{2r+d}^{d}(K)\,\mathrm{Mat}_{2r}^{d}(L)$$

$$\mathrm{SM}_{\mathbb{K},\vartheta}(d,r) = O\big(\Omega(r)\,{}^{d}\!/_{r} + d\,\mathrm{M}(r)\log r\big) \qquad \text{si } r \geqslant d$$

$$\Omega_{\mathbb{K}}(r) = O(\mathrm{SM}_{\mathbb{K},\vartheta}(r,r) + r\,\mathrm{M}(r)\log r) \qquad \text{si } d = r$$

Applications

Opération	**Complexité**	**Notes**
Produit	$\mathrm{SM}_{\mathbb{K},\vartheta}(d,r)$	détendu
Division exacte	$O(\mathrm{SM}_{\mathbb{K},\vartheta}(d,r)\log d)$	$d \geqslant r$
Pseudo-division	$O(\mathrm{SM}_{\mathbb{K},\vartheta}(d',r)\log d')$	résultats simplifiés de degré $\leqslant d'$
Pseudo-pgcd à droite	$O(\mathrm{SM}_{\mathbb{K},\vartheta}(d',r)\log d')$	pgcd de degré $\leqslant d'$ et $d \leqslant d'$, Las Vegas
Pseudo-ppcm à gauche	$O(\mathrm{SM}_{\mathbb{K},\vartheta}(d',r)\log d')$	ppcm de degré $\leqslant d'$ et $d \leqslant d'$, Las Vegas
Système fondamental	$O(\mathrm{SM}_{\mathbb{K},\vartheta}(d,r)\log d)$	à l'ordre $O(x^d)$
Annulateur	$O(\mathrm{SM}_{\mathbb{K},\vartheta}(d,r)\log r)$	à l'ordre $O(x^d)$

$$\mathbb{L} = \mathbb{K}[\alpha_1, \ldots, \alpha_t] / (\mu_1(\alpha_1), \ldots, \mu_t(\alpha_1, \ldots, \alpha_t))$$

Tours d'extensions algébriques

$$\mathbb{K}\left[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}, \sqrt[8]{43}, \sqrt{11+\sqrt{3}}\right]$$

$$\mathbb{K}\left[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}, \sqrt{43}, \sqrt{11+\sqrt{3}}\right]$$

$$\mathbb{K}[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}, \sqrt{43}]$$

$$\mathbb{K}[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}]$$

$$\mathbb{K}[\sqrt{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}]$$

$$\mathbb{K}[\sqrt{2}, \sqrt[3]{5}, \sqrt{7}]$$

$$\mathbb{K}[\sqrt{2}, \sqrt[3]{5}]$$

$$\mathbb{K}[\sqrt{2}]$$

$$\mathbb{K}$$

Tours d'extensions algébriques

$$\mathbb{K}_t := \mathbb{K}_{t-1}[\alpha_t]$$

$$\mathbb{K}_{t-1} := \mathbb{K}_{t-2}[\alpha_{t-1}]$$

$$\mathbb{K}_{t-2} := \mathbb{K}_{t-3}[\alpha_{t-2}]$$

$$\vdots$$

$$\mathbb{K}_3 := \mathbb{K}_2[\alpha_3]$$

$$\mathbb{K}_2 := \mathbb{K}_1[\alpha_2]$$

$$\mathbb{K}_1 := \mathbb{K}_0[\alpha_1]$$

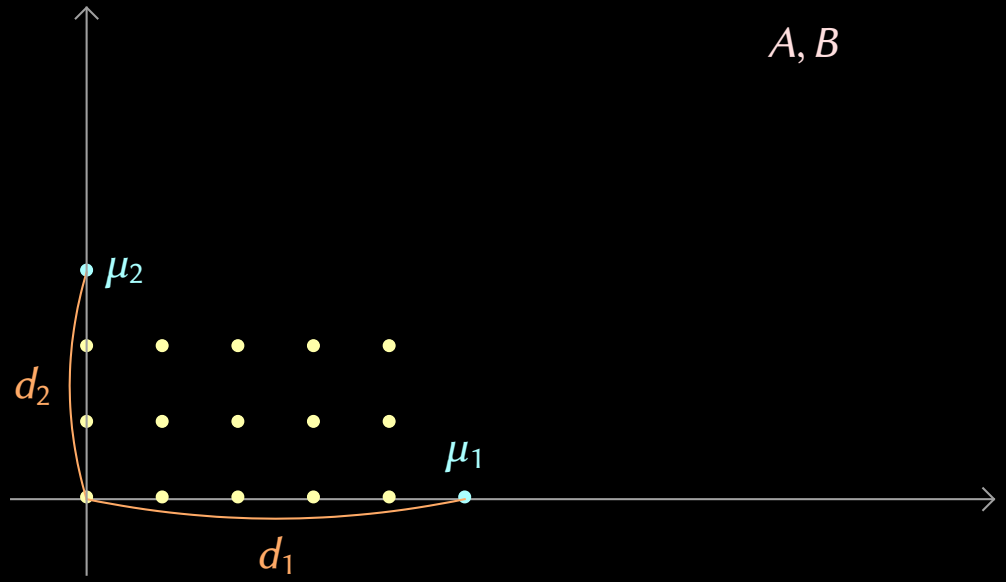
$$\mathbb{K}_0 := \mathbb{K}$$

Kronecker + réduction à la Lebreton

$$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2)), \quad d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0], \quad d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$$

Kronecker + réduction à la Lebreton

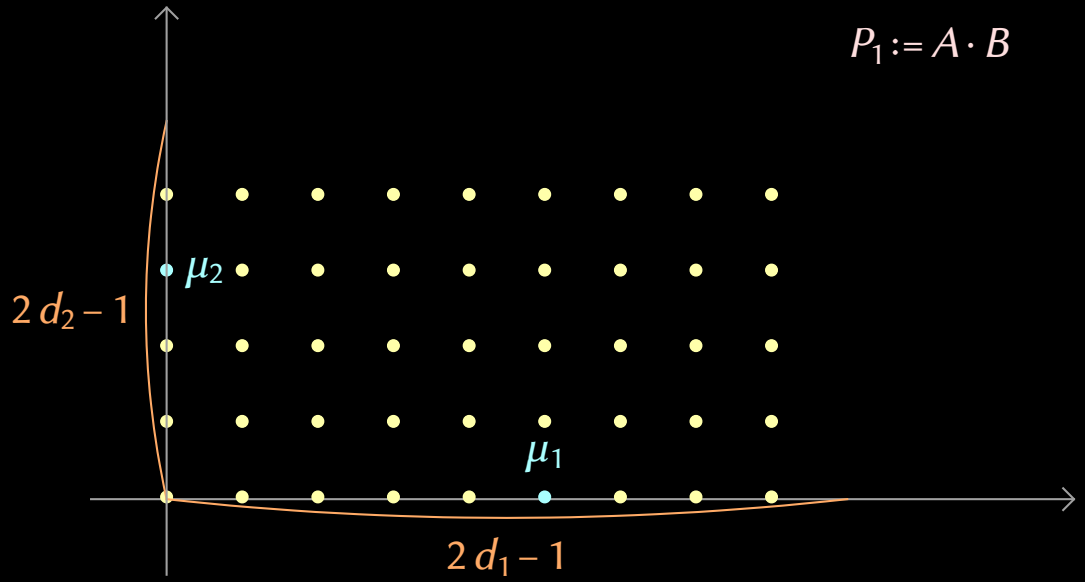
$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$



Kronecker + réduction à la Lebreton

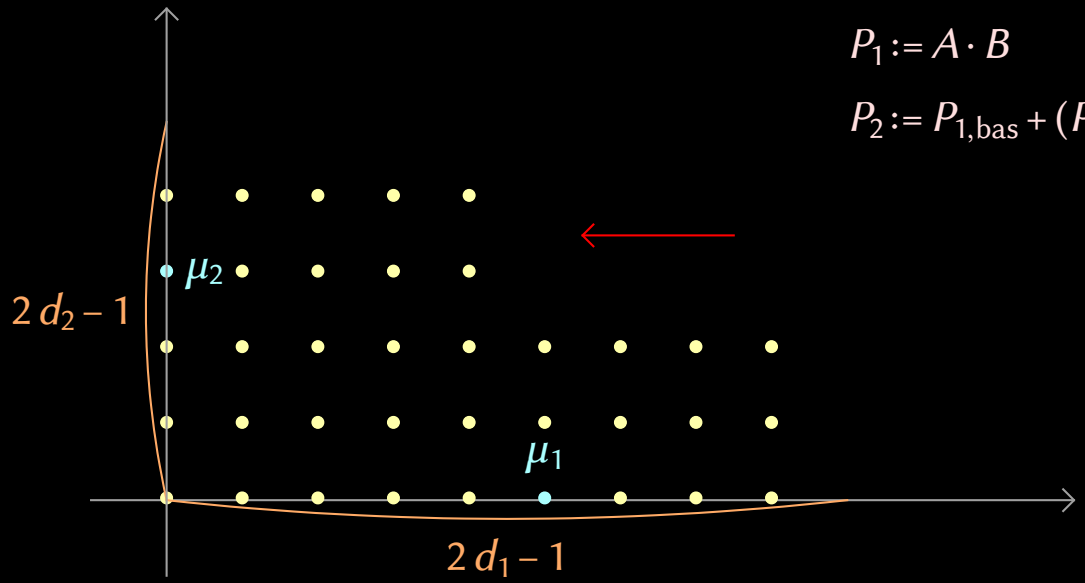
$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$

$P_1 := A \cdot B$



Kronecker + réduction à la Lebreton

$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$

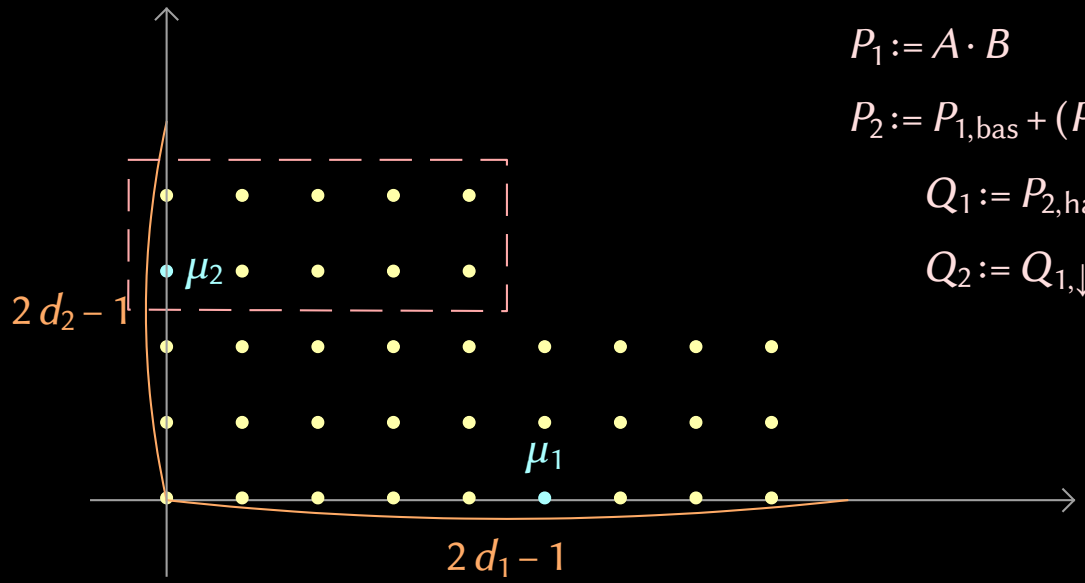


$P_1 := A \cdot B$

$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \operatorname{rem} \mu_1)$

Kronecker + réduction à la Lebreton

$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$



$P_1 := A \cdot B$

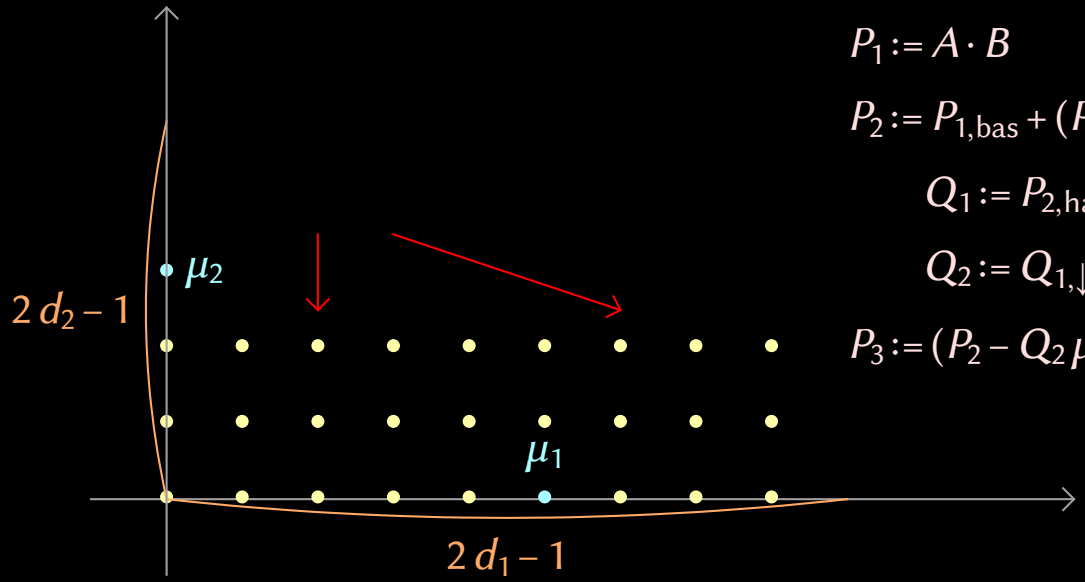
$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \operatorname{rem} \mu_1)$

$Q_1 := P_{2,\text{haut}} \cdot \text{PreInv}(\mu_2)$

$Q_2 := Q_{1,\downarrow} \operatorname{rem} \mu_1$

Kronecker + réduction à la Lebreton

$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$



$P_1 := A \cdot B$

$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \operatorname{rem} \mu_1)$

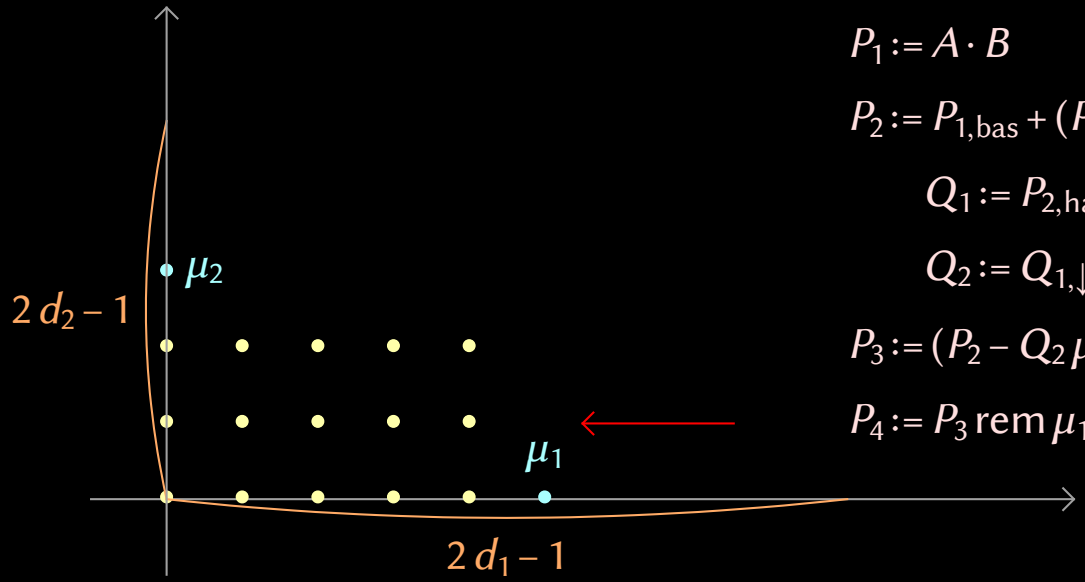
$Q_1 := P_{2,\text{haut}} \cdot \text{PreInv}(\mu_2)$

$Q_2 := Q_{1,\downarrow} \operatorname{rem} \mu_1$

$P_3 := (P_2 - Q_2\,\mu_2)_{\text{bas}}$

Kronecker + réduction à la Lebreton

$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$



$P_1 := A \cdot B$

$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \operatorname{rem} \mu_1)$

$Q_1 := P_{2,\text{haut}} \cdot \text{PreInv}(\mu_2)$

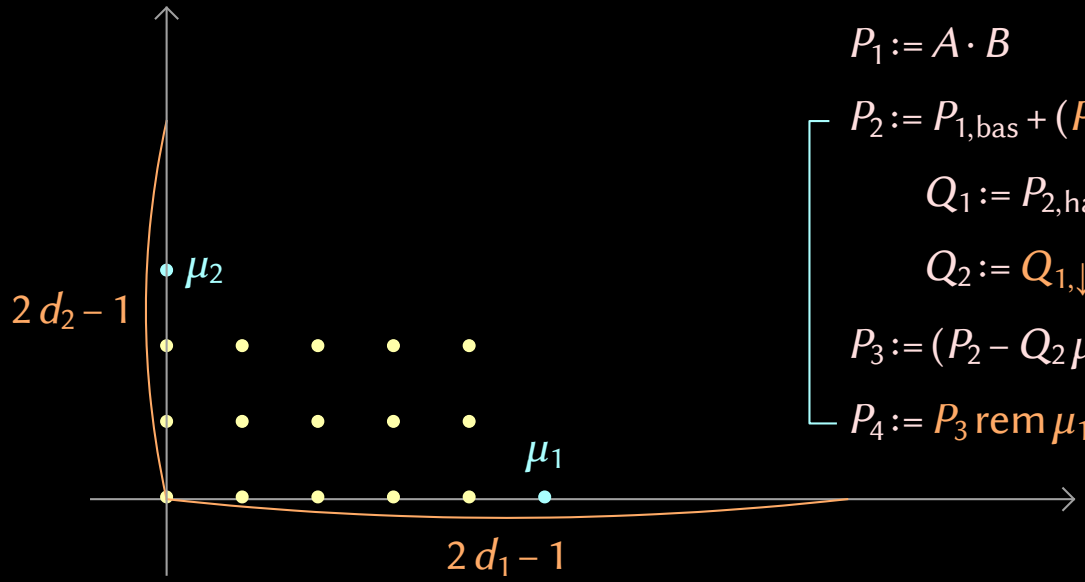
$Q_2 := Q_{1,\downarrow} \operatorname{rem} \mu_1$

$P_3 := (P_2 - Q_2\,\mu_2)_{\text{bas}}$

$P_4 := P_3 \operatorname{rem} \mu_1$

Kronecker + réduction à la Lebreton

$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $\quad d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $\quad d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$



$P_1 := A \cdot B$

$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \operatorname{rem} \mu_1)$

$Q_1 := P_{2,\text{haut}} \cdot \text{PreInv}(\mu_2)$

$Q_2 := Q_{1,\downarrow} \operatorname{rem} \mu_1$

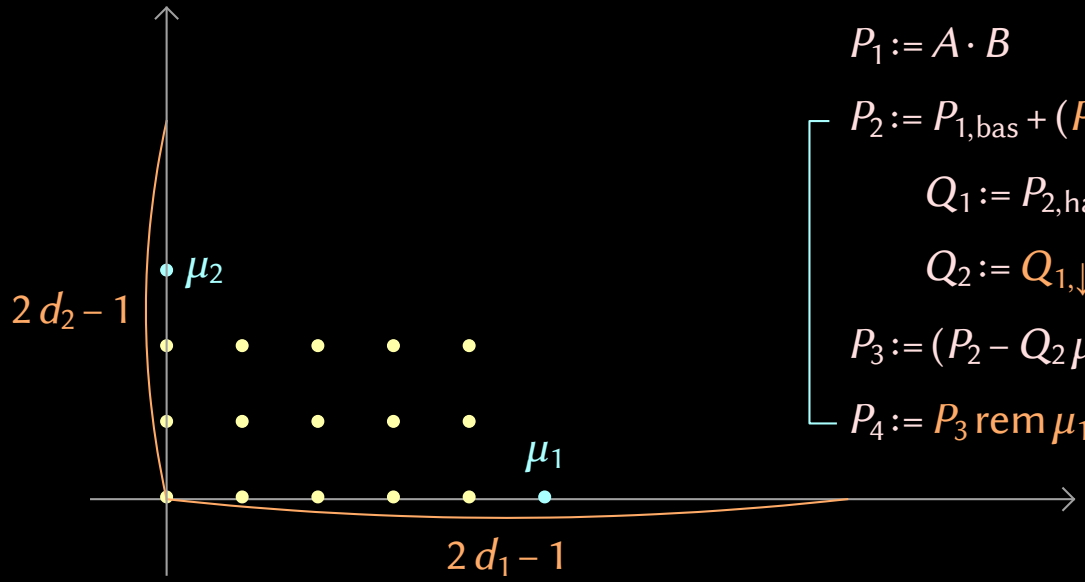
$P_3 := (P_2 - Q_2\,\mu_2)_{\text{bas}}$

$P_4 := P_3 \operatorname{rem} \mu_1$

1 réduction à l'étage t $\longrightarrow$ 3 réductions à l'étage $t-1$

Kronecker + réduction à la Lebreton

$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2))$, $\quad d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0]$, $\quad d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$



$P_1 := A \cdot B$

$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \operatorname{rem} \mu_1)$

$Q_1 := P_{2,\text{haut}} \cdot \text{PreInv}(\mu_2)$

$Q_2 := Q_{1,\downarrow} \operatorname{rem} \mu_1$

$P_3 := (P_2 - Q_2\,\mu_2)_{\text{bas}}$

$P_4 := P_3 \operatorname{rem} \mu_1$

$\mathsf{m}_{\mathbb{L}} := M_{\mathbb{L}}(1) = O(M_{\mathbb{K}}(3^t d)) \qquad d = [\mathbb{L} : \mathbb{K}]$

Cas le plus défavorable

$$d_1 = \cdots = d_t = 2 \quad \Longrightarrow \quad \mathsf{m}_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Comment faire mieux ?

Cas le plus défavorable

$$d_1 = \cdots = d_t = 2 \quad \Longrightarrow \quad \mathsf{m}_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Éléments primitif β

$$\begin{aligned} \mathbb{L} &\cong \mathbb{K}[\beta] \\ \mathsf{m}_{\mathbb{K}[\beta]} &= O(M_{\mathbb{K}}(d)) \end{aligned}$$

Comment faire mieux ?

Cas le plus défavorable

$$d_1 = \cdots = d_t = 2 \quad \Longrightarrow \quad \mathsf{m}_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2{,}585}))$$

Éléments primitif β

$$\begin{aligned} \mathbb{L} &\cong \mathbb{K}[\beta] \\ \mathsf{m}_{\mathbb{K}[\beta]} &= O(M_{\mathbb{K}}(d)) \end{aligned}$$

Problèmes

Il faut pré-calculer l'élément primitif

Comment faire mieux ?

Cas le plus défavorable

$$d_1 = \cdots = d_t = 2 \quad \Longrightarrow \quad \mathsf{m}_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Éléments primitif β

$$\begin{aligned} \mathbb{L} &\cong \mathbb{K}[\beta] \\ \mathsf{m}_{\mathbb{K}[\beta]} &= O(M_{\mathbb{K}}(d)) \end{aligned}$$

Problèmes

Il faut pré-calculer l'élément primitif

Coût des conversions $\mathbb{L} \Longleftrightarrow \mathbb{K}[\beta]$ en $O(\mathsf{m}_{\mathbb{K}}\, d^{\omega})$ où $3/2 < \omega \leqslant 2$

Tours accélérés

$$\mathbb{K}\left[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}, \sqrt[8]{43}, \sqrt{11+\sqrt{3}}\right]$$

$$\mathbb{K}\left[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}, \sqrt{43}, \sqrt{11+\sqrt{3}}\right]$$

$$\mathbb{K}[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}, \sqrt{43}]$$

$$\mathbb{K}[\sqrt[4]{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}]$$

$$\mathbb{K}[\sqrt{2}, \sqrt[3]{5}, \sqrt{7}, \sqrt{3}]$$

$$\mathbb{K}[\sqrt{2}, \sqrt[3]{5}, \sqrt{7}]$$

$$\mathbb{K}[\sqrt{2}, \sqrt[3]{5}]$$

$$\mathbb{K}[\sqrt{2}]$$

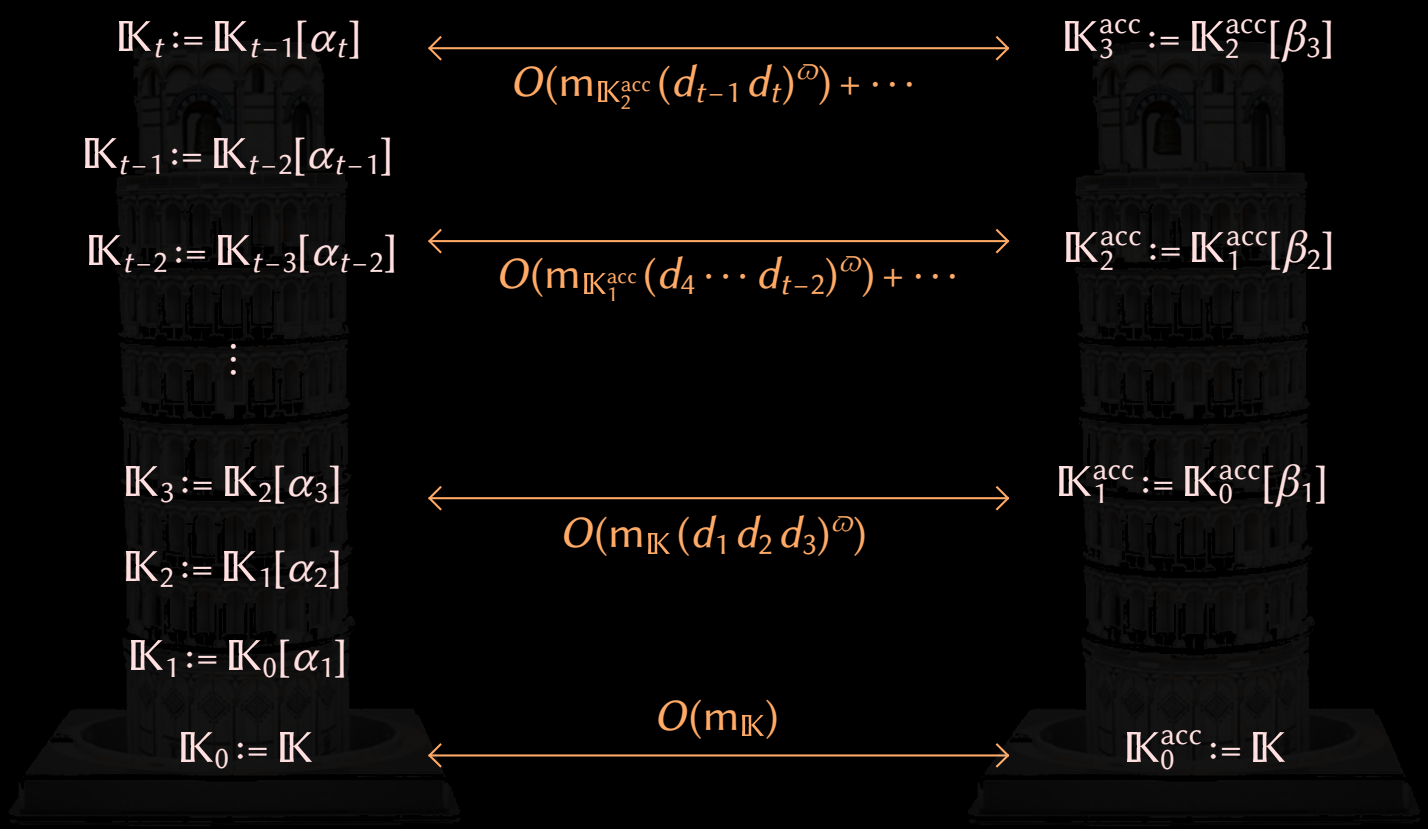
$$\mathbb{K}$$

$$\mathbb{K}\left[\sqrt[4]{2}+\sqrt[3]{5}+\sqrt{7}+\sqrt{3}, \sqrt[8]{43}+\sqrt{11+\sqrt{3}}\right]$$

$$\mathbb{K}[\sqrt[4]{2}+\sqrt[3]{5}+\sqrt{7}+\sqrt{3}]$$

$$\mathbb{K}$$

Tours accélérés



Tours accélérés

$$\mathrm{m}_{\mathbb{L}} \;=\; \mathrm{M}_{\mathbb{K}}(d)\,\mathrm{e}^{O\left(\sqrt{\log d}\right)}$$

Tours accélérés

$$\mathsf{m}_{\mathbb{L}} \;=\; \mathsf{M}_{\mathbb{K}}(d)\,\mathrm{e}^{O\left(\sqrt{\log d}\right)}$$

Généralisation

Marche pour des tours *séparables* tant que l'on ne divise pas par zéro

Tours accélérés

$$\mathsf{m}_{\mathbb{L}} = \mathsf{M}_{\mathbb{K}}(d)\, \mathrm{e}^{O\left(\sqrt{\log d}\right)}$$

Généralisation

Marche pour des tours *séparables* tant que l'on ne divise pas par zéro

Évaluation dirigée

Séparer le calcul en deux branches en cas de division par zéro

- Privilégier la branche de plus haut degré
- Traiter les branches résiduelles collectivement à la fin

(variante de l'« évaluation dynamique » de Duval et al.)

Tours accélérés

$$\mathsf{m}_{\mathbb{L}} \;=\; \mathsf{M}_{\mathbb{K}}(d)\, e^{O\left(\sqrt{\log d}\right)}$$

Généralisation

Marche pour des tours *séparables* tant que l'on ne divise pas par zéro

Évaluation dirigée

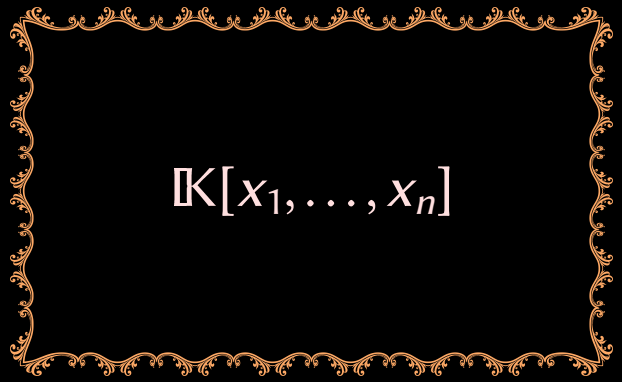
Séparer le calcul en deux branches en cas de division par zéro

- Privilégier la branche de plus haut degré
- Traiter les branches résiduelles collectivement à la fin

(variante de l'« évaluation dynamique » de Duval et al.)

Application

Multiplication dans $\mathbb{L}^{r\times r}$ en temps $O(\Omega(r)\, d)$ lorsque $d = r^{O(1)}$


$\mathbb{K}[x_1, \ldots, x_n]$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

$$f = ab$$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

$$f = ab$$

$$f(x) = c_1 x^{e_1} + \cdots + c_s x^{e_s} \qquad (x^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

$$f = ab$$

$$f(x) = c_1 x^{e_1} + \cdots + c_s x^{e_s} \qquad (x^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer $s, e_1, \ldots, e_s$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

$$f = ab$$

$$f(x) = c_1 x^{e_1} + \cdots + c_s x^{e_s} \qquad (x^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer $s, e_1, \ldots, e_s$

Étape 2 : déterminer $c_1, \ldots, c_s$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

$$f = ab$$

$$f(x) = c_1 x^{e_1} + \cdots + c_s x^{e_s} \qquad (x^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer $s, e_1, \ldots, e_s$

Étape 2 : déterminer $c_1, \ldots, c_s$

- Étape 1 souvent facile : a et b sont denses jusqu'à un certain degré total
- Ou peu cher : $\mathbb{K} = \mathbb{Q}$, $c_1, \ldots, c_s$ « gros », et $e_1, \ldots, e_s$ déterminés pour $f \bmod p$

Multiplication creuse

$$a, b \in \mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$

$$f = ab$$

$$f(x) = c_1 x^{e_1} + \cdots + c_s x^{e_s} \qquad (x^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer $s, e_1, \ldots, e_s$

Étape 2 : déterminer $c_1, \ldots, c_s$

- Étape 1 souvent facile : a et b sont denses jusqu'à un certain degré total
- Ou peu cher : $\mathbb{K} = \mathbb{Q}$, $c_1, \ldots, c_s$ « gros », et $e_1, \ldots, e_s$ déterminés pour $f \bmod p$

$\longrightarrow$ nous allons nous focaliser sur l'Étape 2

Idée : considérer l'évaluation de f sur une suite géométrique $1, \alpha, \alpha^2, \alpha^3, \ldots \in \mathbb{K}^n$

$$\begin{pmatrix} f(1) \\ f(\alpha) \\ f(\alpha^2) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{e_1} & \alpha^{e_2} & \cdots & \alpha^{e_s} \\ (\alpha^{e_1})^2 & (\alpha^{e_2})^2 & \cdots & (\alpha^{e_s})^2 \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_s \end{pmatrix}$$

Méthode de Prony

Idée : considérer l'évaluation de f sur une suite géométrique $1, \alpha, \alpha^2, \alpha^3, \ldots \in \mathbb{K}^n$

$$\begin{pmatrix} f(1) \\ f(\alpha) \\ f(\alpha^2) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{e_1} & \alpha^{e_2} & \cdots & \alpha^{e_s} \\ (\alpha^{e_1})^2 & (\alpha^{e_2})^2 & \cdots & (\alpha^{e_s})^2 \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_s \end{pmatrix}$$

Évaluation : a et $b \longrightarrow a(1), a(\alpha), \ldots, a(\alpha^{s-1})$ et $b(1), b(\alpha), \ldots, b(\alpha^{s-1})$

Multiplication par Vandermonde = transposé de l'évaluation multi-points

Méthode de Prony

Idée : considérer l'évaluation de f sur une suite géométrique $1, \alpha, \alpha^2, \alpha^3, \ldots \in \mathbb{K}^n$

$$\begin{pmatrix} f(1) \\ f(\alpha) \\ f(\alpha^2) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{e_1} & \alpha^{e_2} & \cdots & \alpha^{e_s} \\ (\alpha^{e_1})^2 & (\alpha^{e_2})^2 & \cdots & (\alpha^{e_s})^2 \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_s \end{pmatrix}$$

Évaluation : a et $b \longrightarrow a(1), a(\alpha), \ldots, a(\alpha^{s-1})$ et $b(1), b(\alpha), \ldots, b(\alpha^{s-1})$

Multiplication par Vandermonde = transposé de l'évaluation multi-points

Interpolation : $f(1), f(\alpha), \ldots, f(\alpha^{s-1}) \longrightarrow f$

Multiplication par inverse Vandermonde = transposé de l'interpolation polynomiale

Méthode de Prony

Idée : considérer l'évaluation de f sur une suite géométrique $1, \alpha, \alpha^2, \alpha^3, \ldots \in \mathbb{K}^n$

$$\begin{pmatrix} f(1) \\ f(\alpha) \\ f(\alpha^2) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{e_1} & \alpha^{e_2} & \cdots & \alpha^{e_s} \\ (\alpha^{e_1})^2 & (\alpha^{e_2})^2 & \cdots & (\alpha^{e_s})^2 \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_s \end{pmatrix}$$

Évaluation : a et $b \longrightarrow a(1), a(\alpha), \ldots, a(\alpha^{s-1})$ et $b(1), b(\alpha), \ldots, b(\alpha^{s-1})$

Multiplication par Vandermonde = transposé de l'évaluation multi-points

Interpolation : $f(1), f(\alpha), \ldots, f(\alpha^{s-1}) \longrightarrow f$

Multiplication par inverse Vandermonde = transposé de l'interpolation polynomiale

(suppose $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_s}$ deux à deux distincts)

Méthode de Prony

Idée : considérer l'évaluation de f sur une suite géométrique $1, \alpha, \alpha^2, \alpha^3, \ldots \in \mathbb{K}^n$

$$\begin{pmatrix} f(1) \\ f(\alpha) \\ f(\alpha^2) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{e_1} & \alpha^{e_2} & \cdots & \alpha^{e_s} \\ (\alpha^{e_1})^2 & (\alpha^{e_2})^2 & \cdots & (\alpha^{e_s})^2 \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_s \end{pmatrix}$$

Évaluation : a et $b \longrightarrow a(1), a(\alpha), \ldots, a(\alpha^{s-1})$ et $b(1), b(\alpha), \ldots, b(\alpha^{s-1})$

Multiplication par Vandermonde = transposé de l'évaluation multi-points

Interpolation : $f(1), f(\alpha), \ldots, f(\alpha^{s-1}) \longrightarrow f$

Multiplication par inverse Vandermonde = transposé de l'interpolation polynomiale

(suppose $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_s}$ deux à deux distincts)

$$M_{\mathbb{K}}^{\text{sparse}}(s) = O(M_{\mathbb{K}}(s) \log s)$$

Exploitation de la FFT

Espoir : évaluation-interpolation plus rapide pour α racine de l'unité

Exploitation de la FFT

Espoir : évaluation-interpolation plus rapide pour α racine de l'unité

Problème : « collisions » dans $\{\alpha^{e_1}, \ldots, \alpha^{e_n}\}$

Exploitation de la FFT

Espoir : évaluation-interpolation plus rapide pour α racine de l'unité

Problème : « collisions » dans $\{\alpha^{e_1}, \ldots, \alpha^{e_n}\}$

Cadre plus précis : pour $r \asymp s$,

- Évaluation de a et de b en $t^\lambda := (t^{\lambda_1}, \ldots, t^{\lambda_n})$ dans $\mathbb{K}[t]/(t^r - 1) \longrightarrow \hat{a}$ et $\hat{b}$
- $\hat{f} := \hat{a}\,\hat{b}$ par multiplication FFT
- Interpoler f

Note : $(t^\lambda)^{e_i} = (t^\lambda)^{e_j} \iff t^{\lambda \cdot e_1} = t^{\lambda \cdot e_j} \iff (\lambda \cdot e_i = \lambda \cdot e_j \text{ modulo } r)$

Exploitation de la FFT

Espoir : évaluation-interpolation plus rapide pour α racine de l'unité

Problème : « collisions » dans $\{\alpha^{e_1}, \ldots, \alpha^{e_n}\}$

Cadre plus précis : pour $r \asymp s$,

- Évaluation de a et de b en $t^\lambda := (t^{\lambda_1}, \ldots, t^{\lambda_n})$ dans $\mathbb{K}[t]/(t^r - 1) \longrightarrow \hat{a}$ et $\hat{b}$
- $\hat{f} := \hat{a}\,\hat{b}$ par multiplication FFT
- Interpoler f

Note : $(t^\lambda)^{e_i} = (t^\lambda)^{e_j} \iff t^{\lambda \cdot e_1} = t^{\lambda \cdot e_j} \iff (\lambda \cdot e_i = \lambda \cdot e_j \text{ modulo } r)$

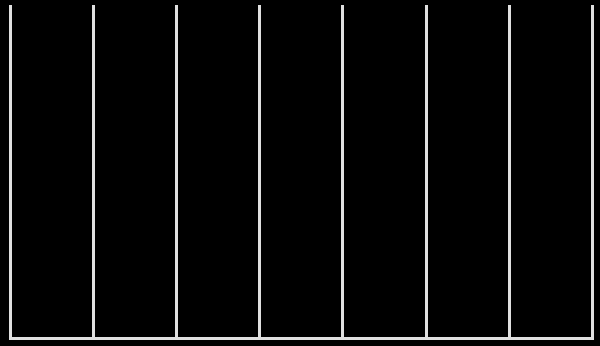
Modèle (ou hypothèse heuristique)

Pour $\lambda_1, \ldots, \lambda_n$ aléatoires :

$\lambda \cdot e_1, \ldots, \lambda \cdot e_s$ modulo $r \quad \leftrightsquigarrow \quad$ tirage aléatoire de s entiers modulo r

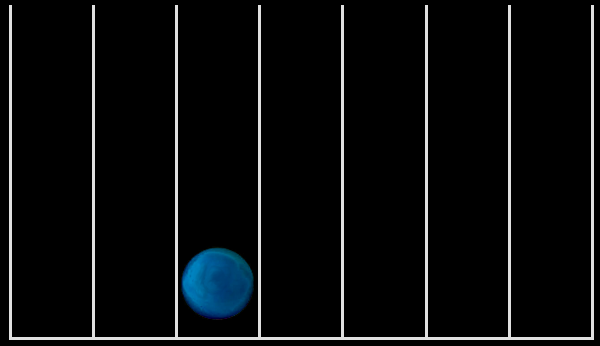
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



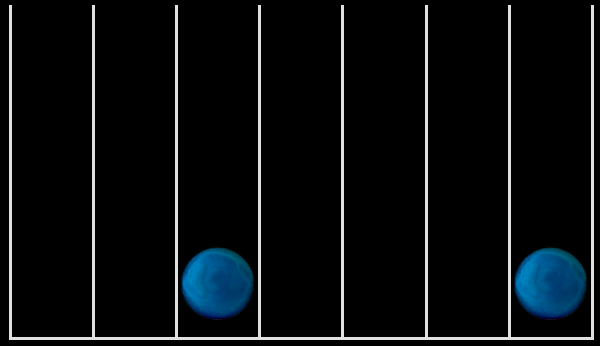
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



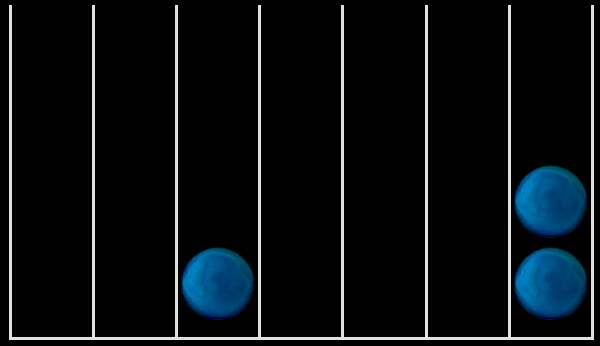
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



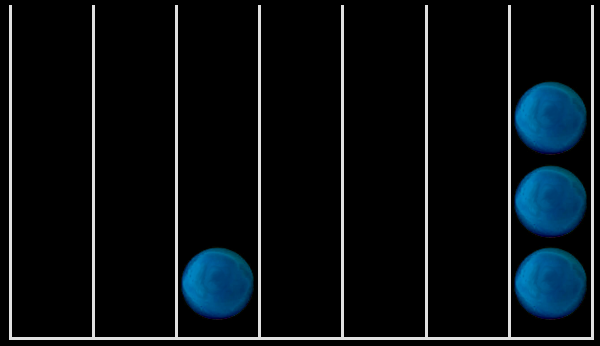
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



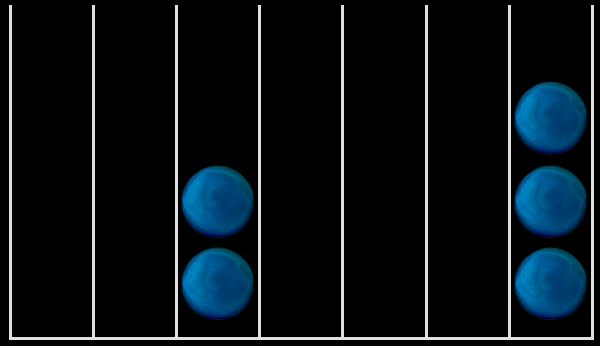
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



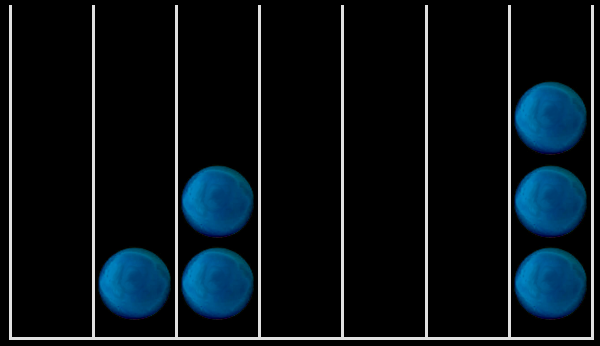
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



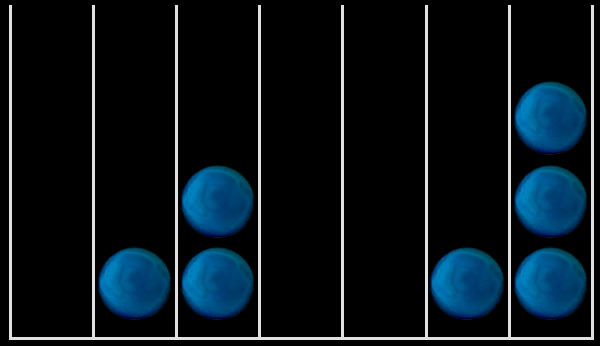
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



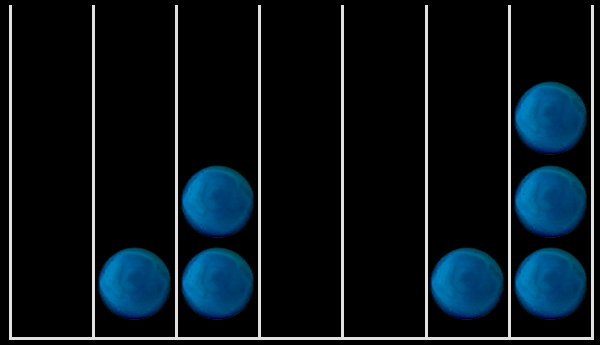
Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



Tirages aléatoires de boules

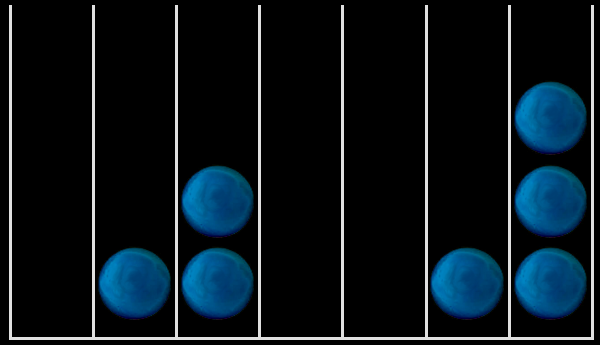
s boules dans $r = \tau s$ tiroirs



p_k : probabilité pour une boule de finir dans un tiroir avec k boules

Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs

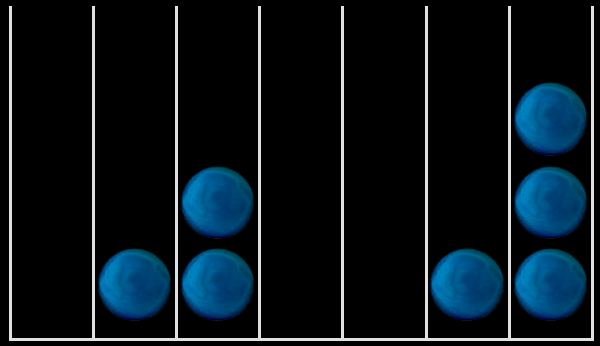


p_k : probabilité pour une boule de finir dans un tiroir avec k boules

$$p_1 = \left(1 - \frac{1}{r}\right)^{s-1} = \mathrm{e}^{(s-1)\log\left(1-\frac{1}{\tau s}\right)} = \mathrm{e}^{-\frac{1}{\tau}+O\left(\frac{1}{s}\right)} = \mathrm{e}^{-\frac{1}{\tau}} + O\left(\frac{1}{s}\right)$$

Tirages aléatoires de boules

s boules dans $r = \tau s$ tiroirs



p_k : probabilité pour une boule de finir dans un tiroir avec k boules

$$p_1 = \left(1-\frac{1}{r}\right)^{s-1} = \mathrm{e}^{(s-1)\log\left(1-\frac{1}{\tau s}\right)} = \mathrm{e}^{-\frac{1}{\tau}+O\left(\frac{1}{s}\right)} = \mathrm{e}^{-\frac{1}{\tau}}+O\left(\frac{1}{s}\right)$$

$$p_k = \binom{s-1}{k-1}\frac{1}{r^{k-1}}\left(1-\frac{1}{r}\right)^{s-k} = \frac{\mathrm{e}^{-\frac{1}{\tau}}}{(k-1)!\,\tau^{k-1}}+O\left(\frac{1}{s}\right)$$

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\, b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\, b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$
- Soit δ^* la partie « sans collisions » de δ

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\, b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$
- Soit δ^* la partie « sans collisions » de δ
- Recommencer avec $\tilde{f} + \delta^*$ jusqu'à $\sigma = s$

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\,b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$
- Soit δ^* la partie « sans collisions » de δ
- Recommencer avec $\tilde{f} + \delta^*$ jusqu'à $\sigma = s$

En moyenne : δ^* contient $\mathrm{e}^{-\frac{1}{\tau}}(s - \sigma)$ termes

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\,b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$
- Soit δ^* la partie « sans collisions » de δ
- Recommencer avec $\tilde{f} + \delta^*$ jusqu'à $\sigma = s$

En moyenne : δ^* contient $\mathrm{e}^{-\frac{1}{\tau}}(s - \sigma)$ termes

Complexité : $\sim \tau\,(M^\circ_{\mathbb{K}}(s) + M^\circ_{\mathbb{K}}((1 - \mathrm{e}^{-\frac{1}{\tau}})\,s) + M^\circ_{\mathbb{K}}((1 - \mathrm{e}^{-\frac{1}{\tau}})^2\,s) + \cdots) + O(s \log s)$

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\,b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$
- Soit δ^* la partie « sans collisions » de δ
- Recommencer avec $\tilde{f} + \delta^*$ jusqu'à $\sigma = s$

En moyenne : δ^* contient $\mathrm{e}^{-\frac{1}{\tau}}(s - \sigma)$ termes

Complexité : $\sim \tau\,\mathrm{e}^{\frac{1}{\tau}}\,\mathsf{M}^{\circ}_{\mathbb{K}}(s) + O(s \log s)$

Interpolation partielle itérée

(amélioration d'une technique de Arnold–Giesbrecht–Roche)

- En entrée : a, b et $\tilde{f} = \sum_{i \leqslant \sigma} c_i x^{e_i}$ avec $\sigma < s$ (modulo permutation d'indices)
- Tirer au hasard λ pour $r = \tau\,(s - \sigma)$
- Calculer $\delta := a(t^\lambda)\,b(t^\lambda) - \tilde{f}(t^\lambda)$ modulo $t^r - 1$
- Soit δ^* la partie « sans collisions » de δ
- Recommencer avec $\tilde{f} + \delta^*$ jusqu'à $\sigma = s$

En moyenne : δ^* contient $\mathrm{e}^{-\frac{1}{\tau}}(s - \sigma)$ termes

Complexité : $\sim \tau\,\mathrm{e}^{\frac{1}{\tau}}\,\mathsf{M}^{\circ}_{\mathbb{K}}(s) + O(s \log s)$

$$\mathsf{M}^{\mathrm{sparse}}_{\mathbb{K}}(s) \;\leqslant_{\text{heuristique}}\; (\mathrm{e} + o(1))\,\mathsf{M}^{\circ}_{\mathbb{K}}(s) + O(s \log s)$$

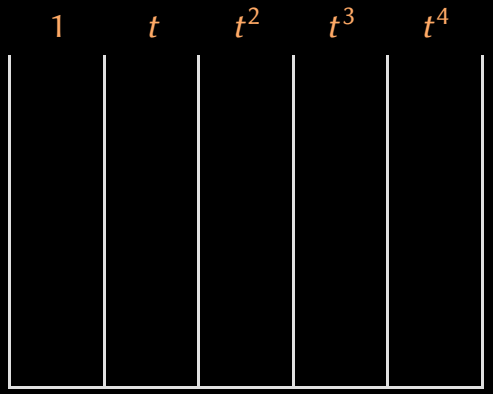
Jeux des boules mystères

$$a = x y^5 + 3 x y^6 z - 2 x^8 y^{10} + x^{10} y^{14} z^3$$
$$b = 2 + y z + 3 x^2 y^4 z^3$$

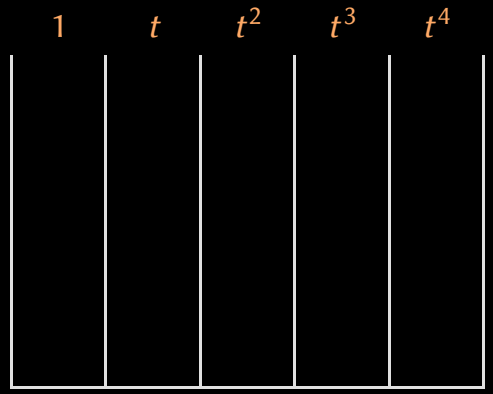
$$f = a b = 3 x^{12} y^{18} z^6 + x^{10} y^{15} z^4 + 9 x^3 y^{10} z^4 + 3 x^3 y^9 z^3 - 4 x^{10} y^{14} z^3 + 3 x y^7 z^2 + 7 x y^6 z - 2 x^8 y^{11} z + 2 x y^5 - 4 x^8 y^{10}$$

Jeux des boules mystères

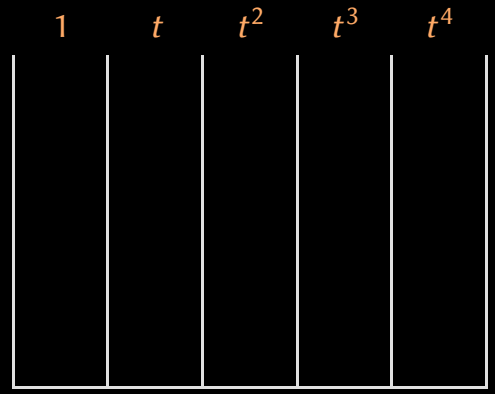
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



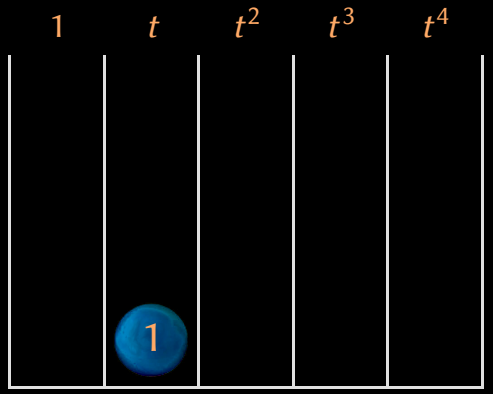
$(x, y, z) = (1, 1, t)$



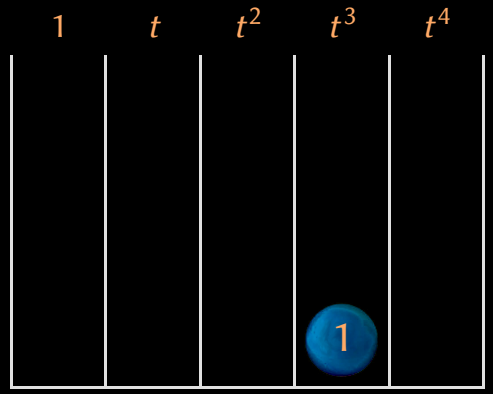
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

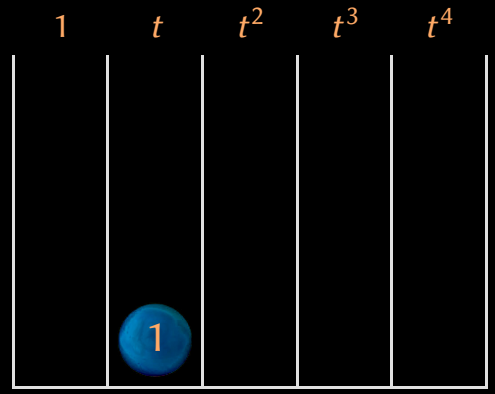
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



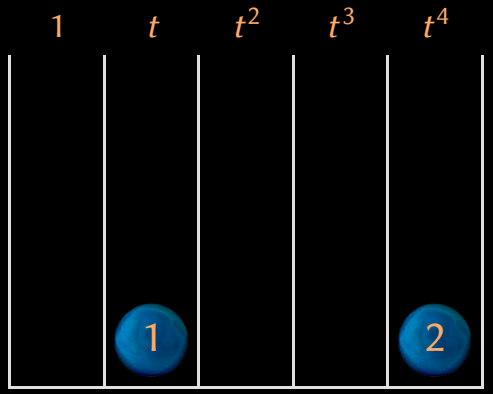
$(x, y, z) = (1, 1, t)$



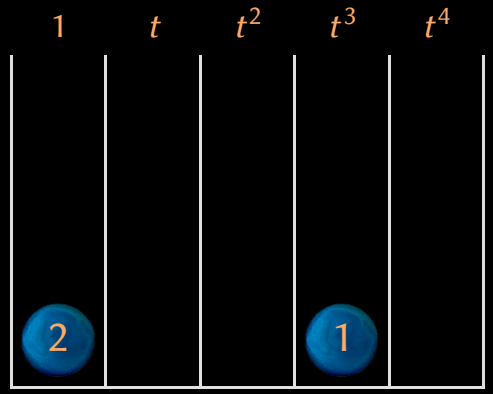
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

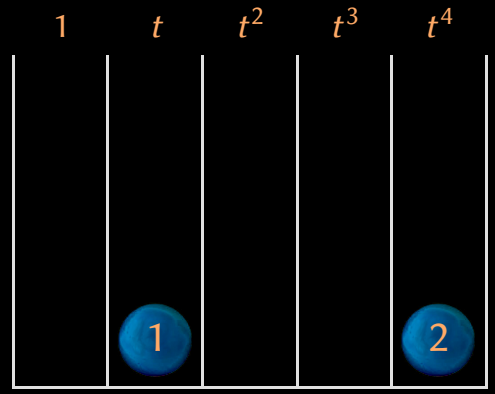
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



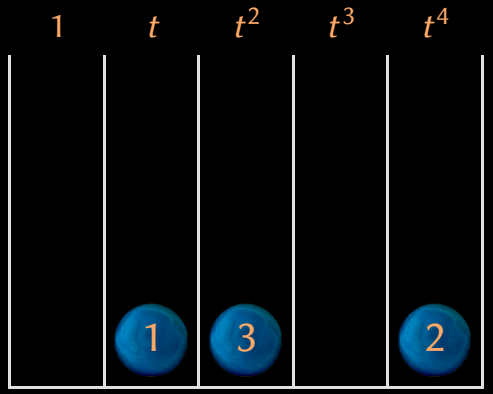
$(x, y, z) = (1, 1, t)$



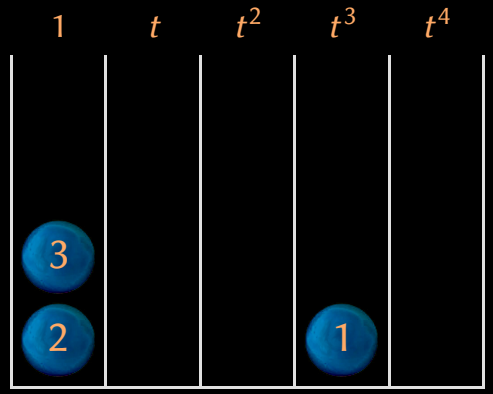
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

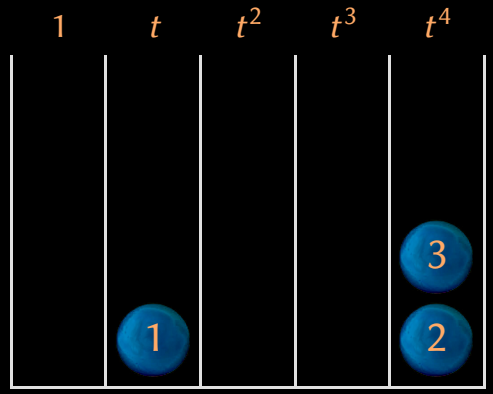
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



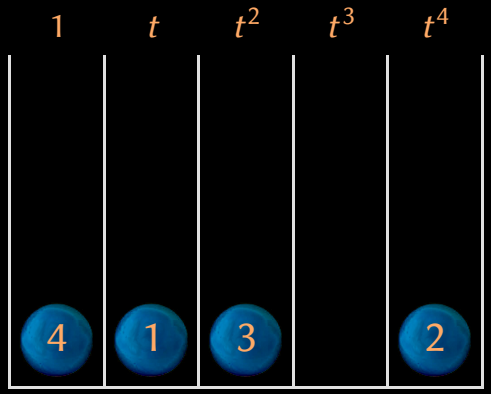
$(x, y, z) = (1, 1, t)$



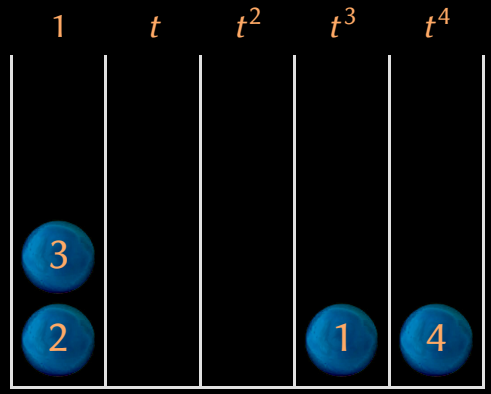
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

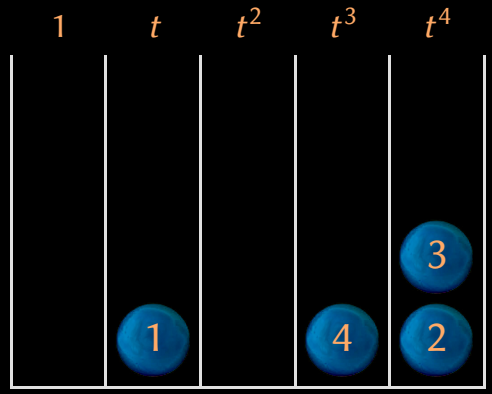
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



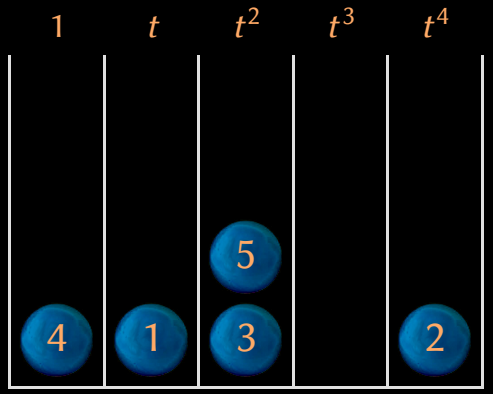
$(x, y, z) = (1, 1, t)$



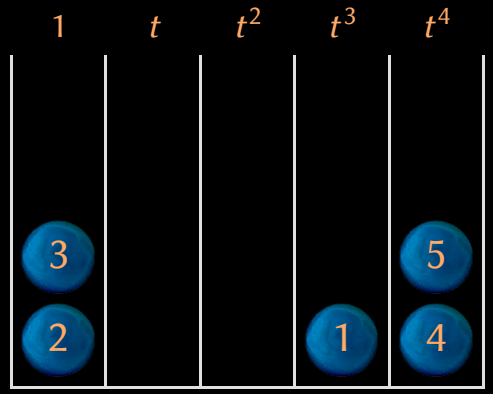
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

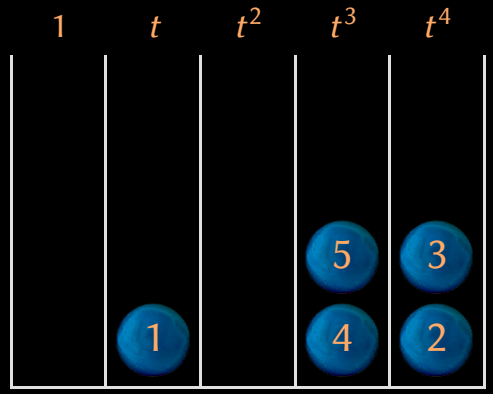
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



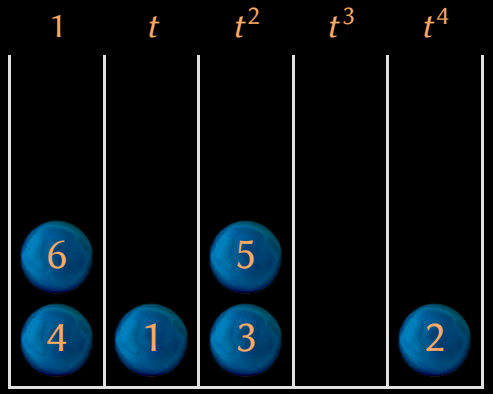
$(x, y, z) = (1, 1, t)$



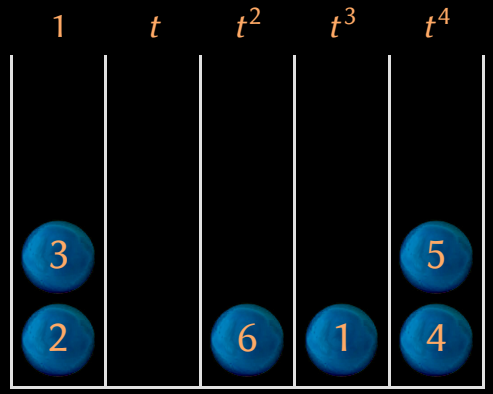
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

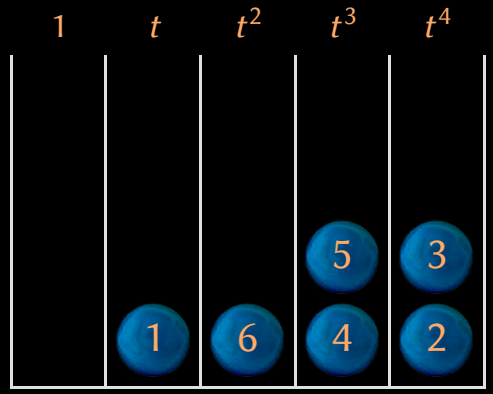
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



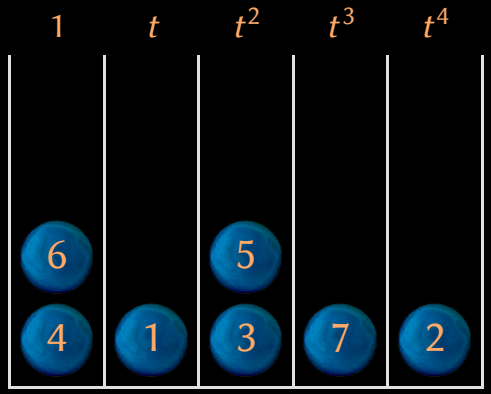
$(x, y, z) = (1, 1, t)$



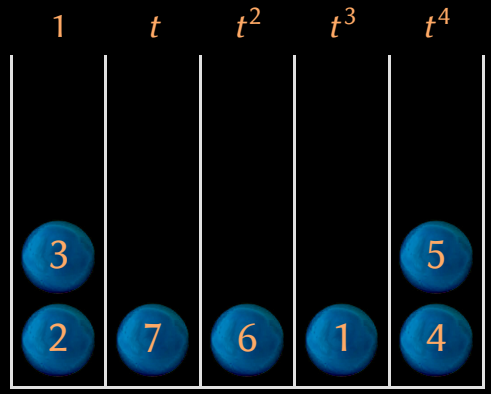
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

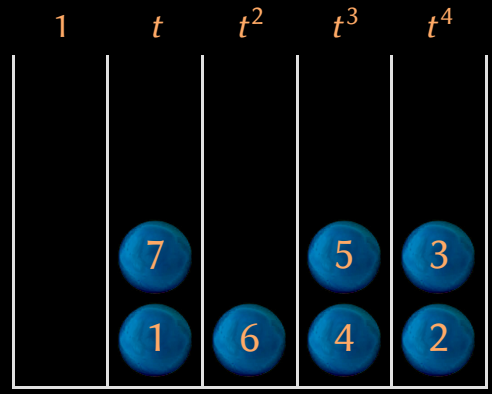
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



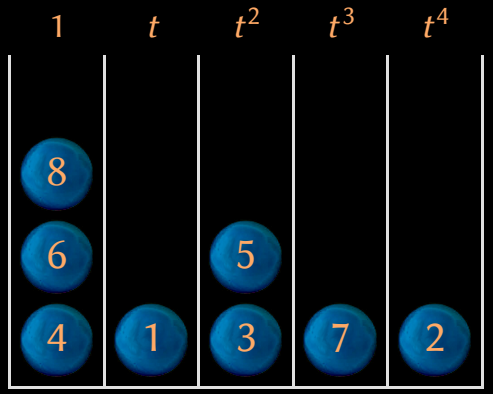
$(x, y, z) = (1, 1, t)$



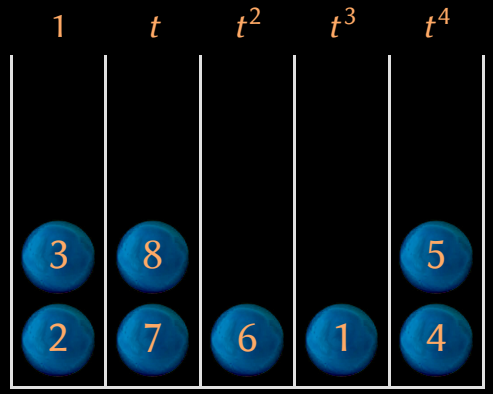
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

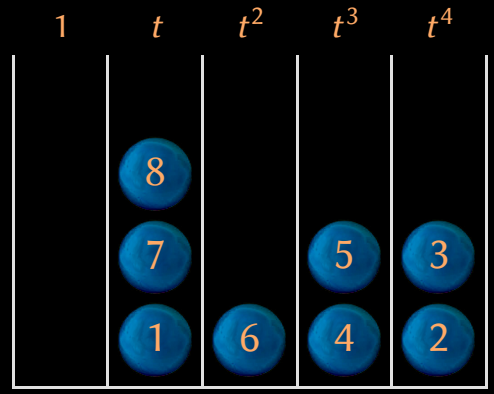
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



$(x, y, z) = (1, 1, t)$

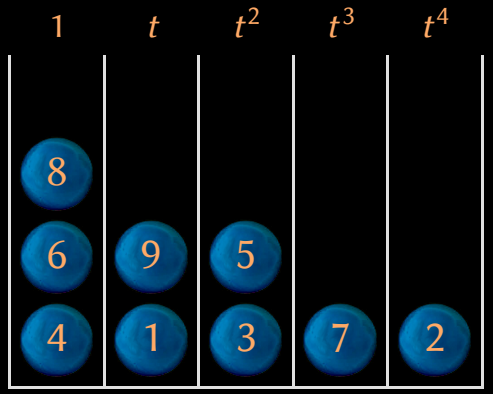


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

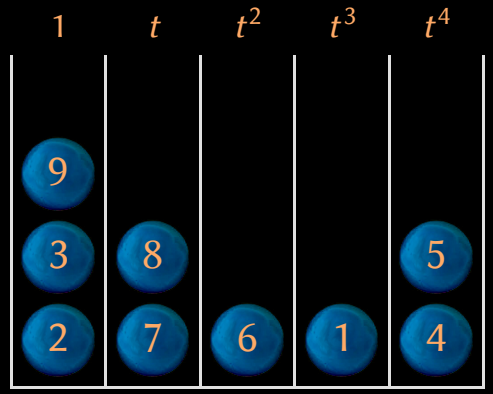
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

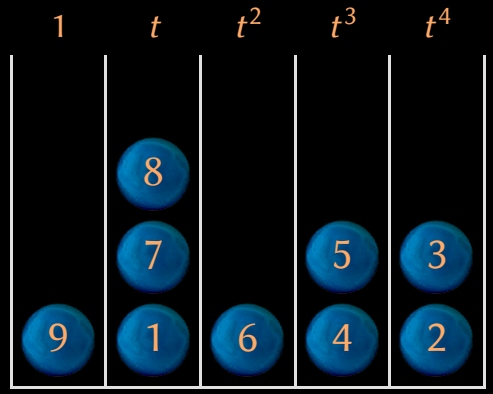
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



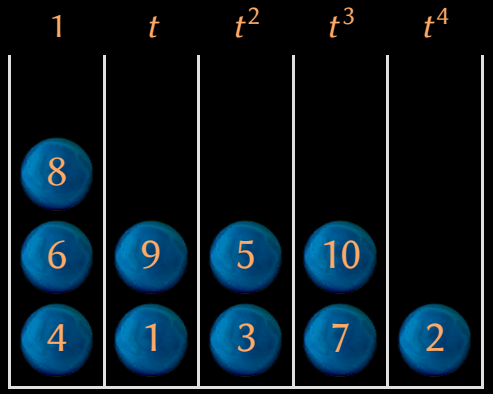
$(x, y, z) = (1, 1, t)$



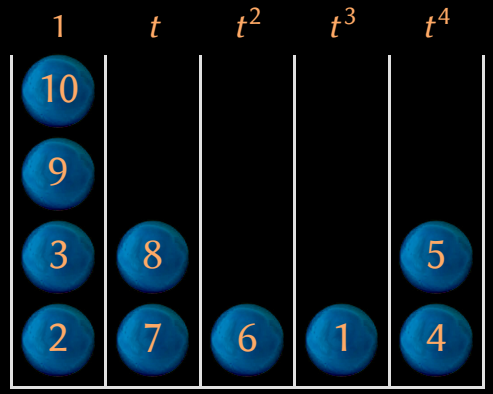
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

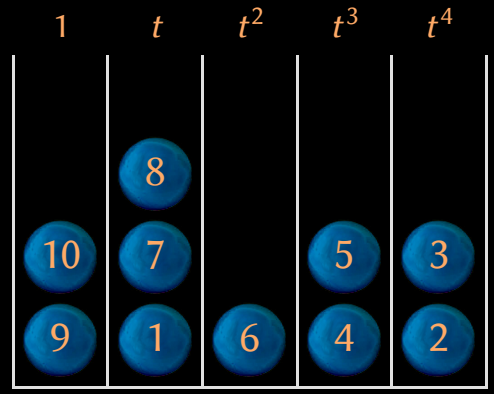
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



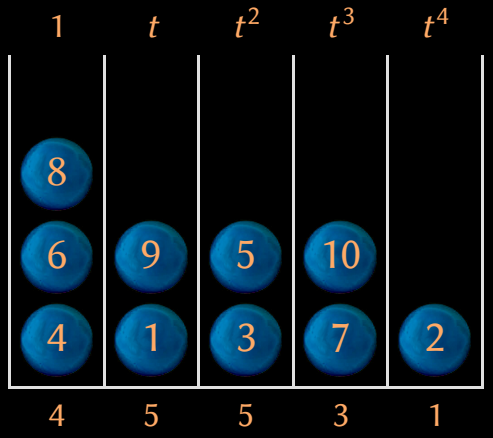
$(x, y, z) = (1, 1, t)$



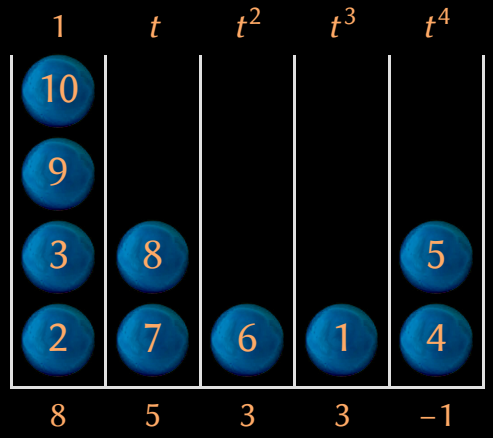
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

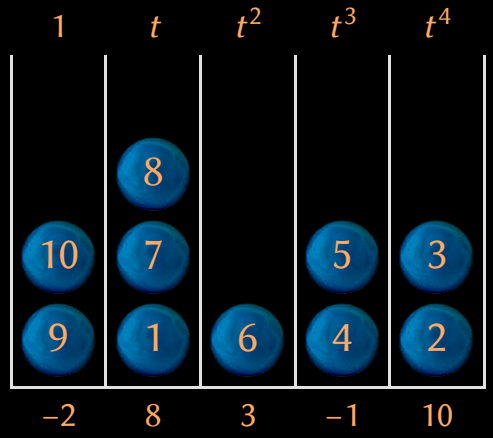
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



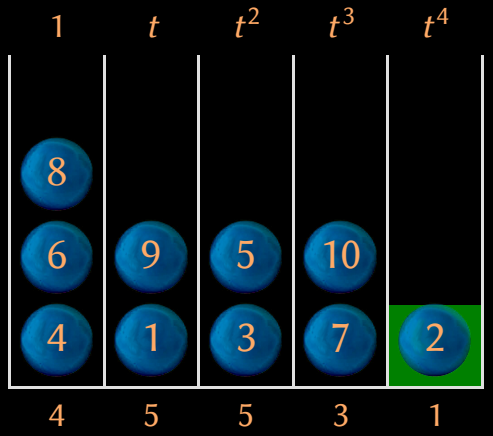
$(x, y, z) = (1, 1, t)$



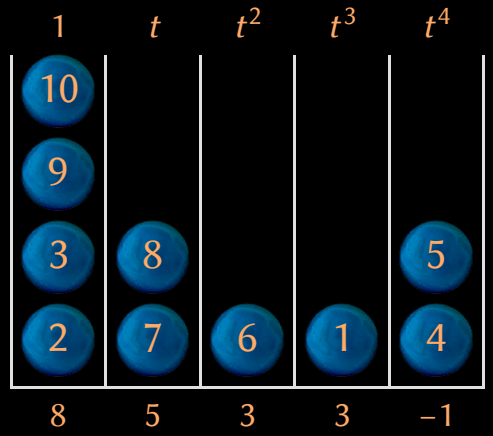
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

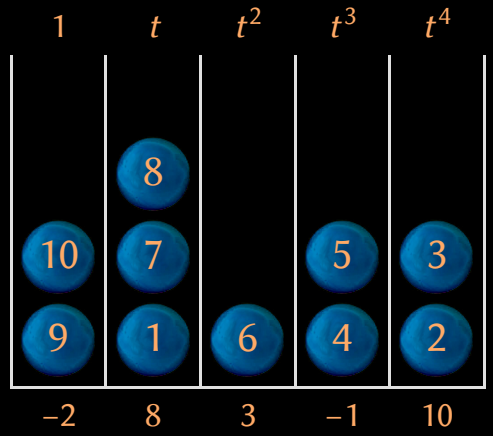
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



$(x, y, z) = (1, 1, t)$

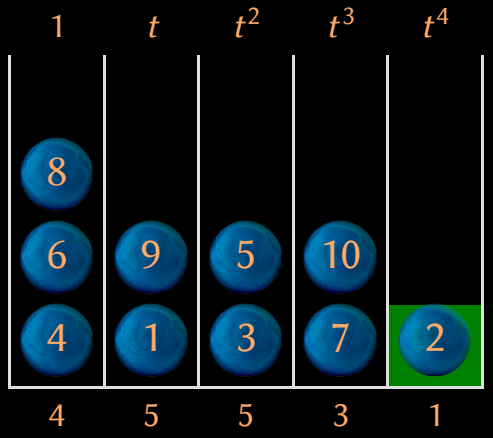


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

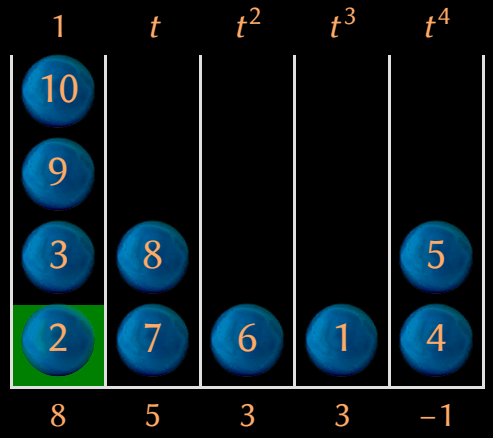
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

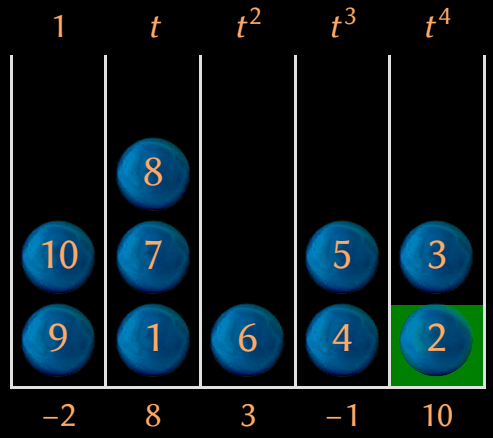
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



$(x, y, z) = (1, 1, t)$



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

$(x, y, z) = (t, t, t)$

1	t	t^2	t^3	t^4
8				
6	9	5	10	
4	1	3	7	
4	5	5	3	0

$(x, y, z) = (1, t, 1)$

1	t	t^2	t^3	t^4
10				
9	8		5	
3	7	6	1	4
7	5	3	3	−1

$(x, y, z) = (1, 1, t)$

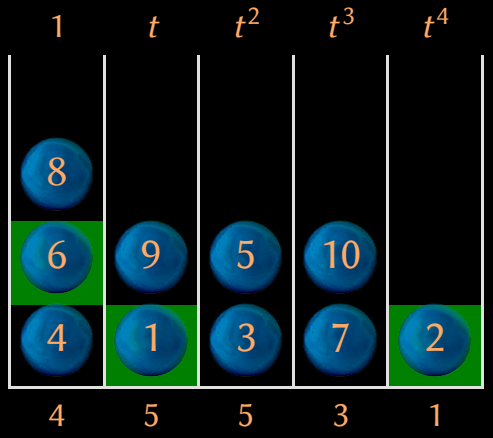
1	t	t^2	t^3	t^4
	8			
10	7		5	
9	1	6	4	3
−2	8	3	−1	9

$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

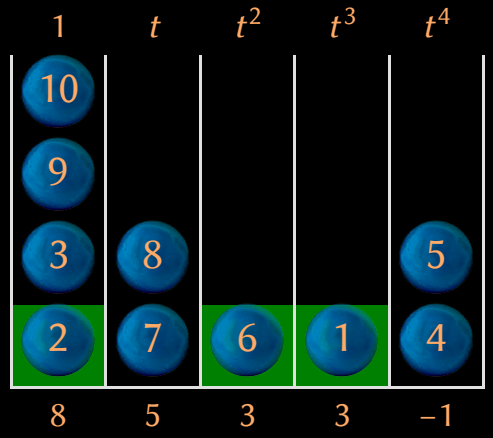
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

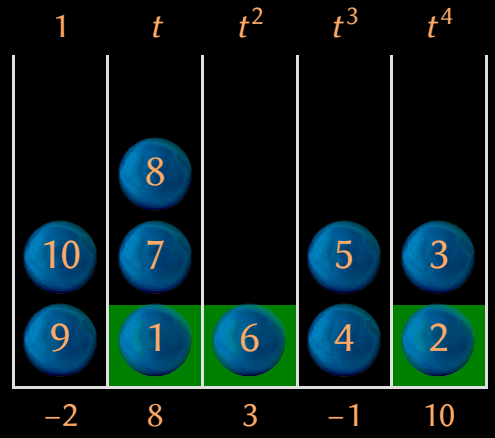
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



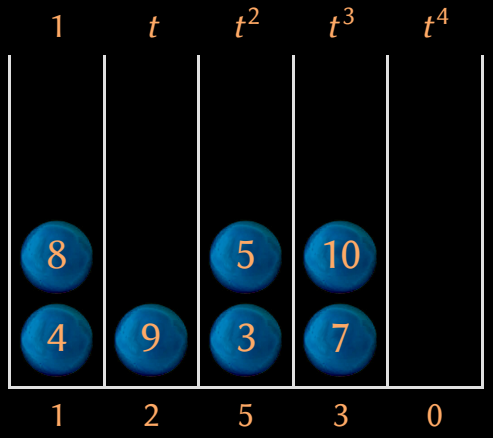
$(x, y, z) = (1, 1, t)$



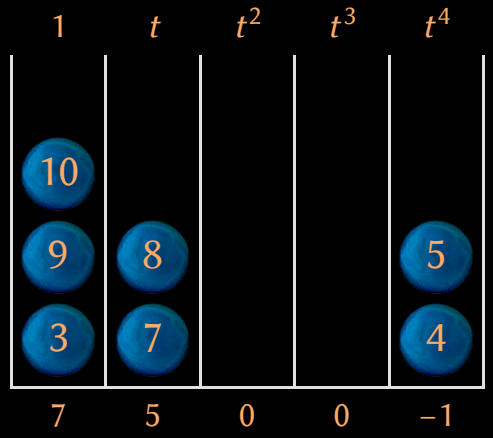
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

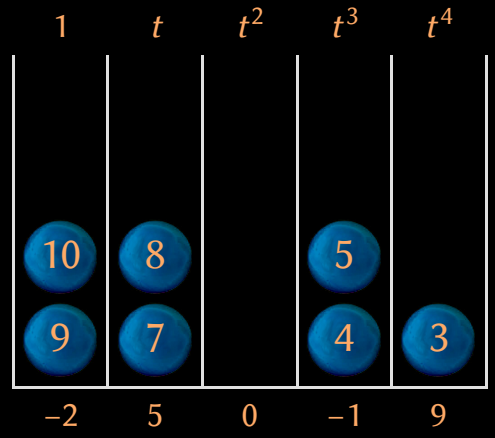
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



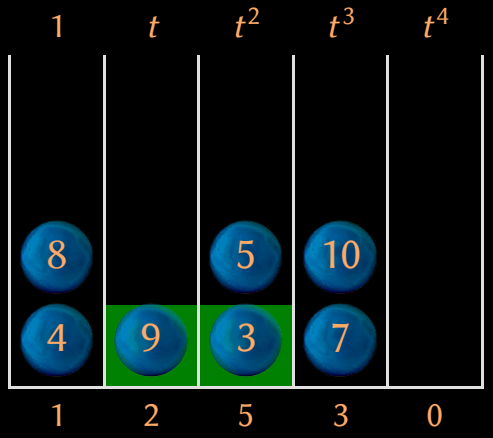
$(x, y, z) = (1, 1, t)$



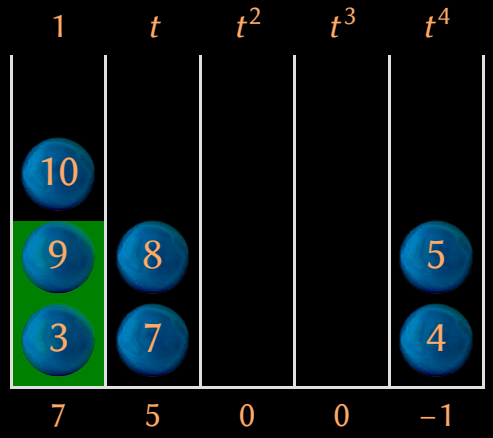
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

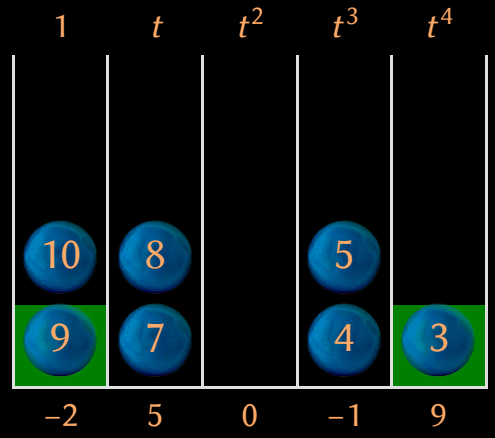
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



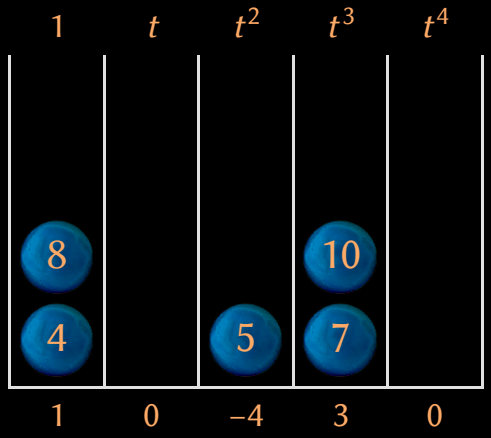
$(x, y, z) = (1, 1, t)$



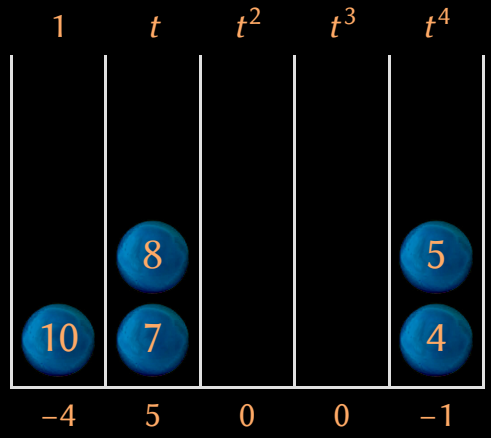
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

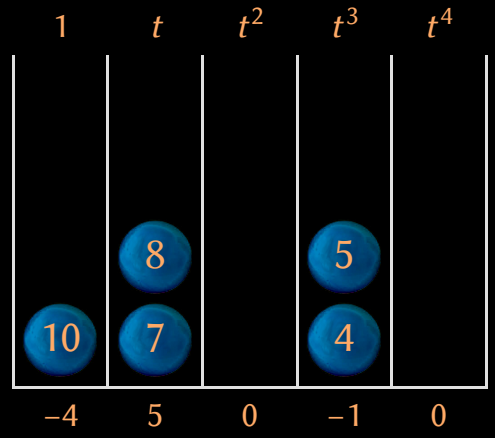
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



$(x, y, z) = (1, 1, t)$

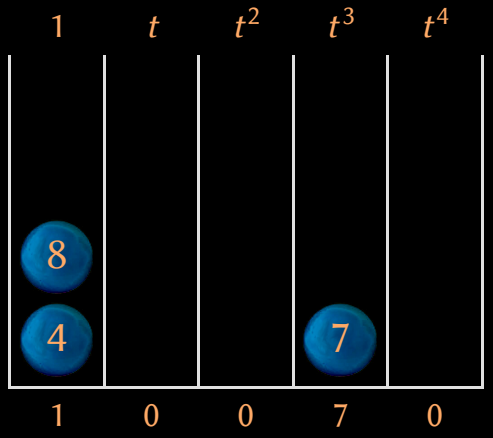


$$f = \overbrace{3\,x^{12}\,y^{18}\,z^{6}}^{1} + \overbrace{1\,x^{10}\,y^{15}\,z^{4}}^{2} + \overbrace{9\,x^{3}\,y^{10}\,z^{4}}^{3} + \overbrace{3\,x^{3}\,y^{9}\,z^{3}}^{4} + \overbrace{(-4)\,x^{10}\,y^{14}\,z^{3}}^{5} +$$

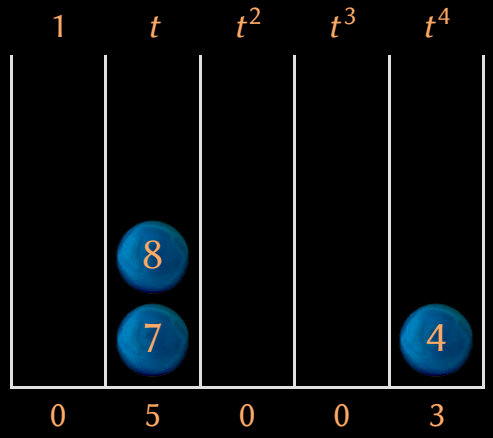
$$\overbrace{3\,x\,y^{7}\,z^{2}}^{6} + \overbrace{7\,x\,y^{6}\,z}^{7} + \overbrace{(-2)\,x^{8}\,y^{11}\,z}^{8} + \overbrace{2\,x\,y^{5}}^{9} + \overbrace{(-4)\,x^{8}\,y^{10}}^{10}$$

Jeux des boules mystères

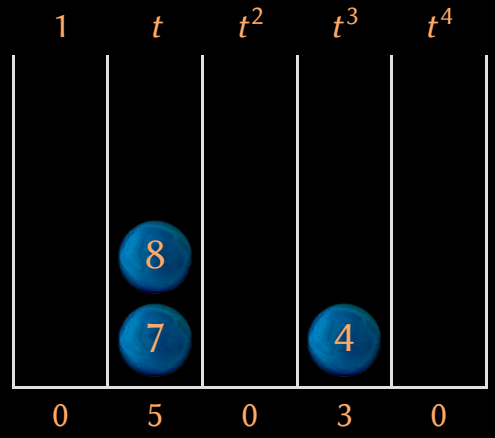
$(x, y, z) = (t, t, t)$



$(x, y, z) = (1, t, 1)$



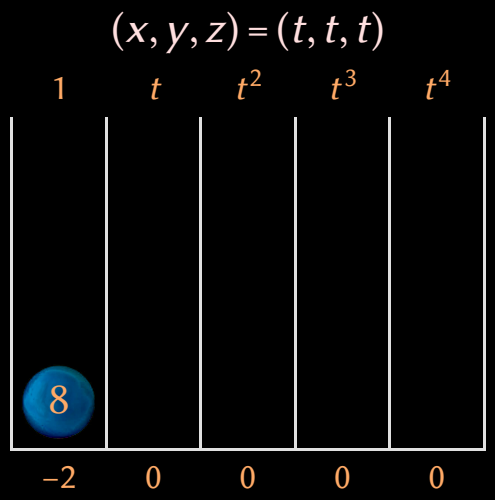
$(x, y, z) = (1, 1, t)$

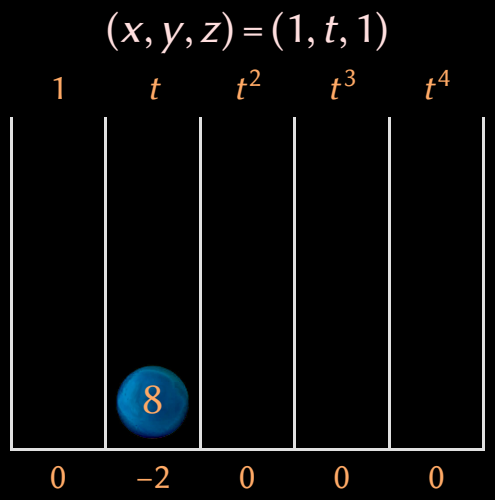


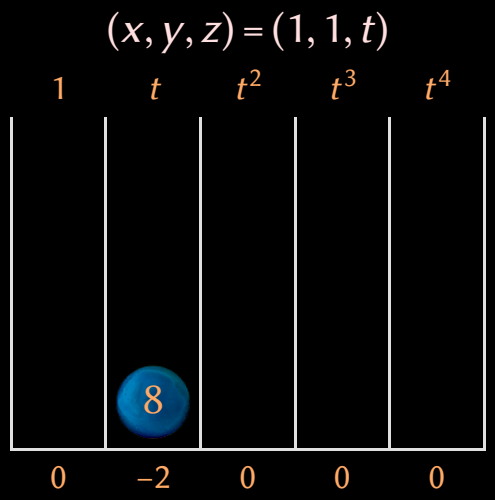
$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères

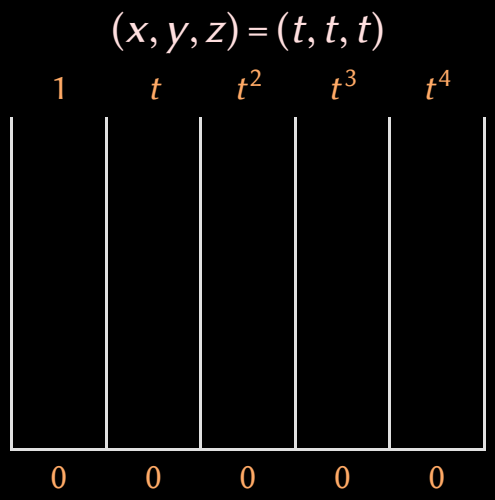


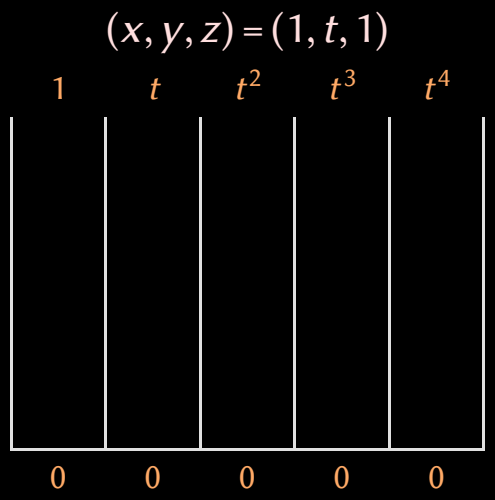


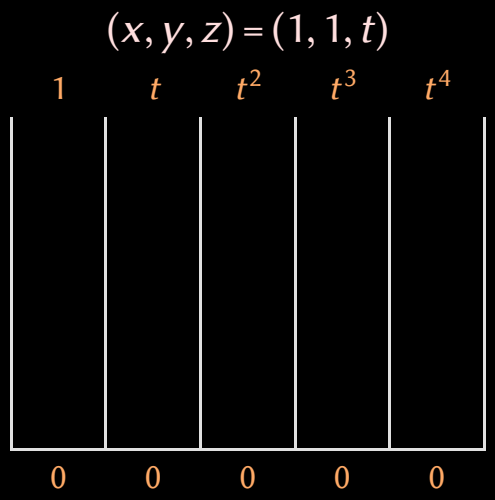


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Jeux des boules mystères







$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

Probabilités pour $\tau = 1/2$

$p_{i,k}$ proportion des boules se trouvant dans un tiroir avec k boules au début du tour i

$p_{i,k}$	$k=1$	2	3	4	5	6	7	σ_i
$i=1$	0.13534	0.27067	0.27067	0.18045	0.09022	0.03609	0.01203	1.00000
2	0.06643	0.25063	0.18738	0.09340	0.03491	0.01044	0.00260	0.64646
3	0.04567	0.21741	0.13085	0.05251	0.01580	0.00380	0.00076	0.46696
4	0.03690	0.18019	0.08828	0.02883	0.00706	0.00138	0.00023	0.34292
5	0.03234	0.13952	0.05443	0.01416	0.00276	0.00043	0.00006	0.24371
6	0.02869	0.09578	0.02811	0.00550	0.00081	0.00009	0.00001	0.15899
7	0.02330	0.05240	0.01033	0.00136	0.00013	0.00001	0.00000	0.08752
8	0.01428	0.01823	0.00193	0.00014	0.00001	0.00000	0.00000	0.03459
9	0.00442	0.00249	0.00009	0.00000	0.00000	0.00000	0.00000	0.00700
10	0.00030	0.00005	0.00000	0.00000	0.00000	0.00000	0.00000	0.00035
11	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000

Probabilités pour $\tau = 1/2$

$p_{i,k}$ proportion des boules se trouvant dans un tiroir avec k boules au début du tour i

$p_{i,k}$	$k=1$	2	3	4	5	6	7	σ_i
$i=1$	0.13534	0.27067	0.27067	0.18045	0.09022	0.03609	0.01203	1.00000
2	0.06643	0.25063	0.18738	0.09340	0.03491	0.01044	0.00260	0.64646
3	0.04567	0.21741	0.13085	0.05251	0.01580	0.00380	0.00076	0.46696
4	0.03690	0.18019	0.08828	0.02883	0.00706	0.00138	0.00023	0.34292
5	0.03234	0.13952	0.05443	0.01416	0.00276	0.00043	0.00006	0.24371
6	0.02869	0.09578	0.02811	0.00550	0.00081	0.00009	0.00001	0.15899
7	0.02330	0.05240	0.01033	0.00136	0.00013	0.00001	0.00000	0.08752
8	0.01428	0.01823	0.00193	0.00014	0.00001	0.00000	0.00000	0.03459
9	0.00442	0.00249	0.00009	0.00000	0.00000	0.00000	0.00000	0.00700
10	0.00030	0.00005	0.00000	0.00000	0.00000	0.00000	0.00000	0.00035
11	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000

$$M_{\mathbb{K}}^{\text{sparse}}(s) \leqslant_{\text{heuristique}} \tfrac{3}{2} M_{\mathbb{K}}^{\circ}(s) + O(s)$$

$$0{,}407264 < \tau_{\text{crit}} < 0{,}407265$$

Probabilités, suite

$$0{,}407264 \;<\; \tau_{\text{crit}} \;<\; 0{,}407265$$

$$M_{\mathbb{K}}^{\text{sparse}}(s) \;\leqslant_{\text{heuristique}}\; 1{,}221795\, M_{\mathbb{K}}^{\circ}(s) + O(s)$$

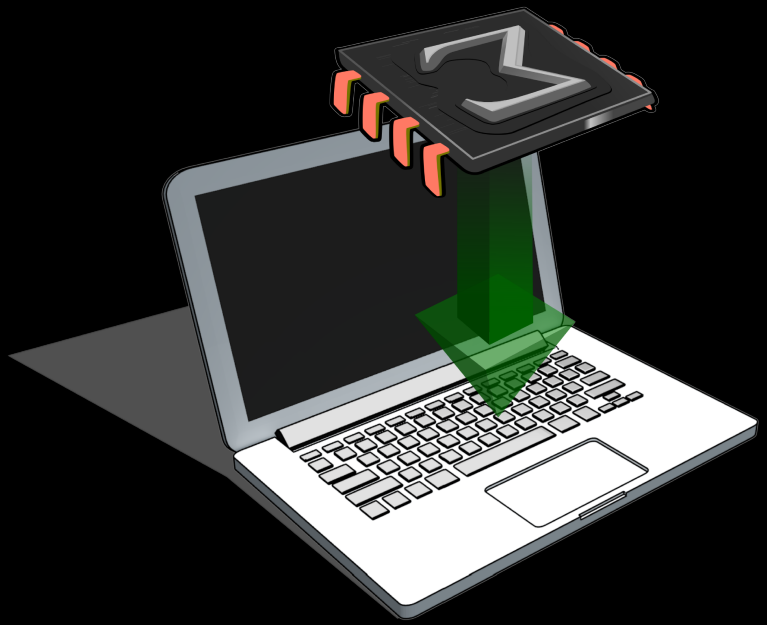
$$0{,}407264 \;<\; \tau_{\text{crit}} \;<\; 0{,}407265$$

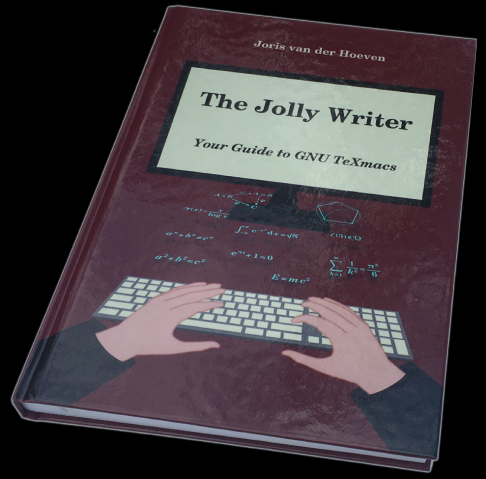
$$M_{\mathbb{K}}^{\text{sparse}}(s) \;\leqslant_{\text{heuristique}}\; 1{,}221795\, M_{\mathbb{K}}^{\circ}(s) + O(s)$$

Polynômes en n variables de degré total d

n	2	2	2	3	3	3	4	4	5	7	10
d	100	250	1000	25	50	100	20	40	20	15	10
s	5151	31626	501501	3276	23426	176853	10626	135751	53130	170544	184756
$3\,\tau$	1.14	1.14	1.14	1.14	1.14	1.14	1.11	1.14	1.14	1.17	1.20

Merci !





http://www.texmacs.org