

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	$l(b) e^{O(\sqrt{\log \log b})}$	détendu	vdH
$\mathbb{K}[[z]]$	$M_{\mathbb{K}}(d) e^{O(\sqrt{\log \log d})}$	détendu	vdH
$\mathbb{K}^{r \times r}[x]$	$O(\Omega_{\mathbb{K}}(r) d + r^2 M_{\mathbb{K}}(d))$	$ \mathbb{K} > d$	Bostan–Schost
$\mathbb{K}[x, \partial_x]$	$O(\Omega_{\mathbb{K}}(r) d/r + r M_{\mathbb{K}}(d) \log d)$	$d \geq r := \deg_{\partial}$	Benoit–Bostan–vdH
	$O(\Omega_{\mathbb{K}}(d) r/d + d M_{\mathbb{K}}(r) \log r)$	$r \geq d := \deg_x$	
$\mathbb{L} \mathbb{K}$ tower	$M_{\mathbb{K}}(d) e^{O(\sqrt{\log d})}$	$d = [\mathbb{L} : \mathbb{K}]$	vdH–Lecerf
$\mathbb{K}[x_1, \dots, x_n]$	$O(M_{\mathbb{K}}(s))$	creux, heuristique	vdH–Lecerf, vdH

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

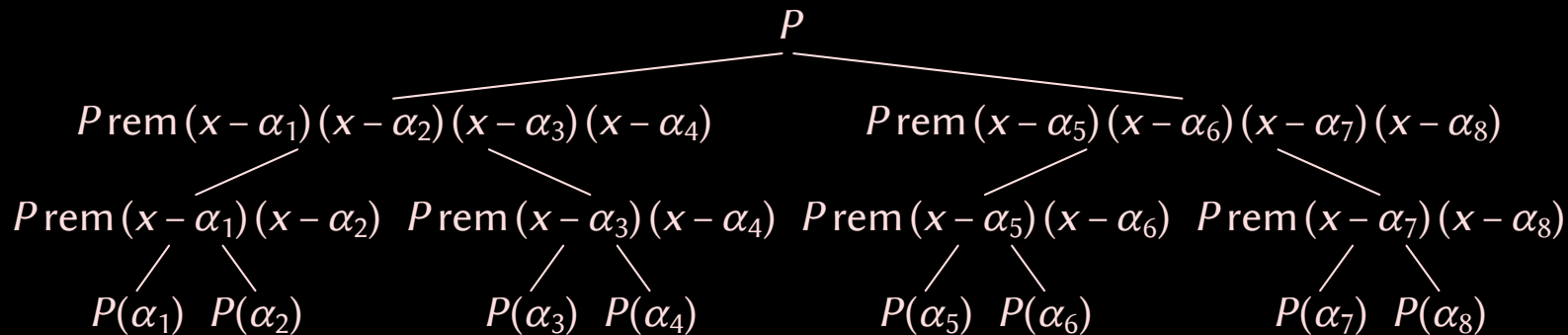
Évaluation multi-points : $P \in \mathbb{K}[x], \deg P < d, \alpha_1, \dots, \alpha_d \in \mathbb{K} \xrightarrow{?} P(\alpha_1), \dots, P(\alpha_d)$

Observation : $P(\alpha_k) = P \bmod (x - \alpha_k)$

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

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

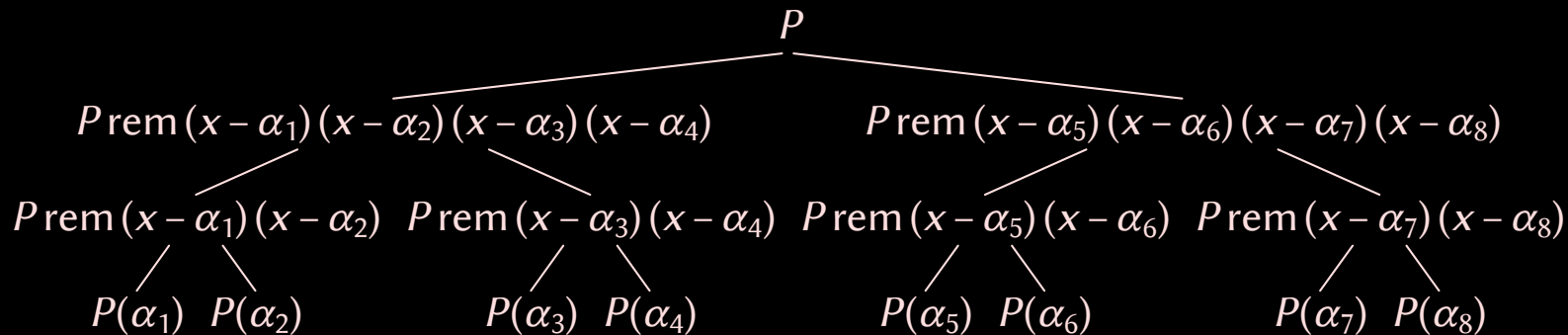
Arbre de restes



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

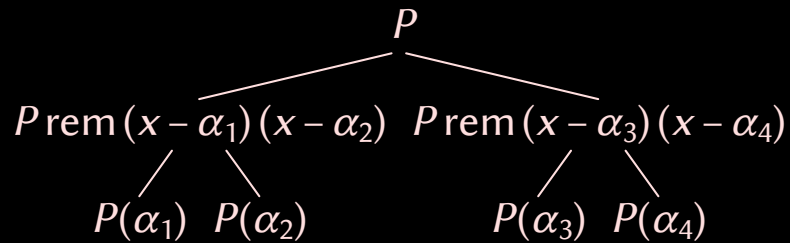
Observation : $P(\alpha_k) = P \operatorname{rem} (x - \alpha_k)$

Arbre de restes



$$E_{\mathbb{K}}(d) = O(2 M_{\mathbb{K}}(d/2) + 4 M_{\mathbb{K}}(d/4) + \dots) = O(M_{\mathbb{K}}(d) \log d)$$

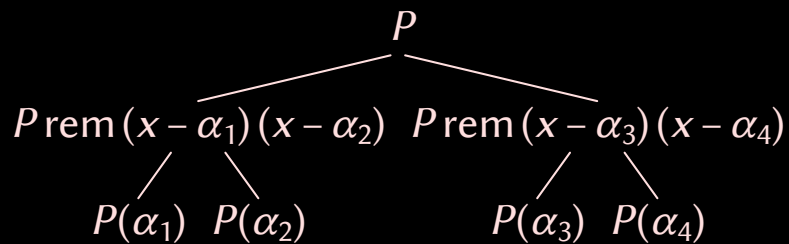
Arbres de restes



$$E_{\mathbb{K}}(d) = O(M_{\mathbb{K}}(d) \log d)$$

$$E_{\mathbb{K}}^{-1}(d) = O(M_{\mathbb{K}}(d) \log d)$$

Arbres de restes



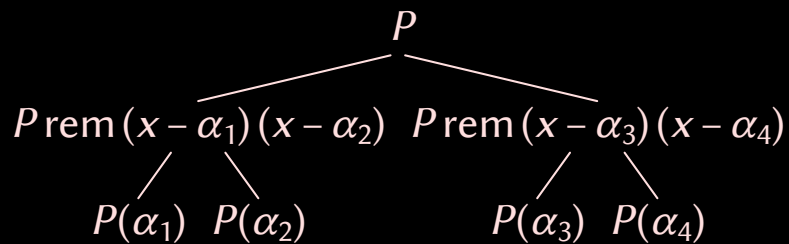
$$E_{\mathbb{K}}(d) = O(M_{\mathbb{K}}(d) \log d)$$

$$E_{\mathbb{K}}^{-1}(d) = O(M_{\mathbb{K}}(d) \log d)$$

Évaluation multi-points

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

Arbres de restes



$$E_{\mathbb{K}}(d) = O(M_{\mathbb{K}}(d) \log d)$$

$$E_{\mathbb{K}}^{-1}(d) = O(M_{\mathbb{K}}(d) \log d)$$

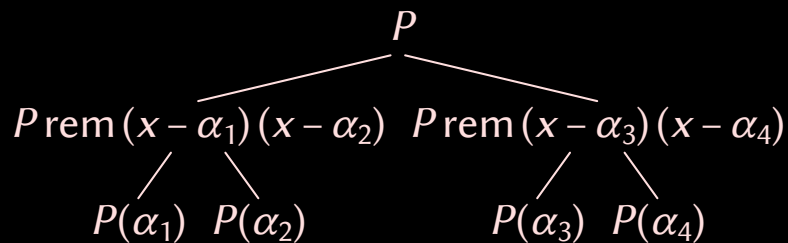
Évaluation multi-points

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

Opération transposée

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

Arbres de restes



$$E_{\mathbb{K}}(d) = O(M_{\mathbb{K}}(d) \log d)$$

$$E_{\mathbb{K}}^{-1}(d) = O(M_{\mathbb{K}}(d) \log d)$$

$$E_{\mathbb{K}}^{\top}(d) = O(M_{\mathbb{K}}(d) \log d)$$


$$E_{\mathbb{K}}^{-1, \top}(d) = O(M_{\mathbb{K}}(d) \log d)$$

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

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


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

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

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

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

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

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

$$\begin{aligned}M_{\mathbb{K}^{r \times r}}(d) &\leq 3 F_{\mathbb{K}^{r \times r}}(n) + n \Omega_{\mathbb{K}}(r) \\ &= 3 r^2 F_{\mathbb{K}}(n) + n \Omega_{\mathbb{K}}(r) \\ &\lesssim r^2 M_{\mathbb{K}}(d) + n \Omega_{\mathbb{K}}(r).\end{aligned}$$

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

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

$$\begin{aligned}M_{\mathbb{K}^{r \times r}}(d) &\leq 3 F_{\mathbb{K}^{r \times r}}(n) + n \Omega_{\mathbb{K}}(r) \\ &= 3 r^2 F_{\mathbb{K}}(n) + n \Omega_{\mathbb{K}}(r) \\ &\lesssim r^2 M_{\mathbb{K}}(d) + n \Omega_{\mathbb{K}}(r).\end{aligned}$$

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

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

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

$$\begin{aligned}M_{\mathbb{K}^{r \times r}}(d) &\leq 3 F_{\mathbb{K}^{r \times r}}(n) + n \Omega_{\mathbb{K}}(r) \\ &= 3 r^2 F_{\mathbb{K}}(n) + n \Omega_{\mathbb{K}}(r) \\ &\lesssim r^2 M_{\mathbb{K}}(d) + n \Omega_{\mathbb{K}}(r).\end{aligned}$$

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

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

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

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

$$\begin{aligned} M_{\mathbb{K}^{r \times r}}(d) &\leq 3 F_{\mathbb{K}^{r \times r}}(n) + n \Omega_{\mathbb{K}}(r) \\ &= 3 r^2 F_{\mathbb{K}}(n) + n \Omega_{\mathbb{K}}(r) \\ &\lesssim r^2 M_{\mathbb{K}}(d) + n \Omega_{\mathbb{K}}(r). \end{aligned}$$

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

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

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

→ Évaluation-interpolation suite géométrique de d points

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

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

$$\begin{aligned}M_{\mathbb{K}^{r \times r}}(d) &\leq 3 F_{\mathbb{K}^{r \times r}}(n) + n \Omega_{\mathbb{K}}(r) \\ &= 3 r^2 F_{\mathbb{K}}(n) + n \Omega_{\mathbb{K}}(r) \\ &\lesssim r^2 M_{\mathbb{K}}(d) + n \Omega_{\mathbb{K}}(r).\end{aligned}$$

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

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

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

→ Évaluation-interpolation suite géométrique de d points

$$M_{\mathbb{K}^{r \times r}}(d) \leq O(r^2 M_{\mathbb{K}}(n)) + n \Omega_{\mathbb{K}}(r)$$

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 $O(MM(d, r))$

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 $O(\text{MM}(d, r))$

Padé-Hermite

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

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

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



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

Des séries comme « flots » de coefficients

$$f = f_0 + \dots$$

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

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

Des séries comme « flots » de coefficients

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

Multiplication paresseuse

$$f = f_0 + \dots$$

$$g = g_0 + \dots$$

$$h = fg = (fg)_0 + \dots$$

g_0	h_0				
	f_0				

Des séries comme « flots » de coefficients

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

Multiplication paresseuse

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

$$g = g_0 + g_1 z + \dots$$

$$h = fg = (fg)_0 + (fg)_1 z + \dots$$

g_1	h_1				
g_0	h_0	h_1			
	f_0	f_1			

Des séries comme « flots » de coefficients

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

Multiplication paresseuse

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

$$g = g_0 + g_1 z + g_2 z^2 + \dots$$

$$h = fg = (fg)_0 + (fg)_1 z + (fg)_2 z^2 + \dots$$

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

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

Multiplication paresseuse

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

$$g = g_0 + g_1 z + g_2 z^2 + g_3 z^3 + \dots$$

$$h = fg = (fg)_0 + (fg)_1 z + (fg)_2 z^2 + (fg)_3 z^3 + \dots$$

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

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

Multiplication paresseuse

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

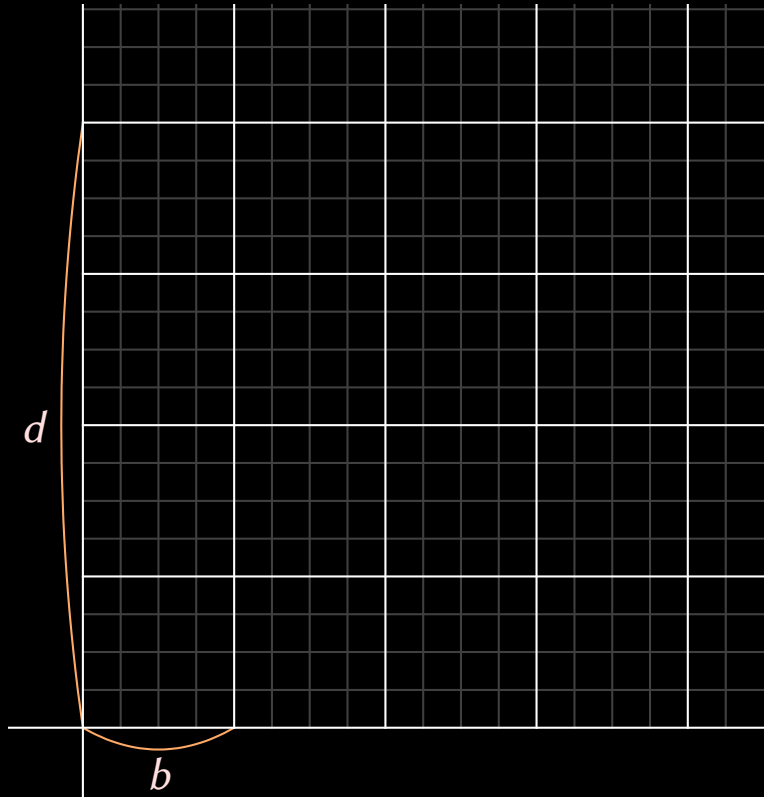
$$g = g_0 + g_1 z + g_2 z^2 + g_3 z^3 + \dots$$

$$h = fg = (fg)_0 + (fg)_1 z + (fg)_2 z^2 + (fg)_3 z^3 + \dots$$

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 $O(d^2)$

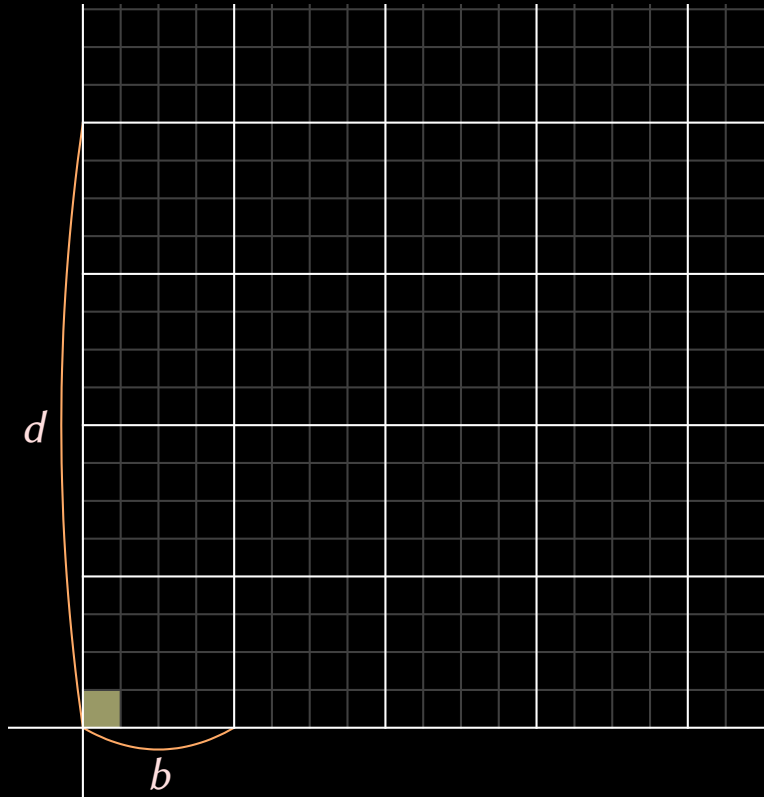
Multiplication détendue d'ordre $d = bl$



$$\omega^{2b} = 1$$

$$R_{\mathbb{K}}(d)?$$

Multiplication détendue d'ordre $d = bl$

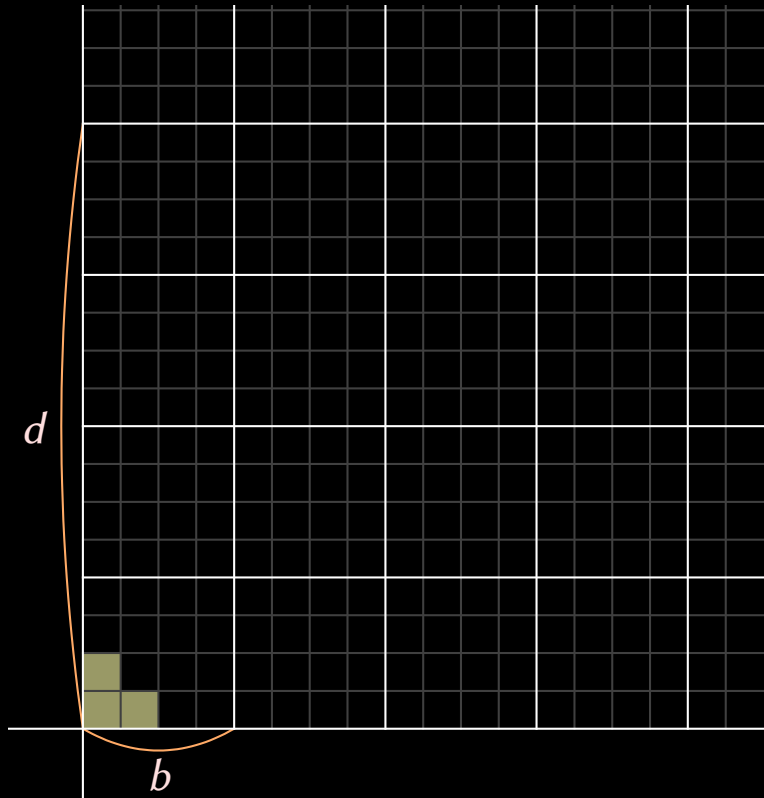


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d)?$$



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

Multiplication détendue d'ordre $d = bl$

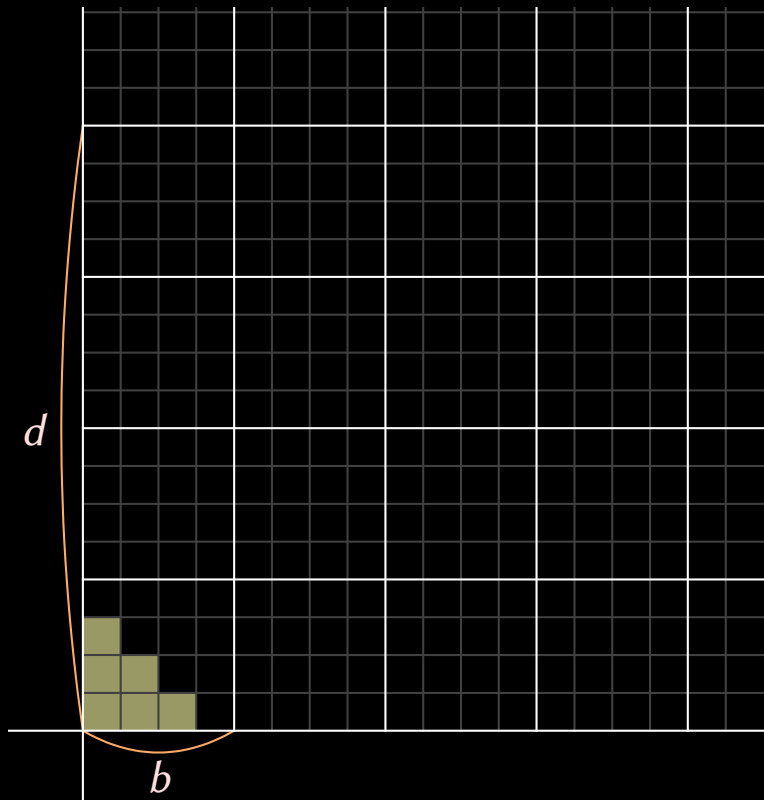


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

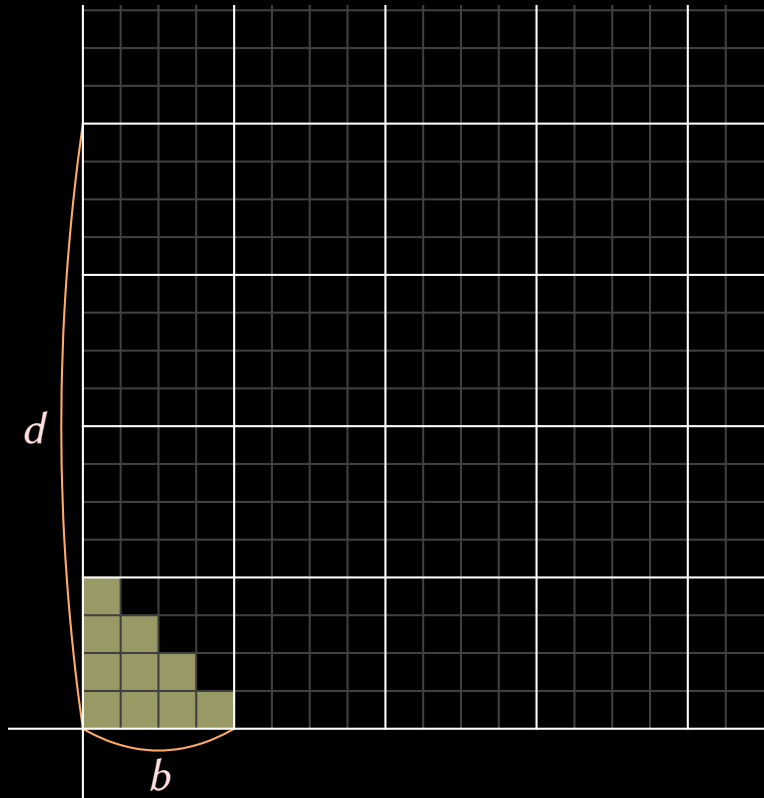


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

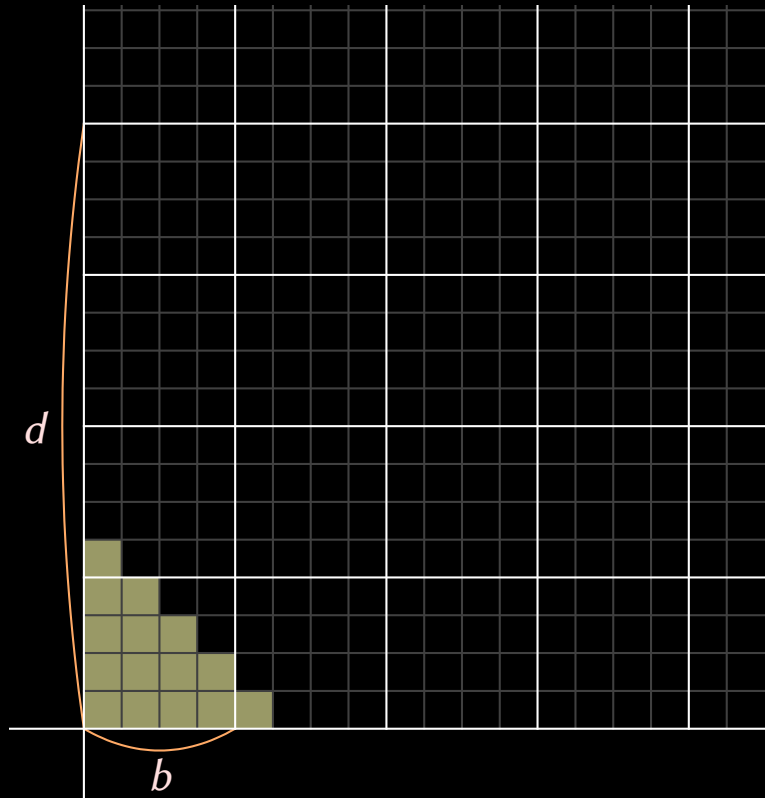


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

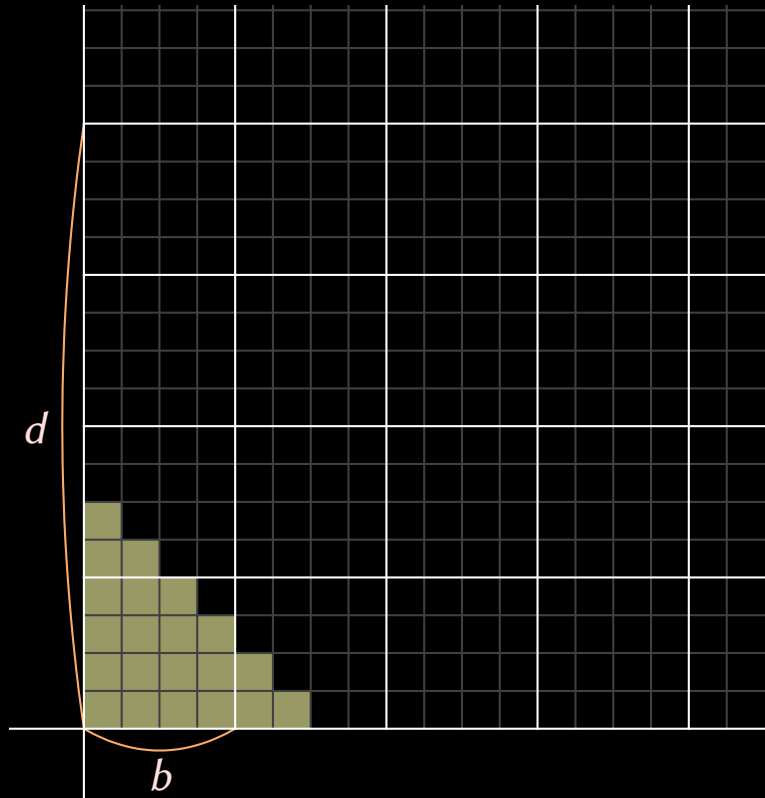


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

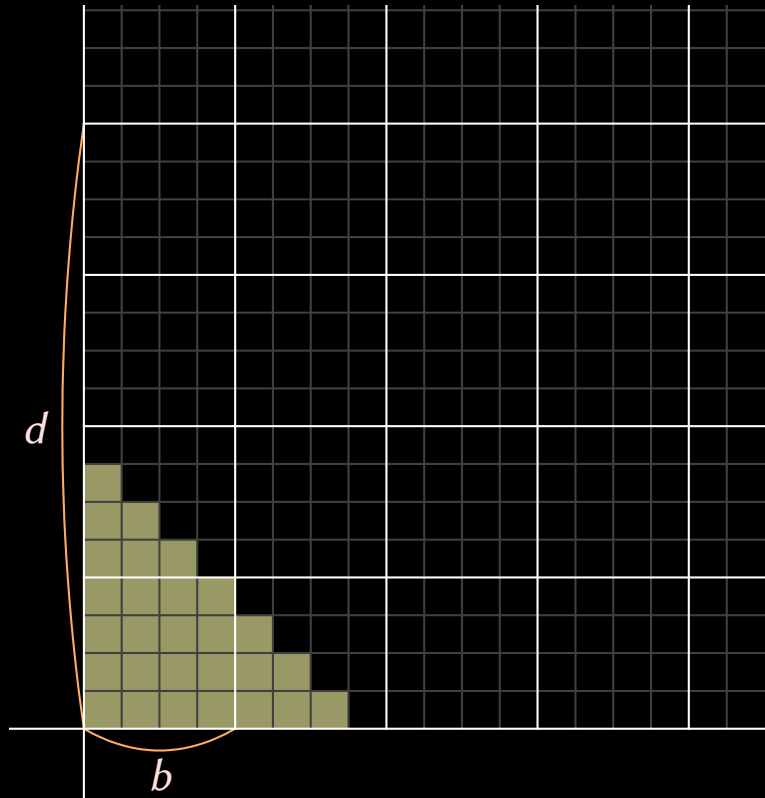


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

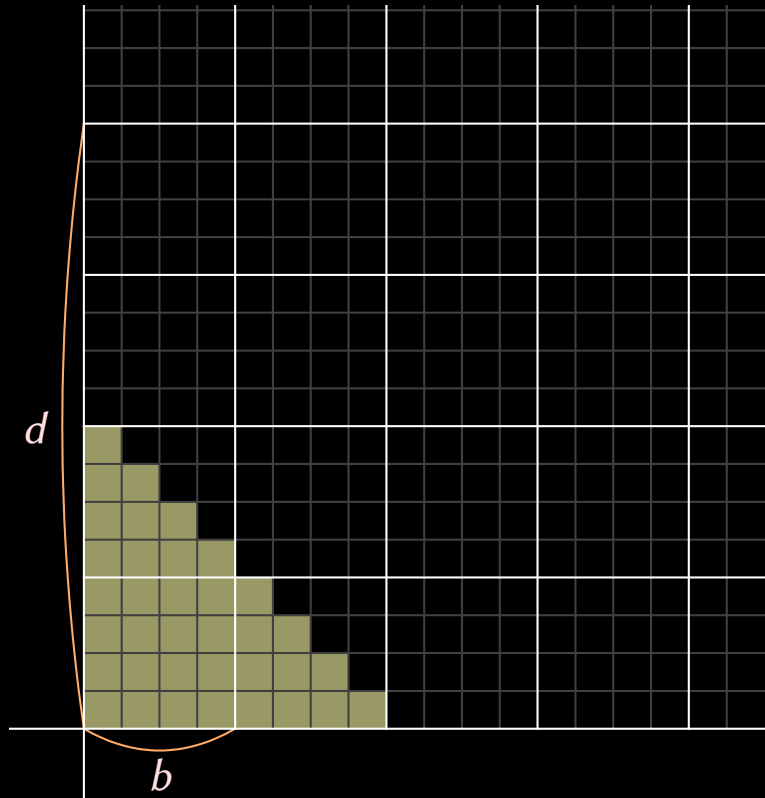


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

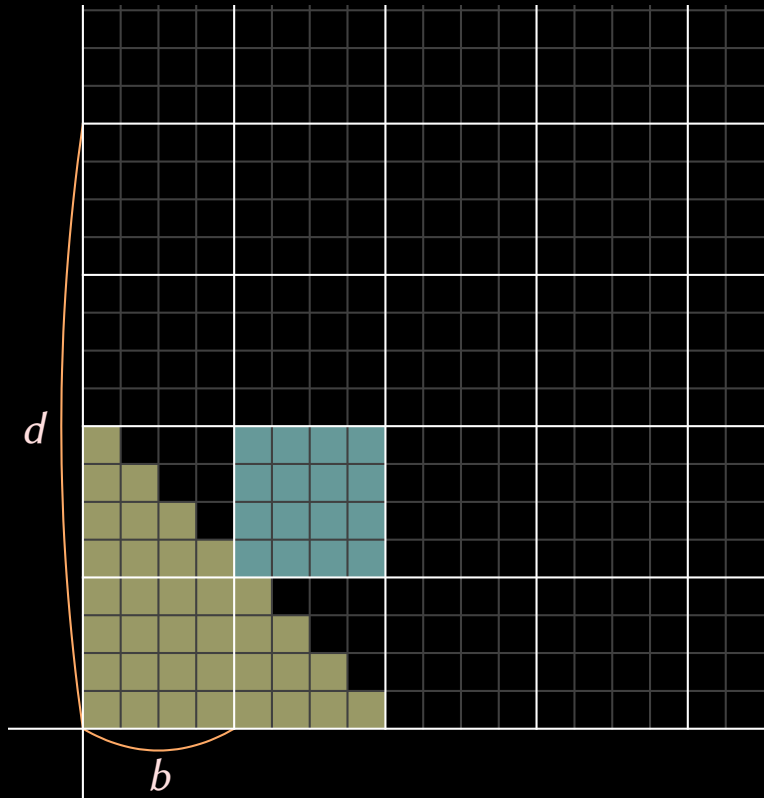


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$



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



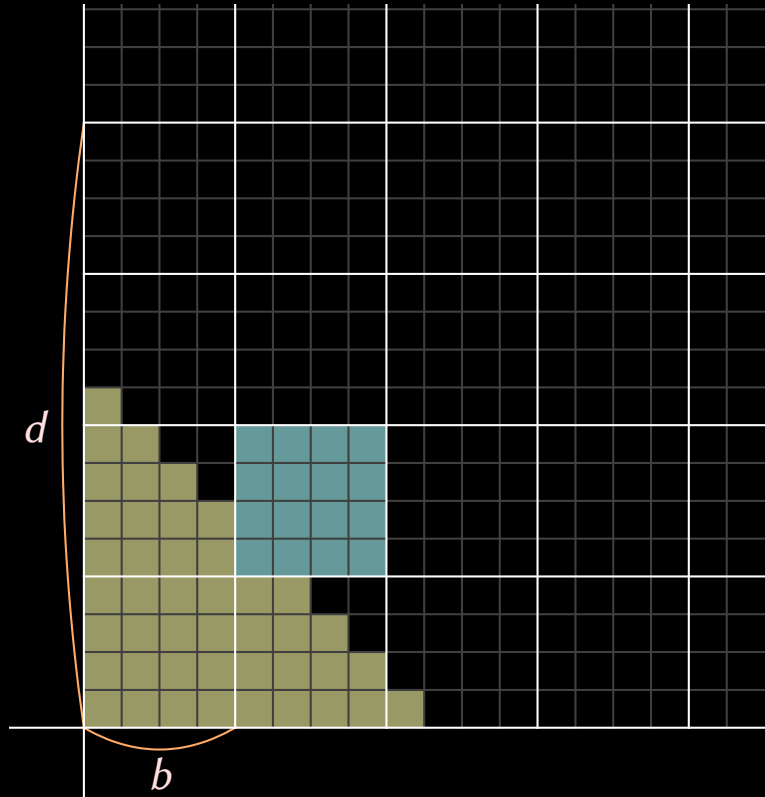
Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b

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

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

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

Multiplication détendue d'ordre $d = bl$

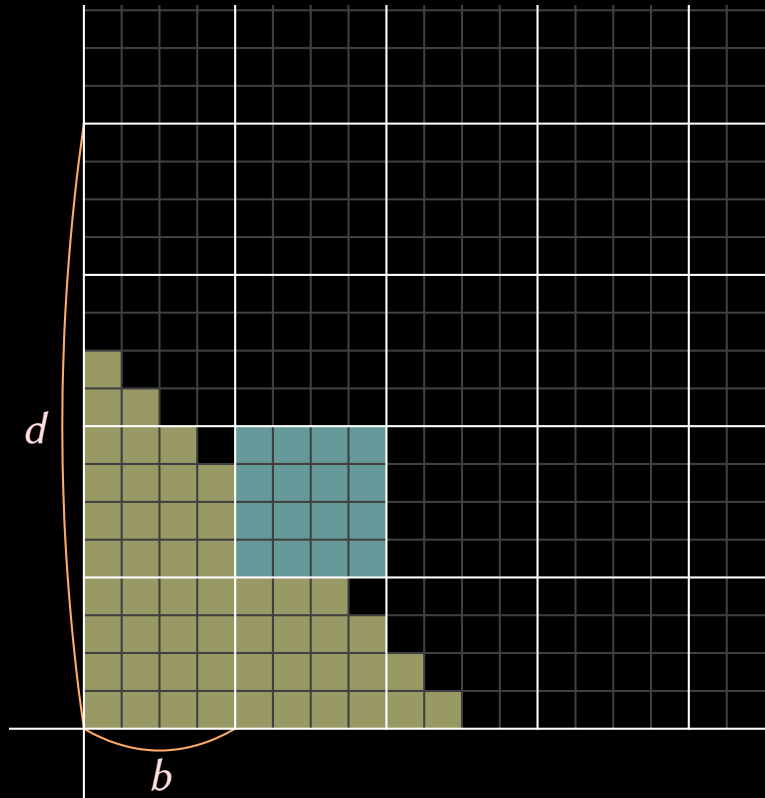


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

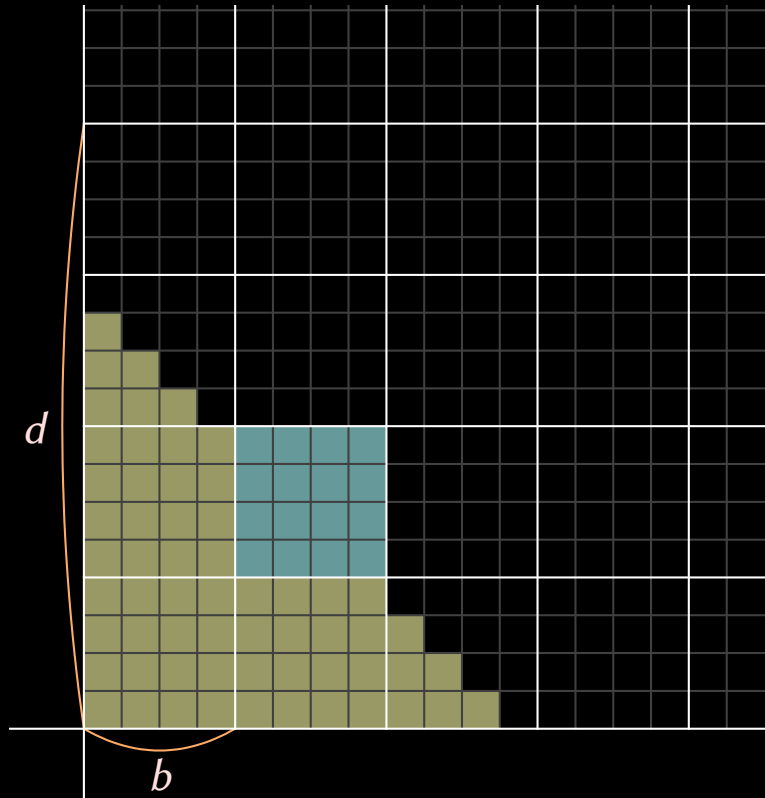


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$

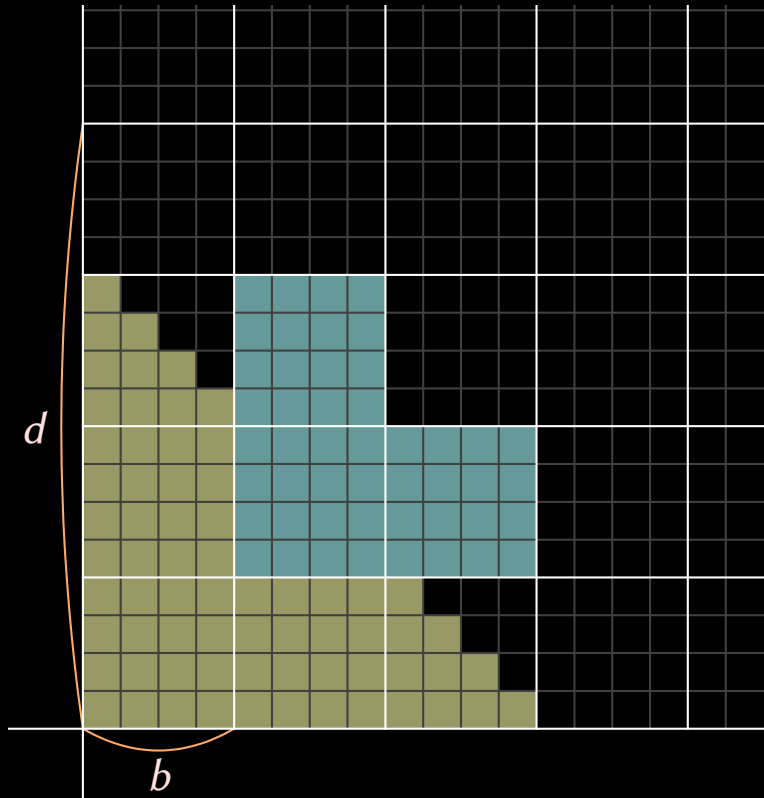


$$\omega^{2b} = 1 \quad R_{\mathbb{K}}(d) ?$$



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

Multiplication détendue d'ordre $d = bl$



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



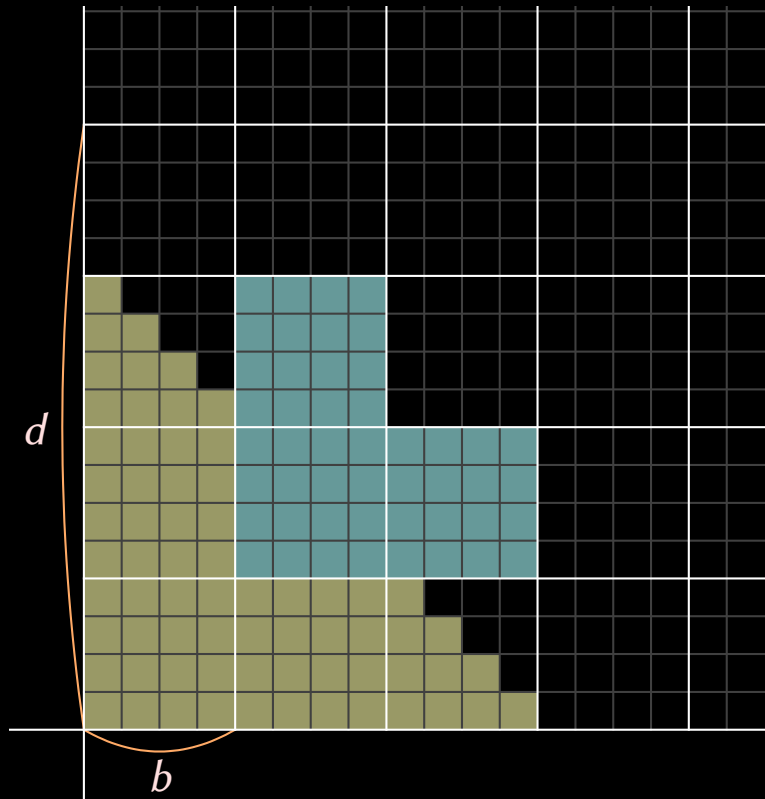
Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b

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

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

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

Multiplication détendue d'ordre $d = bl$



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

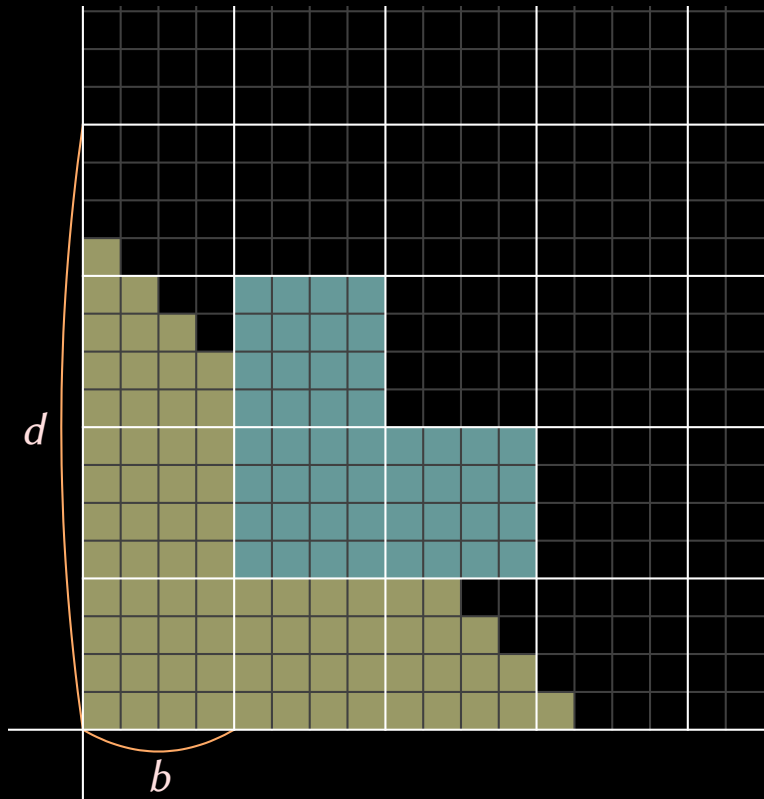


Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b



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

Multiplication détendue d'ordre $d = bl$



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

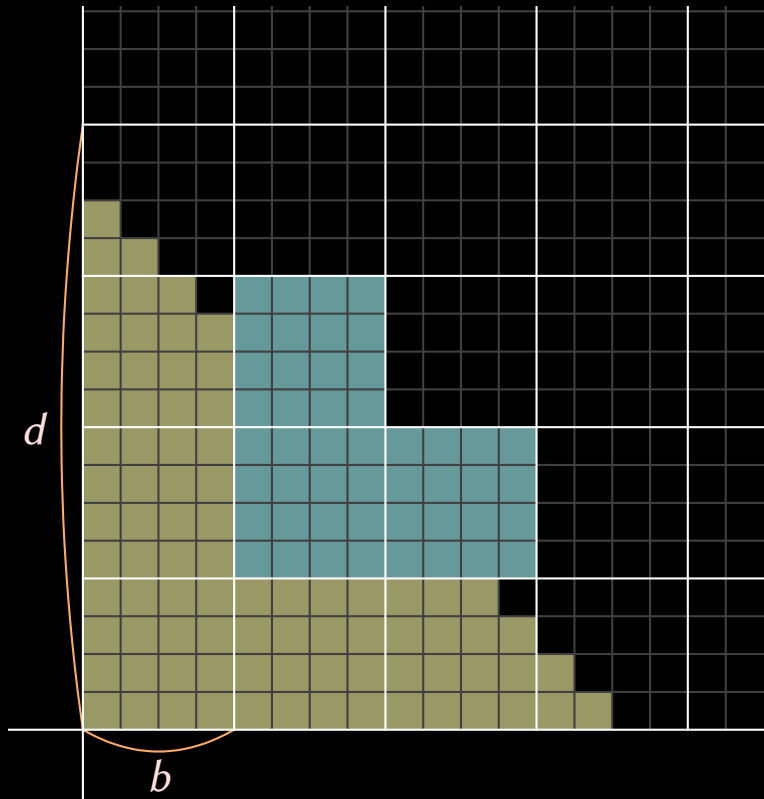


Produits détendues dans $\mathbb{K}[[z]]$ d'ordre b



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

Multiplication détendue d'ordre $d = bl$



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

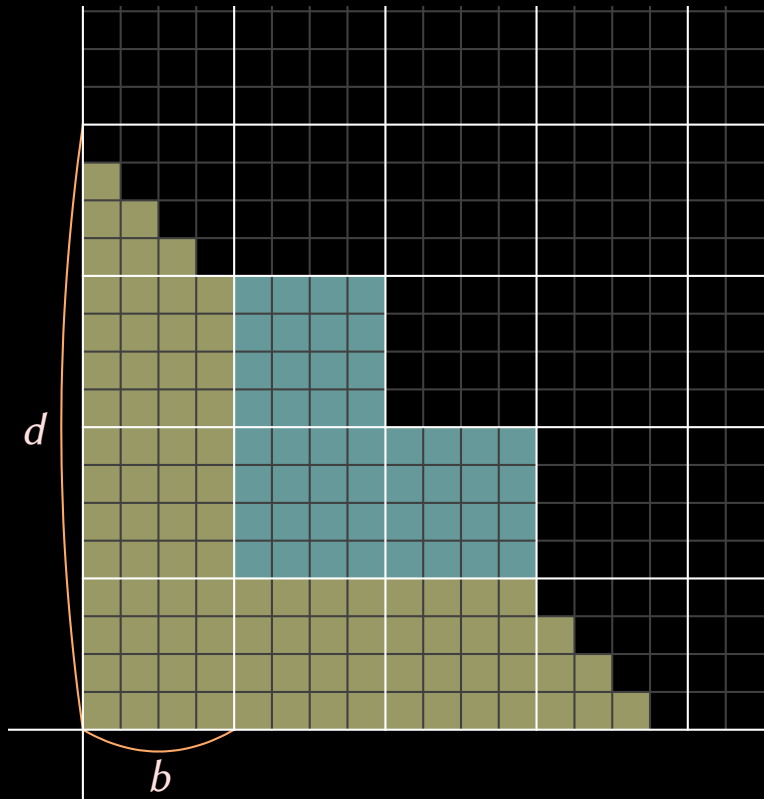


Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b



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

Multiplication détendue d'ordre $d = bl$



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

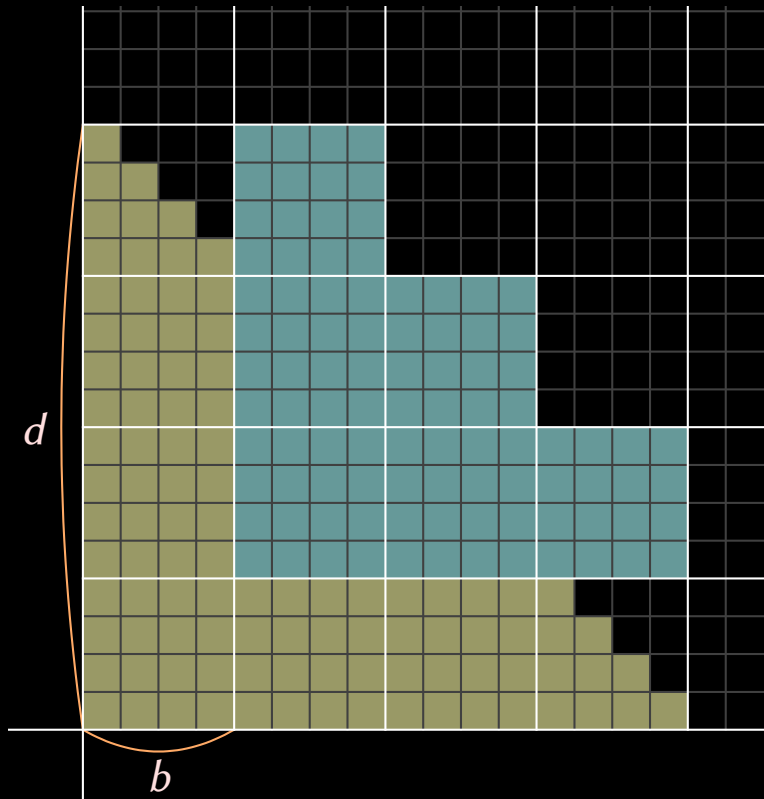


Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b



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

Multiplication détendue d'ordre $d = bl$



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

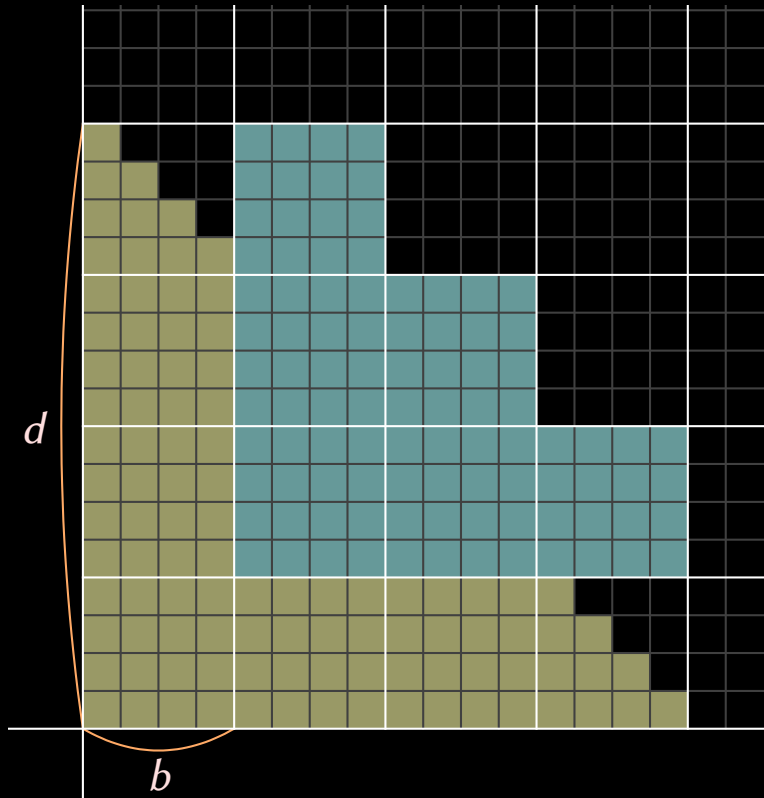


Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b



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

Multiplication détendue d'ordre $d = bl$



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



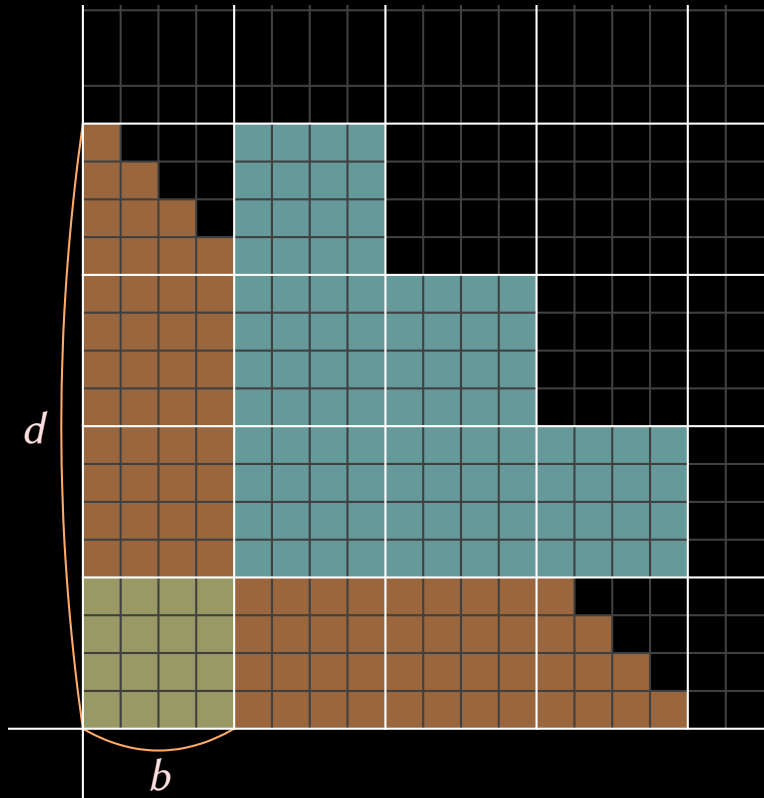
Produits détendus dans $\mathbb{K}[[z]]$ d'ordre b



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

$$R_{\mathbb{K}}(d) \leq (2l-1)R_{\mathbb{K}}(b) + 2bR_{\mathbb{K}}(l-1) + 6lF_{\mathbb{K}}(2b)$$

Multiplication détendue d'ordre $d = bl$



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



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



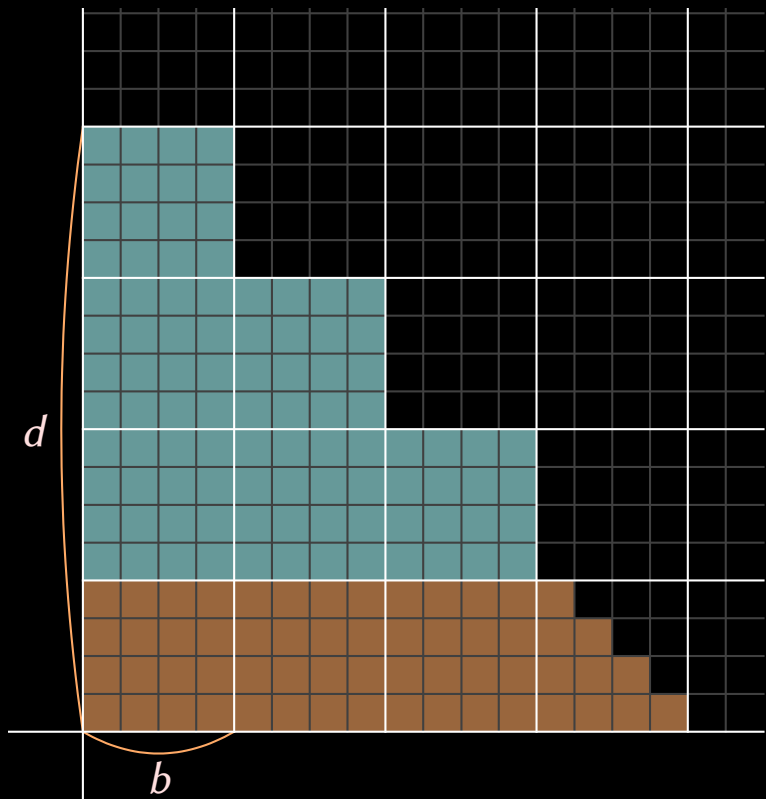
Produits semi-détendus d'ordre b



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

$$R_{\mathbb{K}}(d) \leq R_{\mathbb{K}}(b) + 2l R_{\mathbb{K}}^*(b) + 2b R_{\mathbb{K}}(l) + 6l F_{\mathbb{K}}(2b)$$

Multiplication détendue d'ordre $d = bl$



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



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



Produits semi-détendus d'ordre b

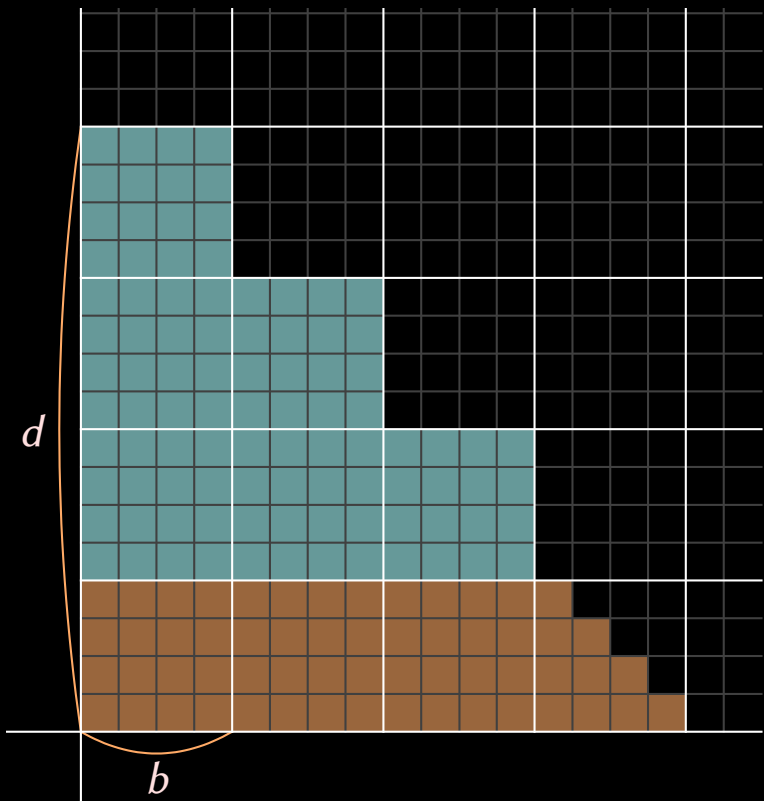


Produit détendu dans $\mathbb{K}^{2b}[[z]]$ d'ordre $l-1$

$$R_{\mathbb{K}}(d) \leq R_{\mathbb{K}}(b) + 2lR_{\mathbb{K}}^*(b) + 2bR_{\mathbb{K}}(l) + 6F_{\mathbb{K}}(2b)$$

$$R_{\mathbb{K}}^*(d) \leq lR_{\mathbb{K}}^*(b) + 2bR_{\mathbb{K}}^*(l) + 4F_{\mathbb{K}}(2b)$$

Multiplication détendue d'ordre $d = bl$



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

$$b \approx \exp \frac{\log d}{e^{\sqrt{2 \log 2 \log \log d}}}$$



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



Produits semi-détendus d'ordre b



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

$$R_{\mathbb{K}}(d) \leq R_{\mathbb{K}}(b) + 2l R_{\mathbb{K}}^*(b) + 2b R_{\mathbb{K}}(l) + 6 F_{\mathbb{K}}(2b)$$

$$R_{\mathbb{K}}^*(d) \leq l R_{\mathbb{K}}^*(b) + 2b R_{\mathbb{K}}^*(l) + 4 F_{\mathbb{K}}(2b)$$

$$R_{\mathbb{K}}(d) = O(R_{\mathbb{K}}^*(d)) = M_{\mathbb{K}}(d) e^{O(\sqrt{\log \log d})}$$

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

$$g' = f' g$$

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

$$g' = f' g$$

$$g = 1 + \int f' g$$

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

$$g' = f' g$$

$$g = 1 + \int f' g$$

$$g_k = \left(\int f' g \right)_k \quad (k > 0)$$

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

$$g' = f' g$$

$$g = 1 + \int f' g$$

$$g_k = \left(\int f' g \right)_k$$

$$= \frac{1}{k} (f' g)_{k-1} \quad (k > 0)$$

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

$$g' = f' g$$

$$g = 1 + \int f' g$$

$$g_k = \left(\int f' g \right)_k$$

$$= \frac{1}{k} (f' g)_{k-1}$$

$$= \frac{1}{k} (f_1 g_{k-1} + 2 f_2 g_{k-2} + \dots + k f_k g_0) \quad (k > 0)$$

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

$$g' = f' g$$

$$g = 1 + \int f' g$$

$$g_k = \left(\int f' g \right)_k$$

$$= \frac{1}{k} (f' g)_{k-1}$$

$$= \frac{1}{k} (f_1 g_{k-1} + 2 f_2 g_{k-2} + \dots + k f_k g_0) \quad (k > 0)$$

→ $E(d) \leq R(d) + O(d)$

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

$$g' = f' g$$

$$g = 1 + \int f' g$$

$$g_k = \left(\int f' g \right)_k$$

$$= \frac{1}{k} (f' g)_{k-1}$$

$$= \frac{1}{k} (f_1 g_{k-1} + 2 f_2 g_{k-2} + \dots + k f_k g_0) \quad (k > 0)$$

→ $E(d) \leq R(d) + O(d)$

→ Résolution d'une équation « récursive » : presque aussi vite que son évaluation


$$\mathbb{K}[x, \vartheta]$$

$$\vartheta = x \frac{\partial}{\partial x}$$

$$\partial_x = x \partial + 1$$

$$\partial(x^k) = k x^{k-1}$$

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

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

$$\begin{aligned}\partial x &= x \partial + x \\ \partial(x^k) &= k x^{k-1}\end{aligned}$$

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

Multiplication par évaluation-interpolation ?

$$\begin{aligned}\partial x &= x \partial + x \\ \partial(x^k) &= k x^{k-1}\end{aligned}$$

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

Multiplication par évaluation-interpolation ?

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

$$\begin{aligned}\partial x &= x \partial + x \\ \partial(x^k) &= kx^{k-1}\end{aligned}$$

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

Multiplication par évaluation-interpolation ?

$$\mathbb{K}[x]_n := \{P \in \mathbb{K}[x] : \deg P \leq n\}$$

$$L : \mathbb{K}[x]_n \rightarrow \mathbb{K}[x]_{n+d}$$

$$L \iff \text{Mat}_n^d(L) ? \quad n ?$$

$$\Lambda = \begin{pmatrix} L_{0,0} & \cdots & L_{0,r} \\ \vdots & & \vdots \\ L_{d,0} & \cdots & L_{d,r} \end{pmatrix}$$

$$\text{Mat}_n^d(L) = \begin{pmatrix} M_{0,0} & & & & \\ \vdots & \ddots & & & \\ M_{d,0} & & M_{0,n} & & \\ & \ddots & & \ddots & \\ & & & & M_{d,n} \end{pmatrix}$$

$$M = \Lambda \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1^r & 2^r & \cdots & n^r \end{pmatrix}$$

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

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

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

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

$\text{Mat}_n^d(L) \longrightarrow L$ en temps $O(dM(r)\log r)$ si $n \geq r$

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

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

$\text{Mat}_n^d(L) \longrightarrow L$ en temps $O(dM(r)\log r)$ si $n \geq r$

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

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

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

$\text{Mat}_n^d(L) \longrightarrow L$ en temps $O(dM(r)\log r)$ si $n \geq r$

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

$$SM_{\mathbb{K},\vartheta}(d,r) = O(\Omega(r)^{d/r} + dM(r)\log r)$$

si $r \geq d$

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

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

$\text{Mat}_n^d(L) \longrightarrow L$ en temps $O(dM(r)\log r)$ si $n \geq r$

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

$$SM_{\mathbb{K},\vartheta}(d,r) = O(\Omega(r)^{d/r} + dM(r)\log r) \quad \text{si } r \geq d$$

$$\Omega_{\mathbb{K}}(r) = O(SM_{\mathbb{K},\vartheta}(r,r) + rM(r)\log r) \quad \text{si } d = r$$

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

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

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

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

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

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

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

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

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

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

$$\mathbb{K}$$

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

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

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

$$\vdots$$

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

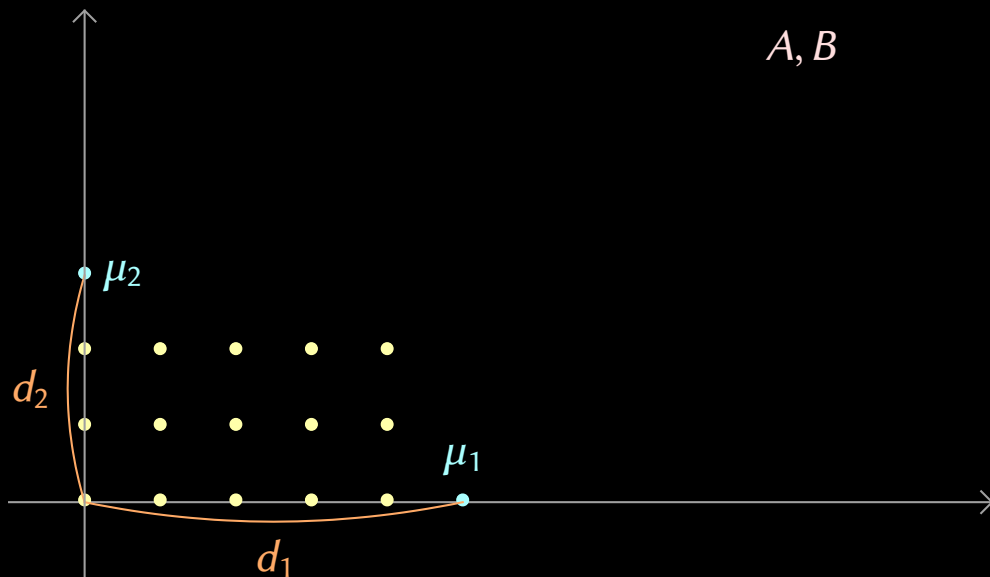
$$\mathbb{K}_2 := \mathbb{K}_1[\alpha_2]$$

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

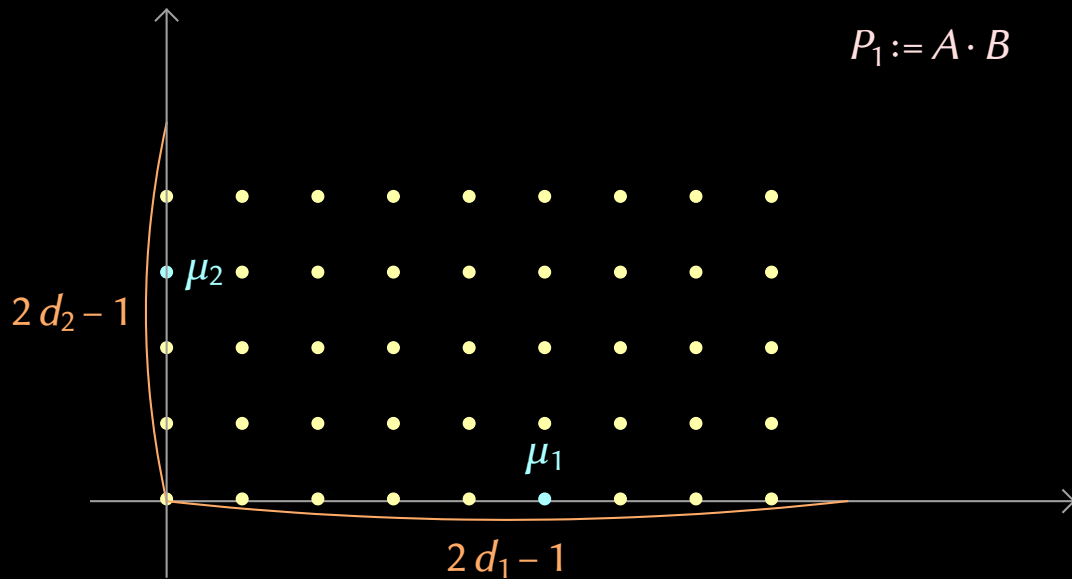
$$\mathbb{K}_0 := \mathbb{K}$$

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

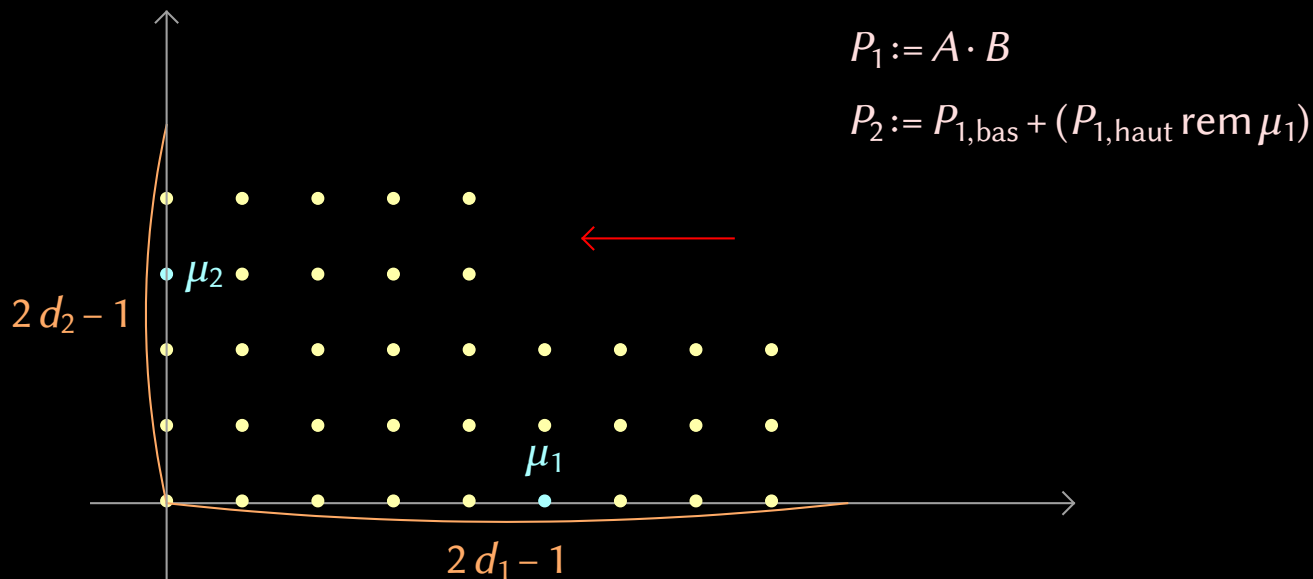
$$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2]/(\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2)), \quad d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0], \quad d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$$



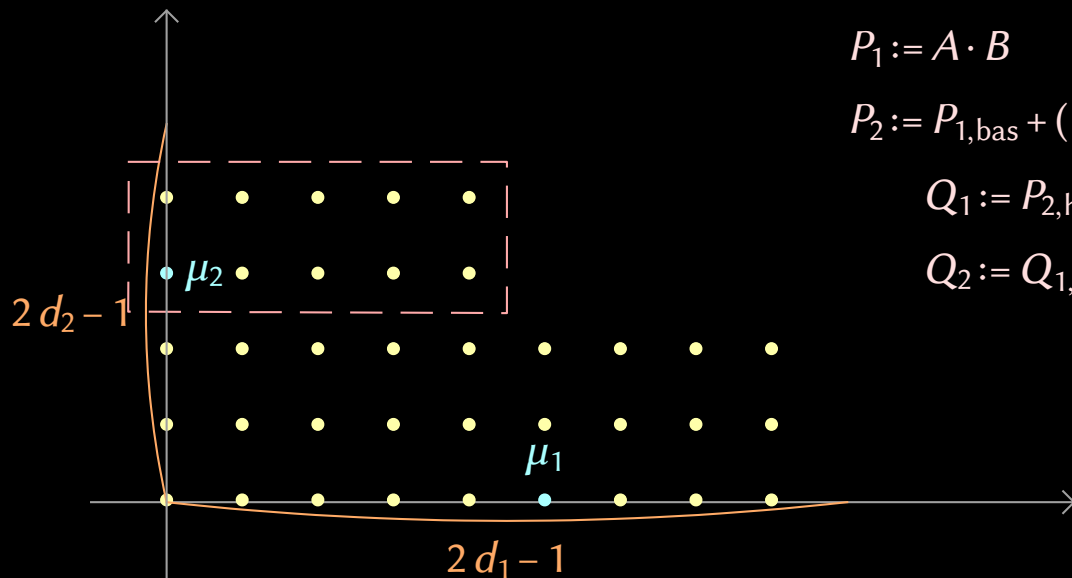
$$\mathbb{L} = \mathbb{K}[\alpha_1, \alpha_2] / (\mu_1(\alpha_1), \mu_2(\alpha_1, \alpha_2)), \quad d_1 := \deg_{\alpha_1} \mu_1 = [\mathbb{K}_1 : \mathbb{K}_0], \quad d_2 := \deg_{\alpha_2} \mu_2 = [\mathbb{K}_2 : \mathbb{K}_1]$$



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



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



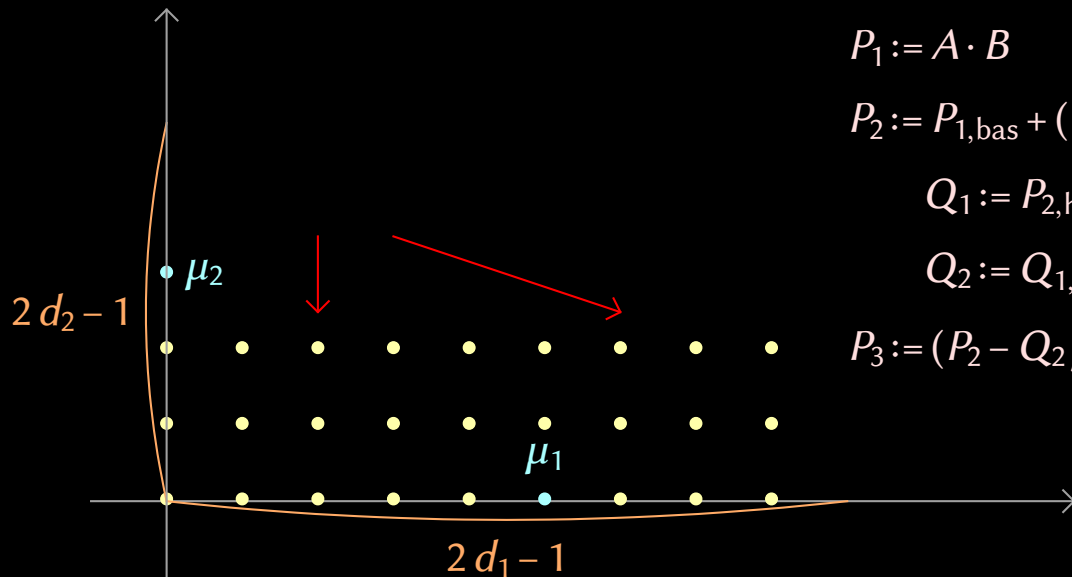
$$P_1 := A \cdot B$$

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

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

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

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



$$P_1 := A \cdot B$$

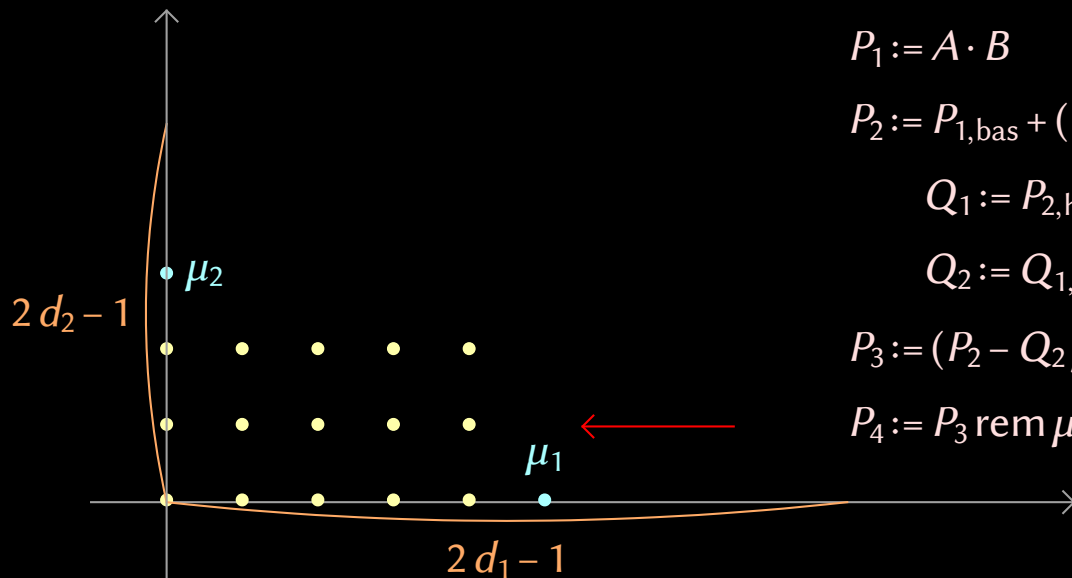
$$P_2 := P_{1,\text{bas}} + (P_{1,\text{haut}} \text{ rem } \mu_1)$$

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

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

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

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



$$P_1 := A \cdot B$$

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

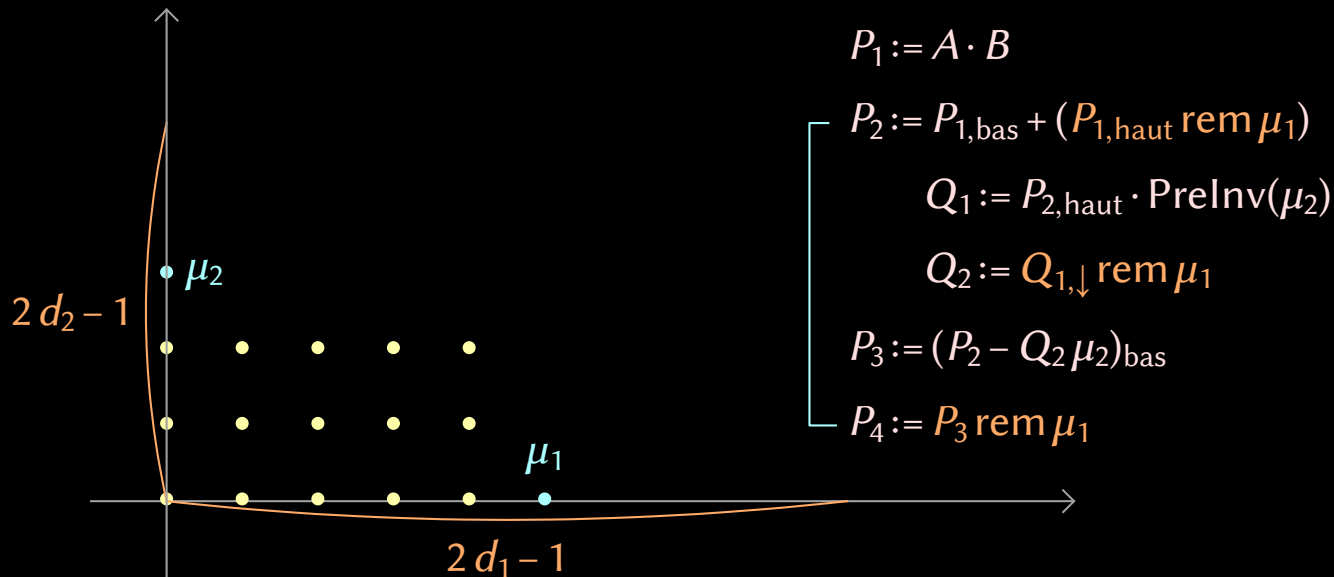
$$Q_1 := P_{2,\text{haut}} \cdot \text{PreInv}(\mu_2)$$

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

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

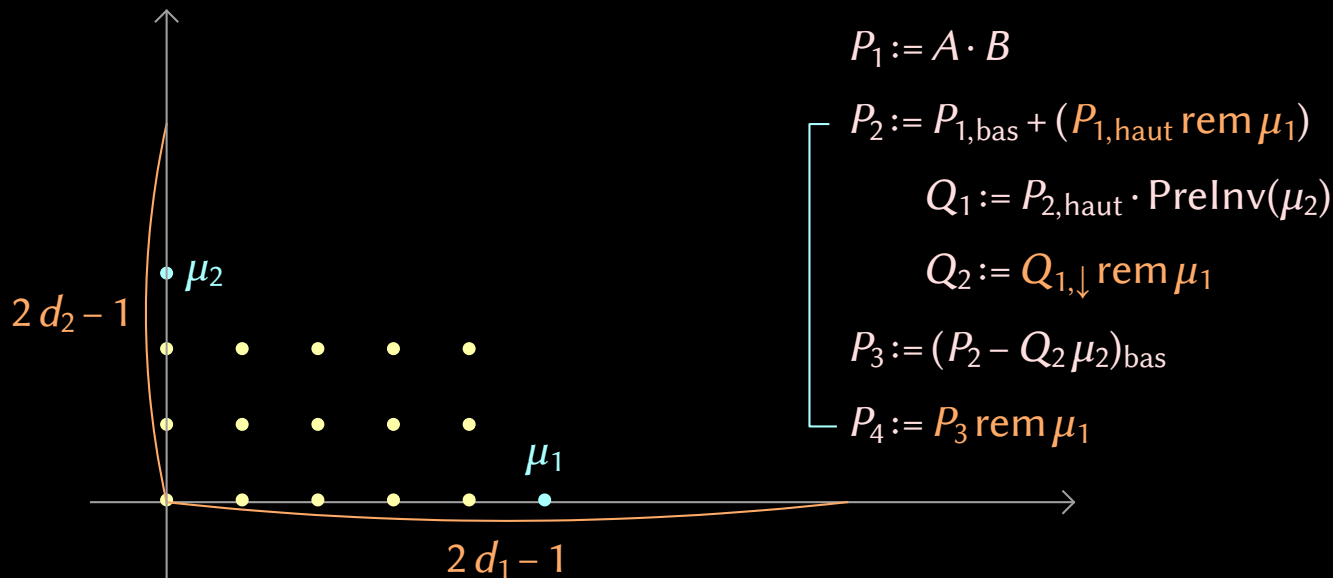
$$P_4 := P_3 \text{ rem } \mu_1$$

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



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

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



$$m_{\mathbb{L}} := M_{\mathbb{L}}(1) = O(M_{\mathbb{K}}(3^t d))$$

$$d = [\mathbb{L} : \mathbb{K}]$$

Cas le plus défavorable

$$d_1 = \cdots = d_t = 2 \implies m_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Cas le plus défavorable

$$d_1 = \cdots = d_t = 2 \implies m_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Éléments primitif β

$$\mathbb{L} \cong \mathbb{K}[\beta]$$

$$m_{\mathbb{K}[\beta]} = O(M_{\mathbb{K}}(d))$$

Cas le plus défavorable

$$d_1 = \dots = d_t = 2 \implies m_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Éléments primitif β

$$\mathbb{L} \cong \mathbb{K}[\beta]$$

$$m_{\mathbb{K}[\beta]} = O(M_{\mathbb{K}}(d))$$

Problèmes

Il faut pré-calculer l'élément primitif

Cas le plus défavorable

$$d_1 = \dots = d_t = 2 \implies m_{\mathbb{L}} = O(M_{\mathbb{K}}(6^t)) = O(M_{\mathbb{K}}(d^{2,585}))$$

Éléments primitif β

$$\mathbb{L} \cong \mathbb{K}[\beta]$$

$$m_{\mathbb{K}[\beta]} = O(M_{\mathbb{K}}(d))$$

Problèmes

Il faut pré-calculer l'élément primitif

Coût des conversions $\mathbb{L} \iff \mathbb{K}[\beta]$ en $O(m_{\mathbb{K}} d^{\omega})$ où $\frac{3}{2} < \omega \leq 2$

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

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

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

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

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

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

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

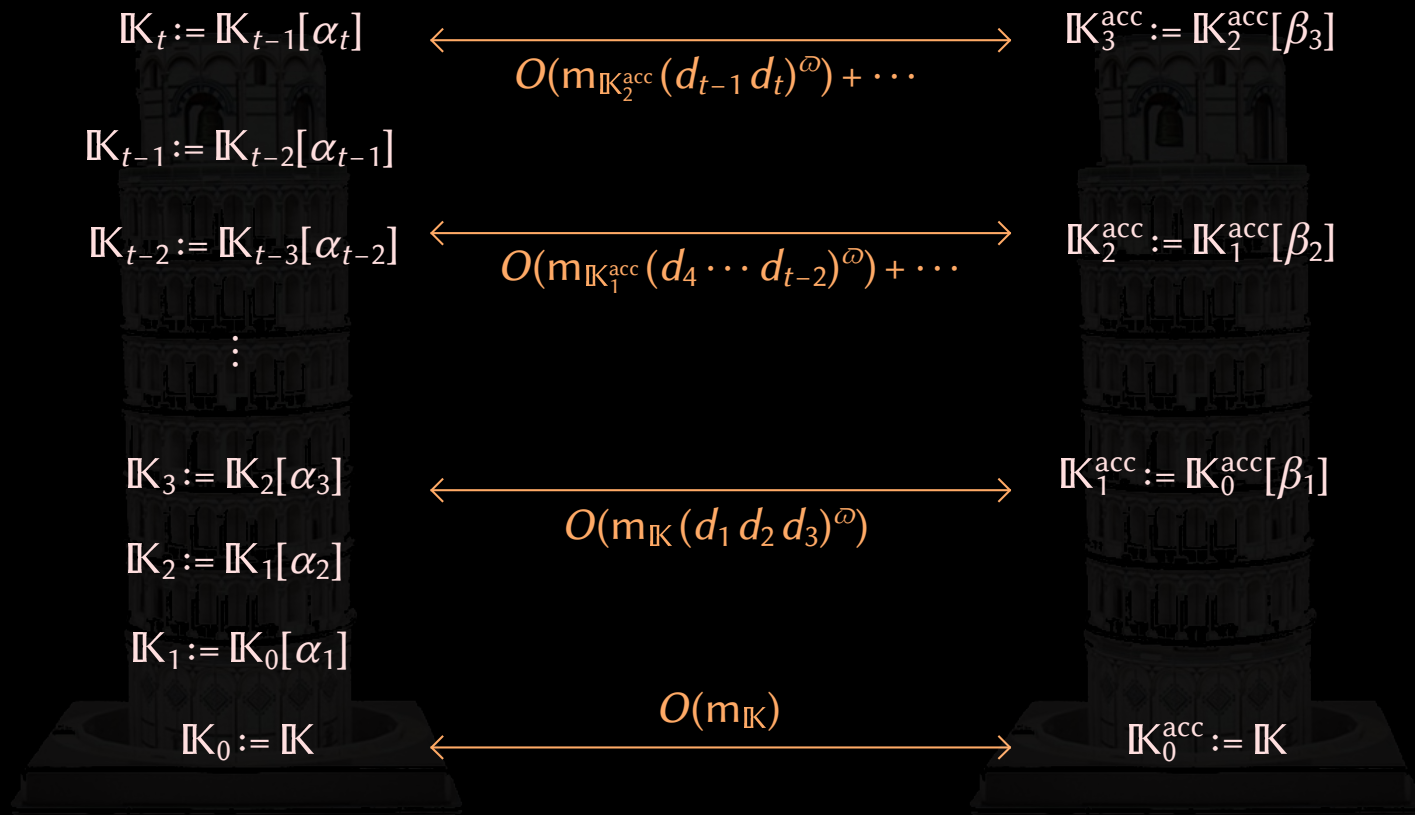
$$\mathbb{K}[\sqrt{2}]$$

$$\mathbb{K}$$

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

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

$$\mathbb{K}$$



Tours accélérés

$$m_{\mathbb{L}} = M_{\mathbb{K}}(d) e^{O(\sqrt{\log d})}$$

Tours accélérés

$$m_{\mathbb{L}} = M_{\mathbb{K}}(d) e^{O(\sqrt{\log d})}$$

Généralisation

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

Tours accélérés

$$m_{\mathbb{L}} = M_{\mathbb{K}}(d) e^{O(\sqrt{\log d})}$$

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

$$m_{\mathbb{L}} = M_{\mathbb{K}}(d) e^{O(\sqrt{\log d})}$$

Généralisation

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

Évaluation dirigée

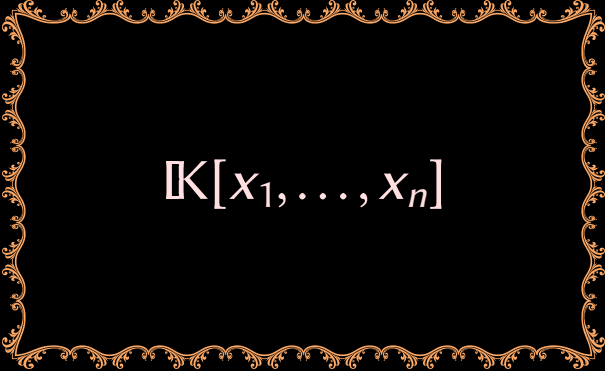
Séparer le calcul en deux branches en cas de division par zéro

- 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 $d = r^{O(1)}$



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

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

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

$$f = ab$$

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

$$f = ab$$

$$f(\mathbf{x}) = c_1 \mathbf{x}^{e_1} + \dots + c_s \mathbf{x}^{e_s}$$

$$(\mathbf{x}^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

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

$$f = ab$$

$$f(\mathbf{x}) = c_1 \mathbf{x}^{e_1} + \dots + c_s \mathbf{x}^{e_s}$$

$$(\mathbf{x}^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer s, e_1, \dots, e_s

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

$$f = ab$$

$$f(\mathbf{x}) = c_1 \mathbf{x}^{e_1} + \dots + c_s \mathbf{x}^{e_s}$$

$$(\mathbf{x}^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer s, e_1, \dots, e_s

Étape 2 : déterminer c_1, \dots, c_s

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

$$f = ab$$

$$f(\mathbf{x}) = c_1 \mathbf{x}^{e_1} + \dots + c_s \mathbf{x}^{e_s}$$

$$(\mathbf{x}^\epsilon = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})$$

Étape 1 : déterminer s, e_1, \dots, e_s

Étape 2 : déterminer c_1, \dots, 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, \dots, c_s « gros », et e_1, \dots, e_s déterminés pour $f \bmod p$

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

$$f = ab$$

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

Étape 1 : déterminer s, e_1, \dots, e_s

Étape 2 : déterminer c_1, \dots, 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, \dots, c_s « gros », et e_1, \dots, e_s déterminés pour $f \bmod p$

→ nous allons nous focaliser sur l'Étape 2

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

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

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

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

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

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

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

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

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

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

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

Multiplication par inverse Vandermonde = transposé de l'interpolation polynomiale

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

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

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

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

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

Multiplication par inverse Vandermonde = transposé de l'interpolation polynomiale

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

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

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

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

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

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

Multiplication par inverse Vandermonde = transposé de l'interpolation polynomiale

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

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

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

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

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

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

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

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

- Évaluation de a et de b en $t^\lambda := (t^{\lambda_1}, \dots, t^{\lambda_n})$ 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 : $(t^\lambda)^{e_i} = (t^\lambda)^{e_j} \iff t^{\lambda \cdot e_i} = t^{\lambda \cdot e_j} \iff (\lambda \cdot e_i = \lambda \cdot e_j \text{ modulo } r)$

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

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

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

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

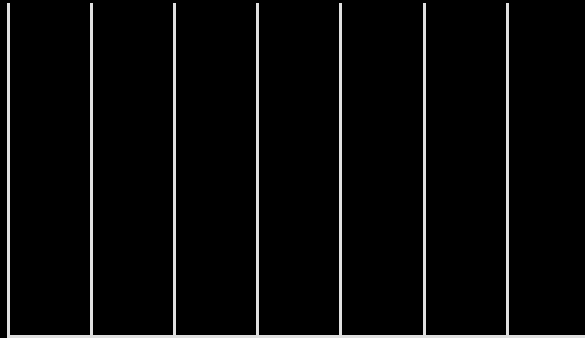
Note : $(t^\lambda)^{e_i} = (t^\lambda)^{e_j} \iff t^{\lambda \cdot e_i} = t^{\lambda \cdot e_j} \iff (\lambda \cdot e_i = \lambda \cdot e_j \text{ modulo } r)$

Modèle (ou hypothèse heuristique)

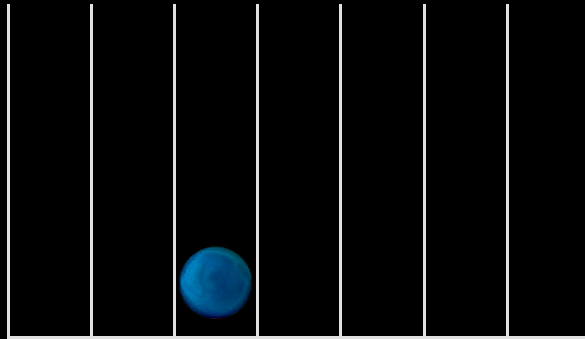
Pour $\lambda_1, \dots, \lambda_n$ aléatoires :

$\lambda \cdot e_1, \dots, \lambda \cdot e_s \text{ modulo } r \iff$ tirage aléatoire de s entiers modulo r

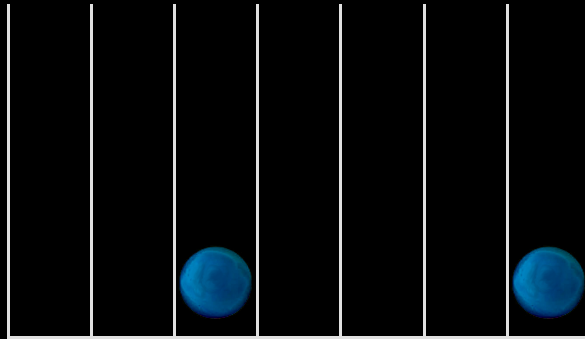
s boules dans $r = \tau s$ tiroirs



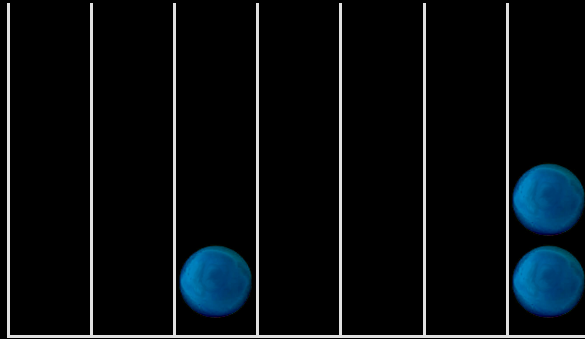
s boules dans $r = \tau s$ tiroirs



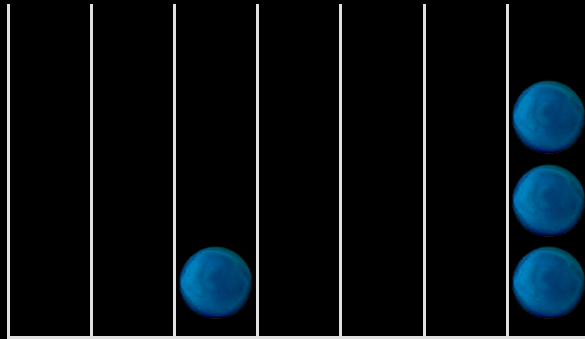
s boules dans $r = \tau s$ tiroirs



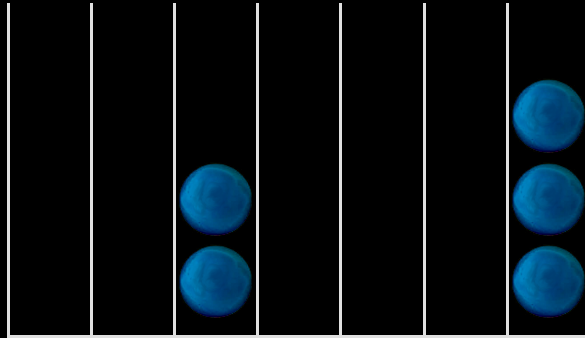
s boules dans $r = \tau s$ tiroirs



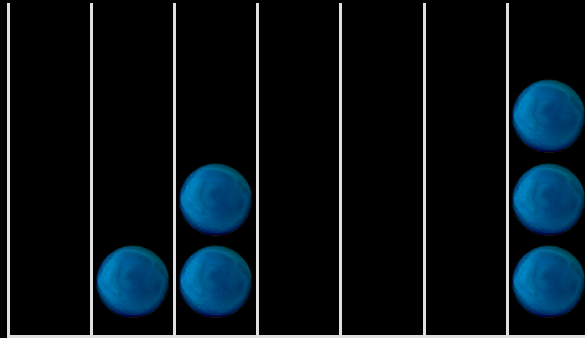
s boules dans $r = \tau s$ tiroirs



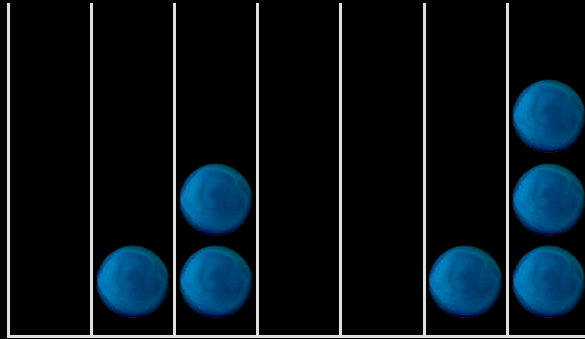
s boules dans $r = \tau s$ tiroirs



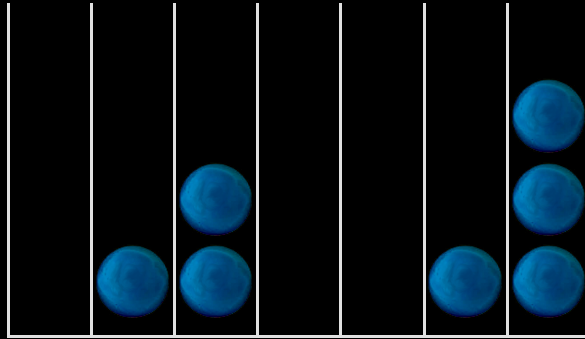
s boules dans $r = \tau s$ tiroirs



s boules dans $r = \tau s$ tiroirs

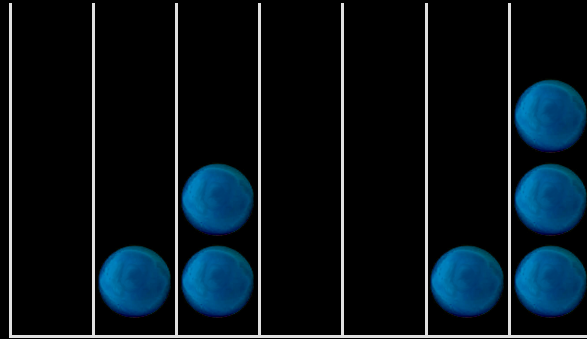


s boules dans $r = \tau s$ tiroirs



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

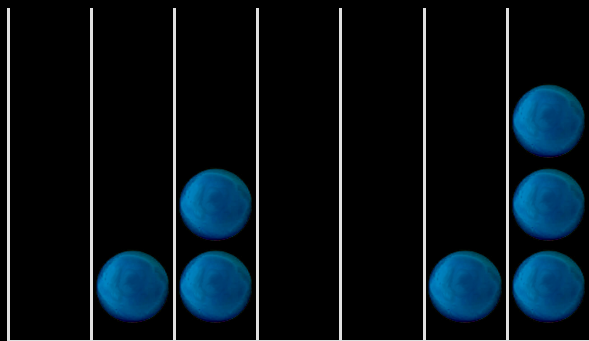
s boules dans $r = \tau s$ tiroirs



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

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

s boules dans $r = \tau s$ tiroirs



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

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

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

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

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

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

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

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

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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 $t^r - 1$

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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 $\sigma = s$

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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 $e^{-\frac{1}{\tau}}(s - \sigma)$ termes

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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 $e^{-\frac{1}{\tau}}(s - \sigma)$ termes

Complexité : $\sim \tau (M_{\mathbb{K}}^{\circ}(s) + M_{\mathbb{K}}^{\circ}((1 - e^{-\frac{1}{\tau}})s) + M_{\mathbb{K}}^{\circ}((1 - e^{-\frac{1}{\tau}})^2 s) + \dots) + O(s \log s)$

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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 $e^{-\frac{1}{\tau}}(s - \sigma)$ termes

Complexité : $\sim \tau e^{\frac{1}{\tau}} M_{\mathbb{K}}^{\circ}(s) + O(s \log s)$

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

- En entrée : a , b et $\tilde{f} = \sum_{i \leq \sigma} c_i x^{e_i}$ 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 $e^{-\frac{1}{\tau}}(s - \sigma)$ termes

Complexité : $\sim \tau e^{\frac{1}{\tau}} M_{\mathbb{K}}^{\circ}(s) + O(s \log s)$

$$M_{\mathbb{K}}^{\text{sparse}}(s) \leq_{\text{heuristique}} (e + o(1)) M_{\mathbb{K}}^{\circ}(s) + O(s \log s)$$

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

$$b = 2 + yz + 3x^2y^4z^3$$

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

Jeux des boules mystères

27/30

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

1 t t^2 t^3 t^4

--	--	--	--	--

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

1 t t^2 t^3 t^4

--	--	--	--	--

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

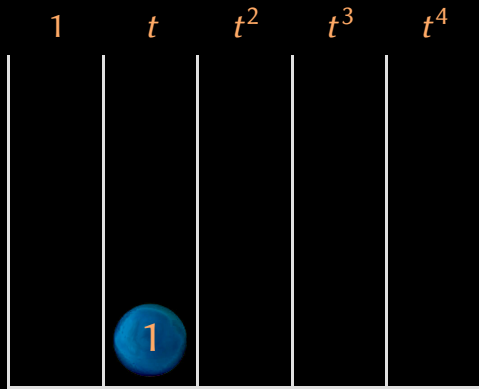
1 t t^2 t^3 t^4

--	--	--	--	--

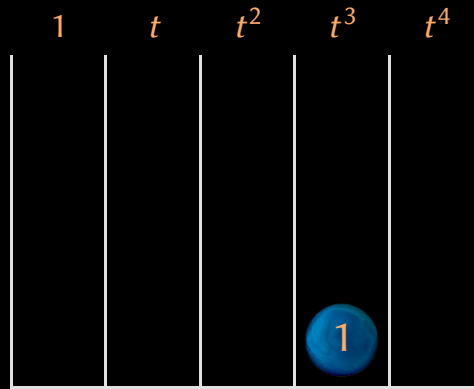
$$f = \overbrace{3x^{12}y^{18}z^6}^1 + \overbrace{1x^{10}y^{15}z^4}^2 + \overbrace{9x^3y^{10}z^4}^3 + \overbrace{3x^3y^9z^3}^4 + \overbrace{(-4)x^{10}y^{14}z^3}^5 +$$
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

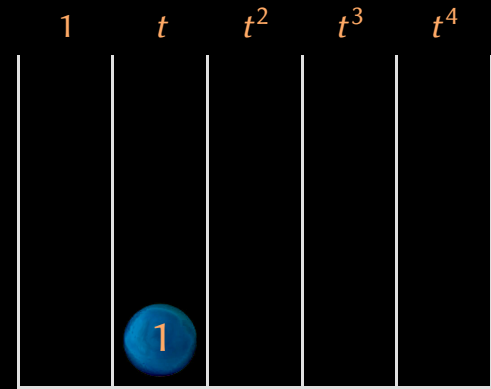
$$(x, y, z) = (t, t, t)$$



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



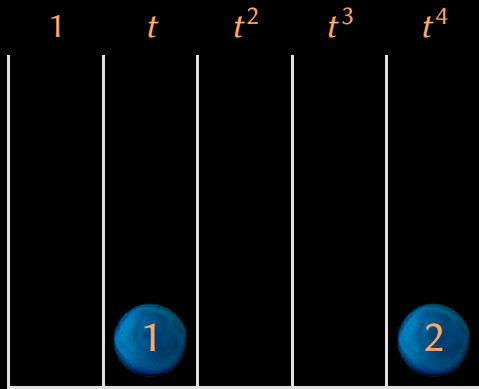
$$(x, y, z) = (1, 1, t)$$



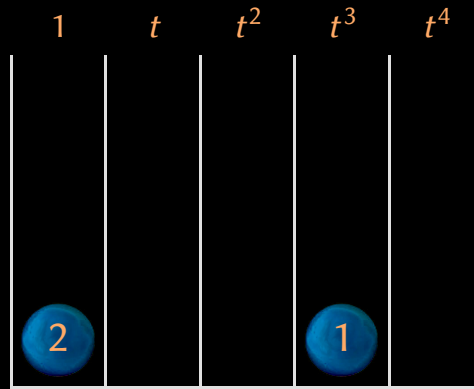
$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 & + 1x^{10}y^{15}z^4 & + 9x^3y^{10}z^4 & + 3x^3y^9z^3 & + (-4)x^{10}y^{14}z^3 + \\
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 & + 7xy^6z & + (-2)x^8y^{11}z & + 2xy^5 & + (-4)x^8y^{10}
 \end{array}
 \end{array}$$

Jeux des boules mystères

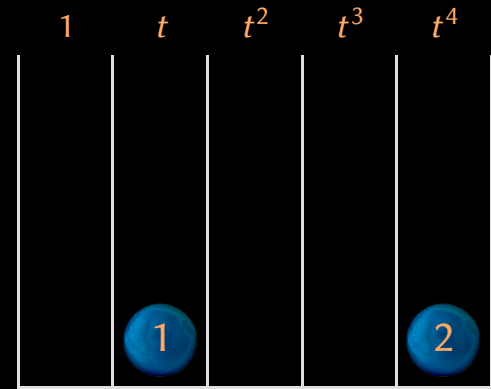
$$(x, y, z) = (t, t, t)$$



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



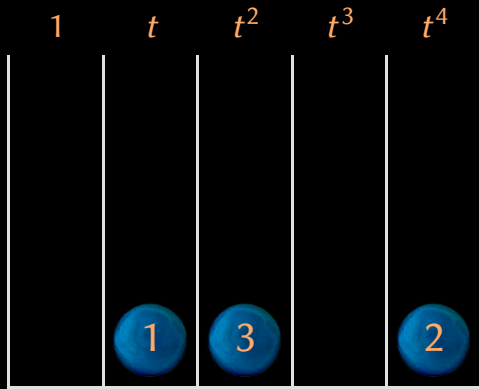
$$(x, y, z) = (1, 1, t)$$



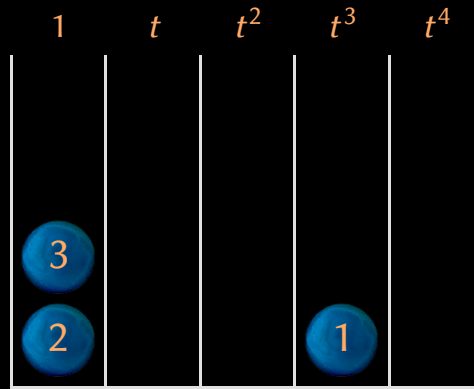
$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 & + 1x^{10}y^{15}z^4 & + 9x^3y^{10}z^4 & + 3x^3y^9z^3 & + (-4)x^{10}y^{14}z^3 + \\
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 & + 7xy^6z & + (-2)x^8y^{11}z & + 2xy^5 & + (-4)x^8y^{10}
 \end{array} \\
 f =
 \end{array}$$

Jeux des boules mystères

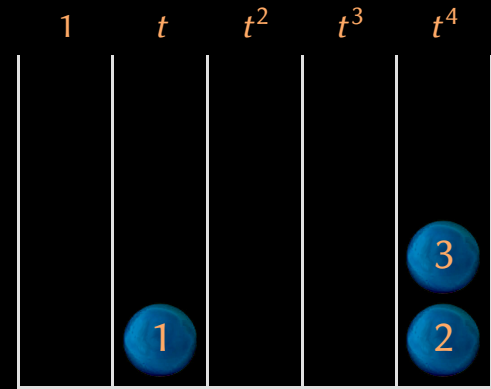
$$(x, y, z) = (t, t, t)$$



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



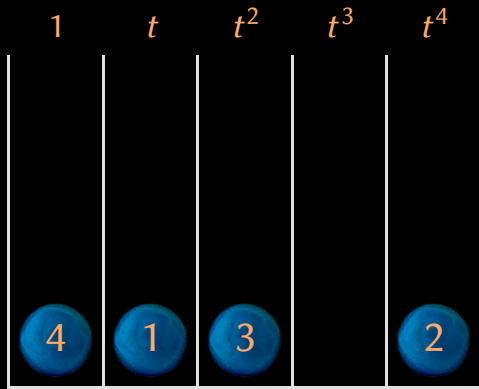
$$(x, y, z) = (1, 1, t)$$



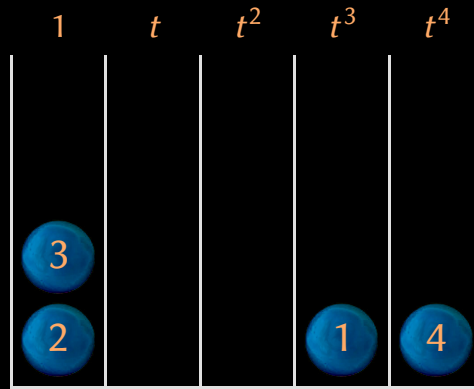
$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 & + 1x^{10}y^{15}z^4 & + 9x^3y^{10}z^4 & + 3x^3y^9z^3 & + (-4)x^{10}y^{14}z^3 + \\
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 & + 7xy^6z & + (-2)x^8y^{11}z & + 2xy^5 & + (-4)x^8y^{10}
 \end{array}
 \end{array}$$

Jeux des boules mystères

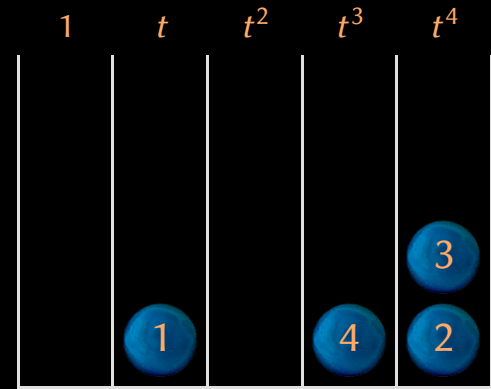
$$(x, y, z) = (t, t, t)$$



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



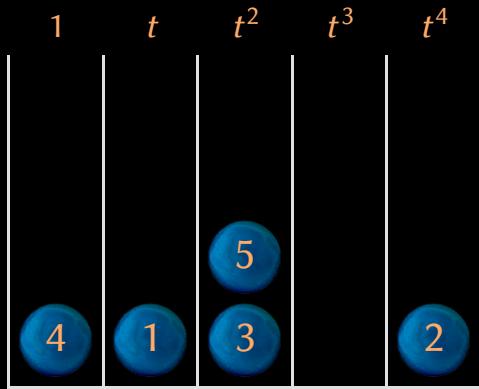
$$(x, y, z) = (1, 1, t)$$



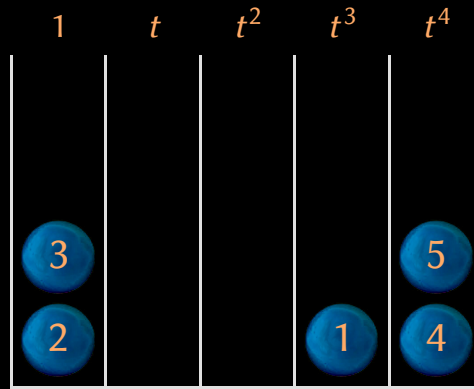
$$\begin{array}{c}
 \text{1} \quad \text{2} \quad \text{3} \quad \text{4} \quad \text{5} \\
 \overbrace{3x^{12}y^{18}z^6} + \overbrace{1x^{10}y^{15}z^4} + \overbrace{9x^3y^{10}z^4} + \overbrace{3x^3y^9z^3} + \overbrace{(-4)x^{10}y^{14}z^3} + \\
 \text{6} \quad \text{7} \quad \text{8} \quad \text{9} \quad \text{10} \\
 \overbrace{3xy^7z^2} + \overbrace{7xy^6z} + \overbrace{(-2)x^8y^{11}z} + \overbrace{2xy^5} + \overbrace{(-4)x^8y^{10}}
 \end{array}$$

Jeux des boules mystères

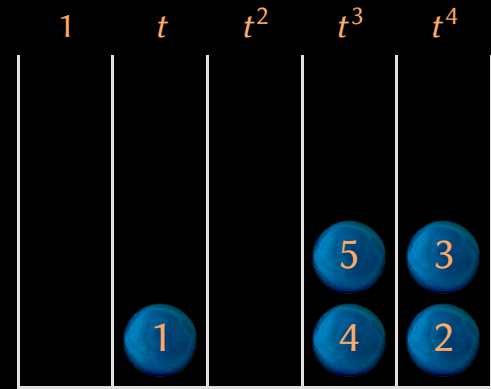
$$(x, y, z) = (t, t, t)$$



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



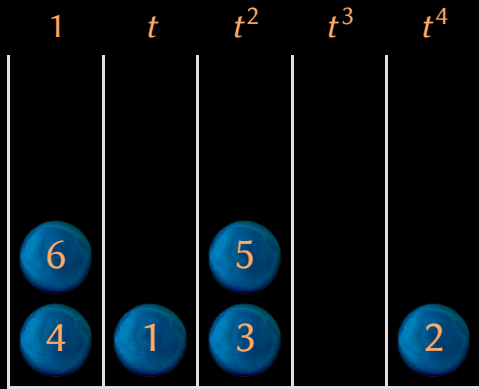
$$(x, y, z) = (1, 1, t)$$



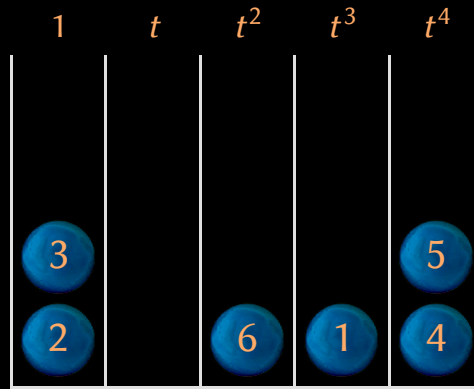
$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 + 1x^{10}y^{15}z^4 + 9x^3y^{10}z^4 + 3x^3y^9z^3 + (-4)x^{10}y^{14}z^3 + \\
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 + 7xy^6z + (-2)x^8y^{11}z + 2xy^5 + (-4)x^8y^{10}
 \end{array}
 \end{array}$$

Jeux des boules mystères

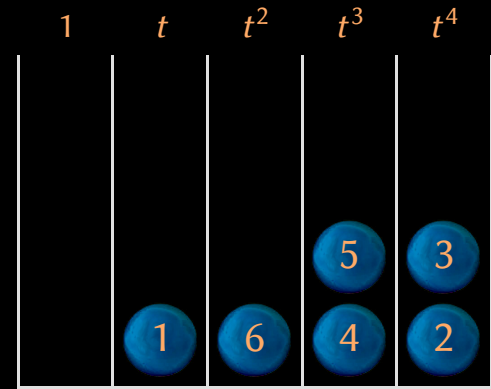
$$(x, y, z) = (t, t, t)$$



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



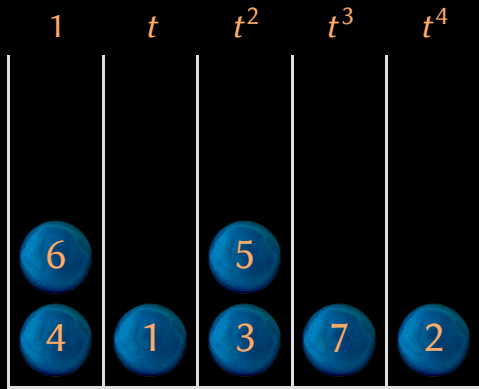
$$(x, y, z) = (1, 1, t)$$



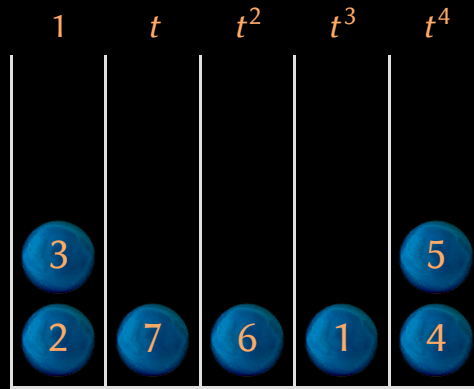
$$\begin{array}{c}
 \textcircled{1} \quad \textcircled{2} \quad \textcircled{3} \quad \textcircled{4} \quad \textcircled{5} \\
 f = \overbrace{3x^{12}y^{18}z^6} + \overbrace{1x^{10}y^{15}z^4} + \overbrace{9x^3y^{10}z^4} + \overbrace{3x^3y^9z^3} + \overbrace{(-4)x^{10}y^{14}z^3} + \\
 \textcircled{6}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

Jeux des boules mystères

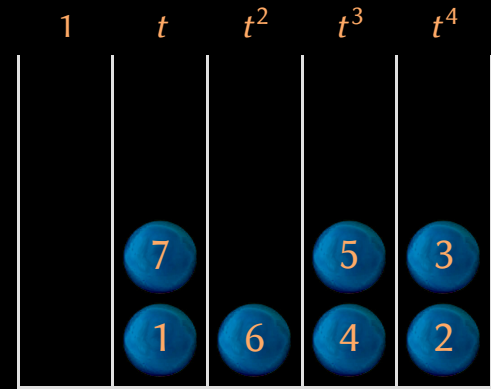
$$(x, y, z) = (t, t, t)$$



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



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



$$\begin{array}{c}
 \text{1} \qquad \text{2} \qquad \text{3} \qquad \text{4} \qquad \text{5} \\
 \overbrace{3x^{12}y^{18}z^6} + \overbrace{1x^{10}y^{15}z^4} + \overbrace{9x^3y^{10}z^4} + \overbrace{3x^3y^9z^3} + \overbrace{(-4)x^{10}y^{14}z^3} + \\
 \text{6} \qquad \text{7} \qquad \text{8} \qquad \text{9} \qquad \text{10} \\
 \overbrace{3xy^7z^2} + \overbrace{7xy^6z} + \overbrace{(-2)x^8y^{11}z} + \overbrace{2xy^5} + \overbrace{(-4)x^8y^{10}}
 \end{array}$$

Jeux des boules mystères

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

1	t	t^2	t^3	t^4
8				
6		5		
4	1	3	7	2

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

1	t	t^2	t^3	t^4
3	8			5
2	7	6	1	4

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

1	t	t^2	t^3	t^4
	8		5	3
	7		4	2
	1	6		

$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 & + 1x^{10}y^{15}z^4 & + 9x^3y^{10}z^4 & + 3x^3y^9z^3 & + (-4)x^{10}y^{14}z^3 + \\
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 & + 7xy^6z & + (-2)x^8y^{11}z & + 2xy^5 & + (-4)x^8y^{10}
 \end{array}
 \end{array}$$

Jeux des boules mystères

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

1	t	t^2	t^3	t^4
8				
6	9	5		
4	1	3	7	2

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

1	t	t^2	t^3	t^4
9				
3	8			5
2	7	6	1	4

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

1	t	t^2	t^3	t^4
	8			
	7		5	3
9	1	6	4	2

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

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	2

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

1	t	t^2	t^3	t^4
10				
9				
3	8			5
2	7	6	1	4

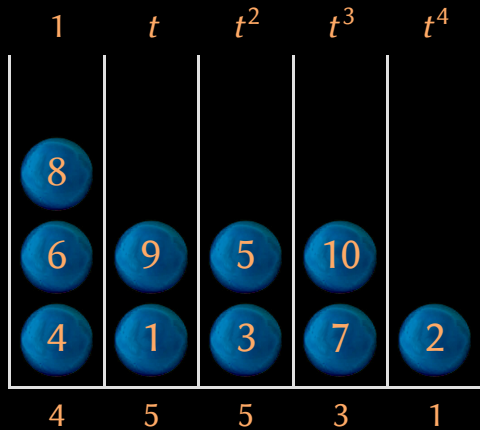
$$(x, y, z) = (1, 1, t)$$

1	t	t^2	t^3	t^4
	8			
10	7		5	3
9	1	6	4	2

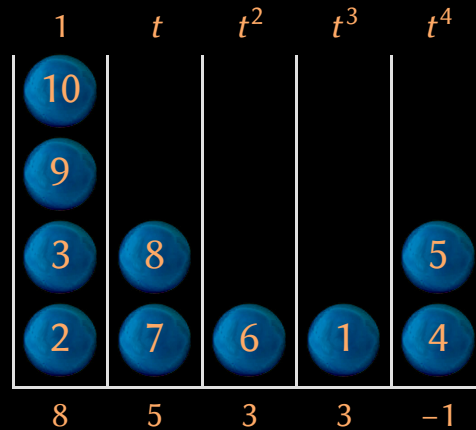
$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 & + 1x^{10}y^{15}z^4 & + 9x^3y^{10}z^4 & + 3x^3y^9z^3 & + (-4)x^{10}y^{14}z^3 + \\
 \\
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 & + 7xy^6z & + (-2)x^8y^{11}z & + 2xy^5 & + (-4)x^8y^{10}
 \end{array}
 \end{array}$$

Jeux des boules mystères

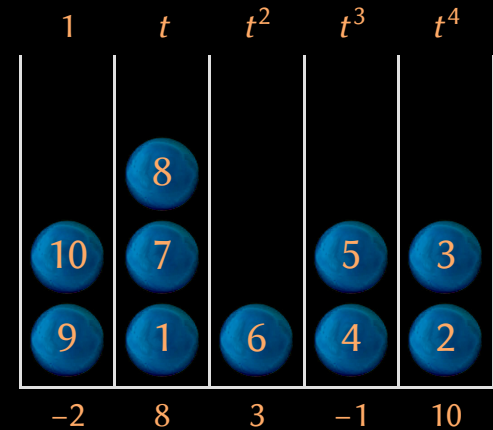
$$(x, y, z) = (t, t, t)$$



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



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



1

2

3

4

5

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

6

7

8

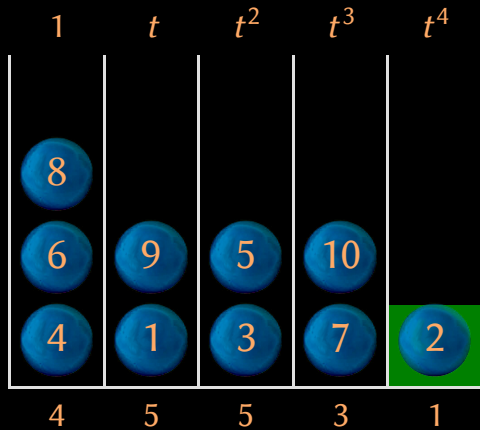
9

10

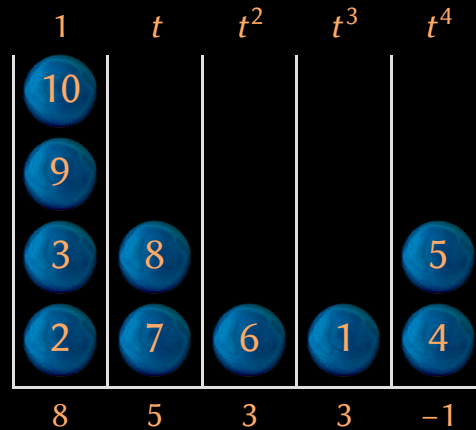
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

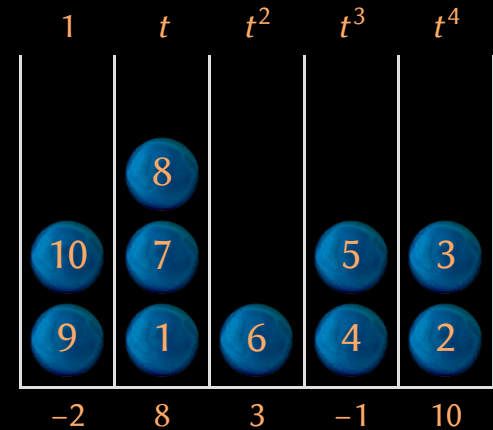
$(x, y, z) = (t, t, t)$



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



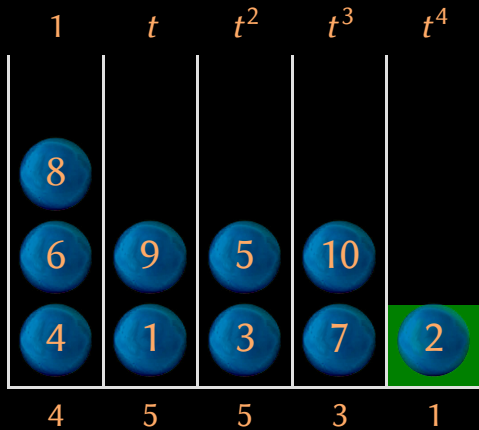
$(x, y, z) = (1, 1, t)$



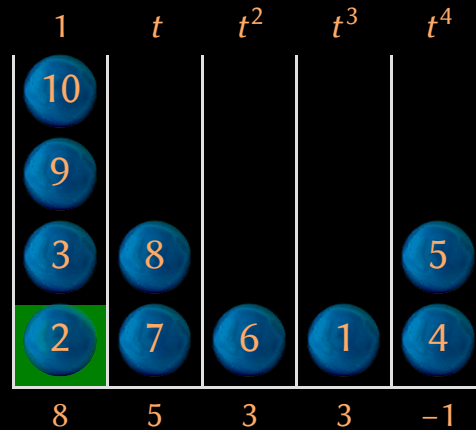
$$\begin{array}{c}
 \begin{array}{ccccc}
 \textcircled{1} & \textcircled{2} & \textcircled{3} & \textcircled{4} & \textcircled{5} \\
 \hline
 3x^{12}y^{18}z^6 + 1x^{10}y^{15}z^4 + 9x^3y^{10}z^4 + 3x^3y^9z^3 + (-4)x^{10}y^{14}z^3 + \\
 \hline
 \textcircled{6} & \textcircled{7} & \textcircled{8} & \textcircled{9} & \textcircled{10} \\
 \hline
 3xy^7z^2 + 7xy^6z + (-2)x^8y^{11}z + 2xy^5 + (-4)x^8y^{10}
 \end{array} \\
 f =
 \end{array}$$

Jeux des boules mystères

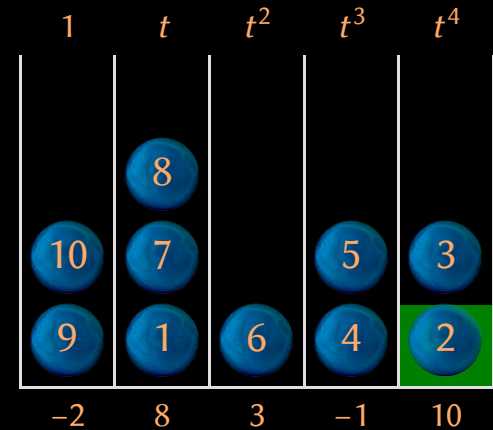
$(x, y, z) = (t, t, t)$



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



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



1

2

3

4

5

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

6

7

8

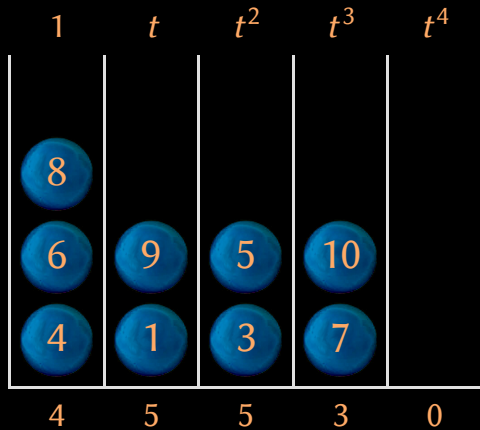
9

10

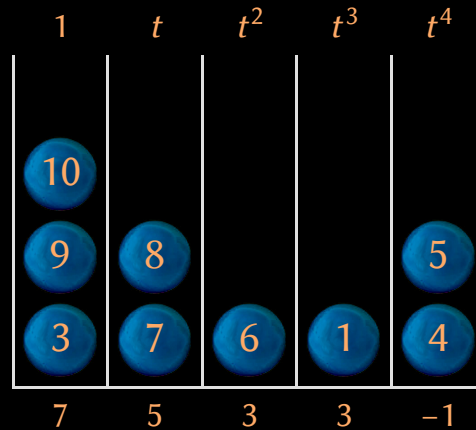
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

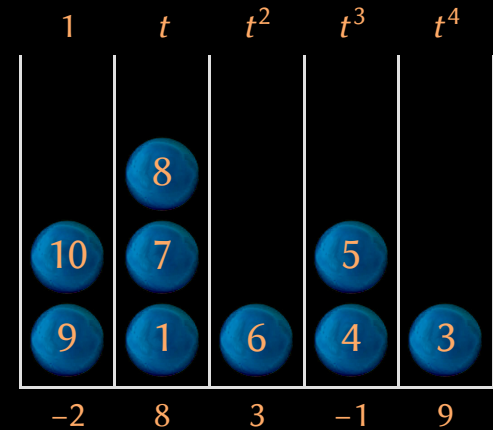
$$(x, y, z) = (t, t, t)$$



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



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



1

2

3

4

5

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

6

7

8

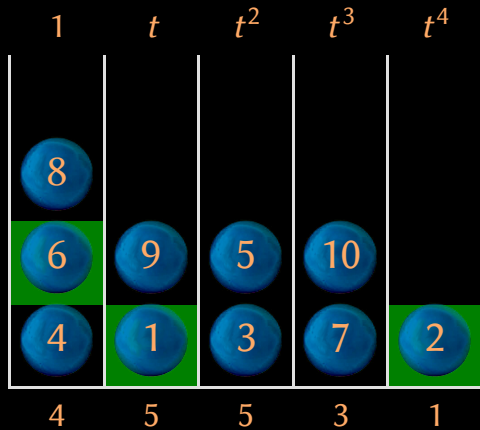
9

10

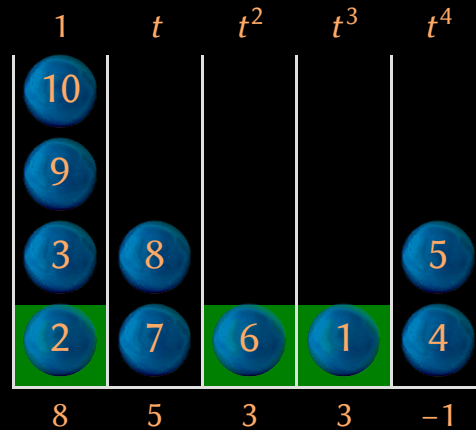
$$\overbrace{3xy^7z^2} + \overbrace{7xy^6z} + \overbrace{(-2)x^8y^{11}z} + \overbrace{2xy^5} + \overbrace{(-4)x^8y^{10}}$$

Jeux des boules mystères

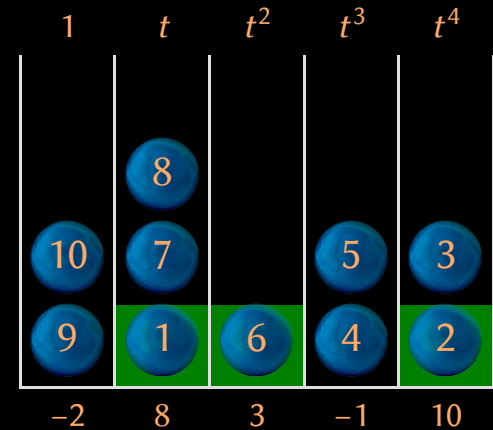
$(x, y, z) = (t, t, t)$



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



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



1

2

3

4

5

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

6

7

8

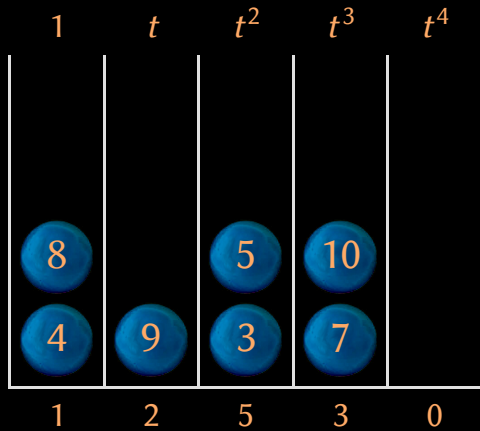
9

10

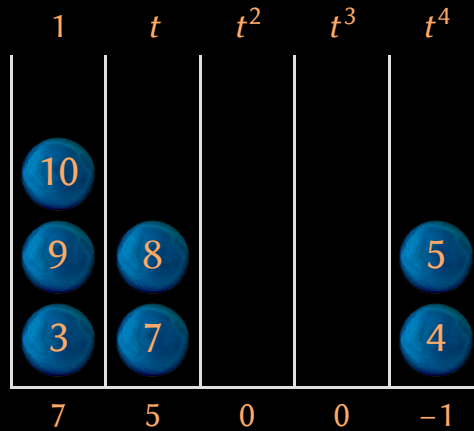
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

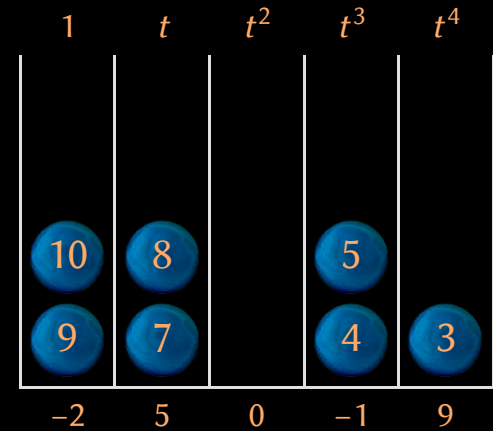
$$(x, y, z) = (t, t, t)$$



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



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



1

2

3

4

5

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

6

7

8

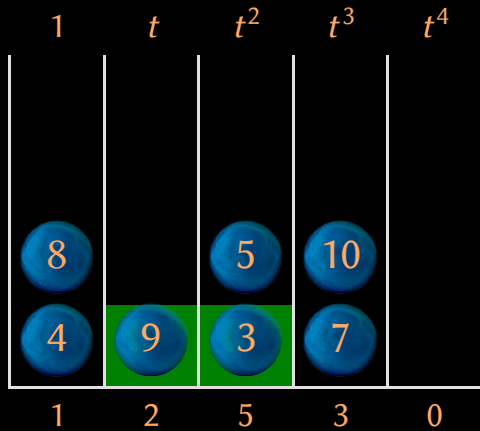
9

10

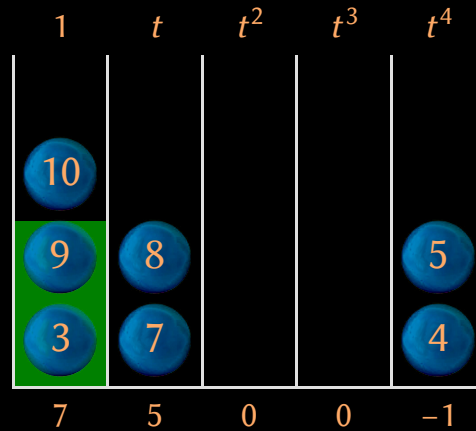
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

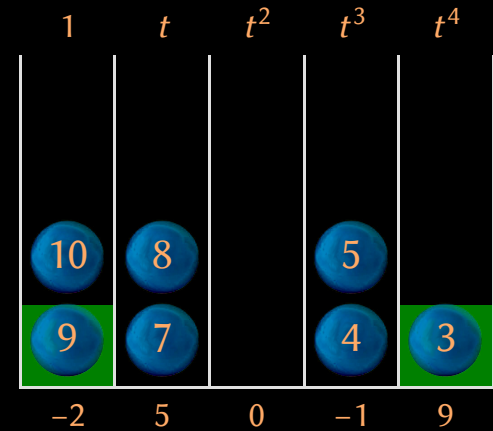
$(x, y, z) = (t, t, t)$



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



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



1

2

3

4

5

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

6

7

8

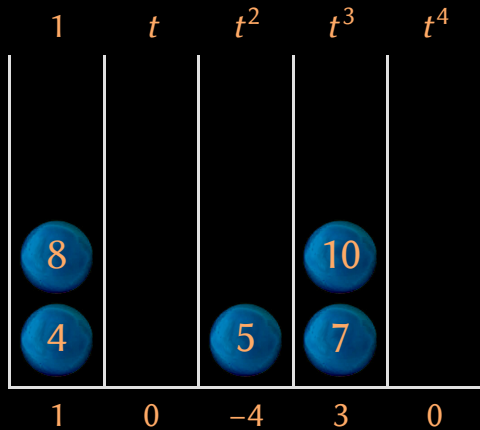
9

10

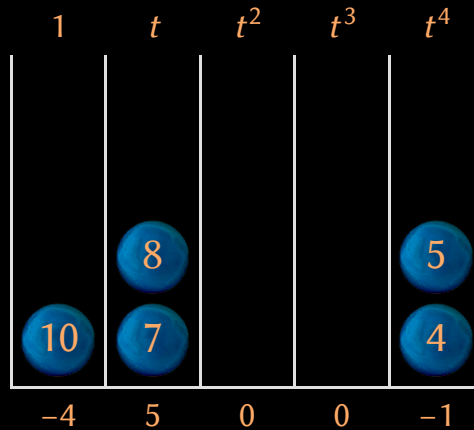
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

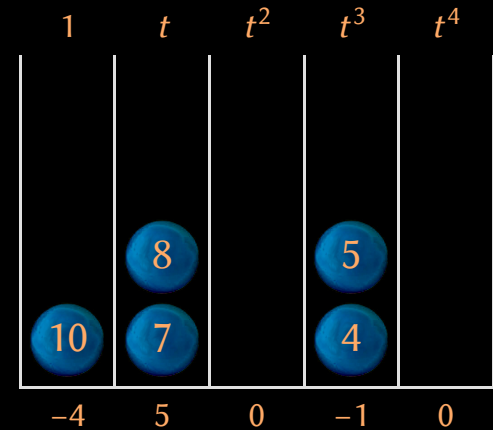
$$(x, y, z) = (t, t, t)$$



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



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



1

2

3

4

5

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

6

7

8

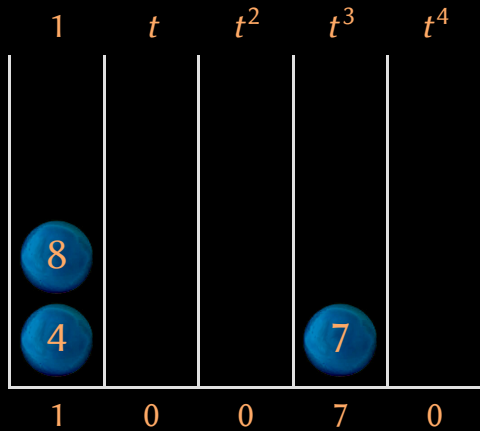
9

10

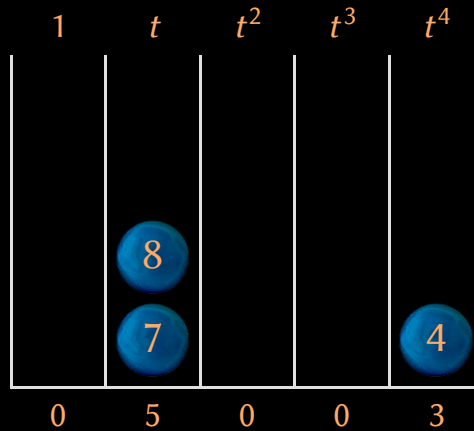
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

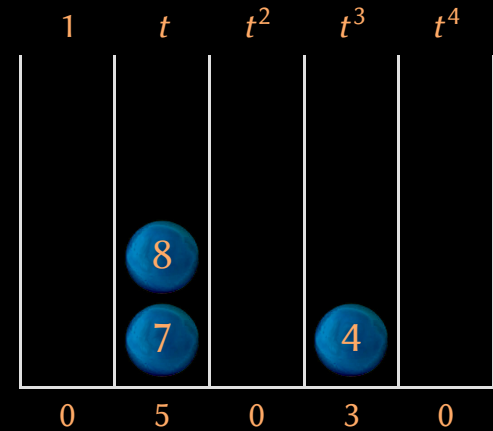
$$(x, y, z) = (t, t, t)$$



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



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



1

2

3

4

5

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

6

7

8

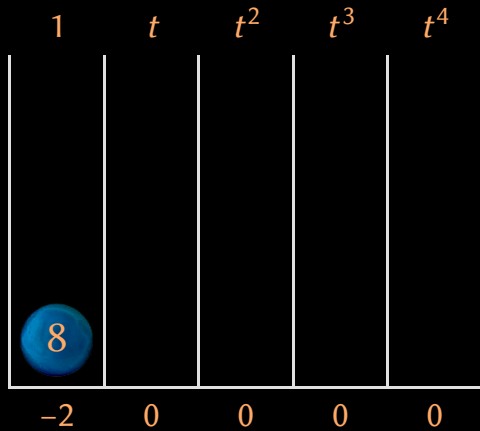
9

10

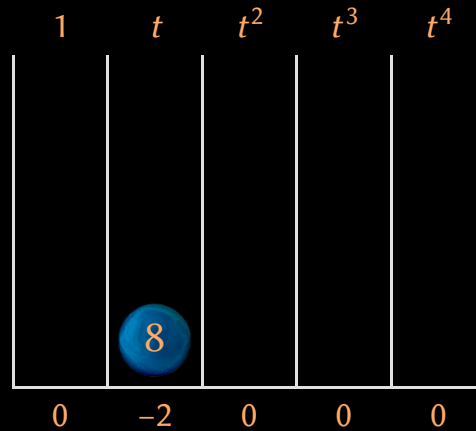
$$\overbrace{3xy^7z^2}^6 + \overbrace{7xy^6z}^7 + \overbrace{(-2)x^8y^{11}z}^8 + \overbrace{2xy^5}^9 + \overbrace{(-4)x^8y^{10}}^{10}$$

Jeux des boules mystères

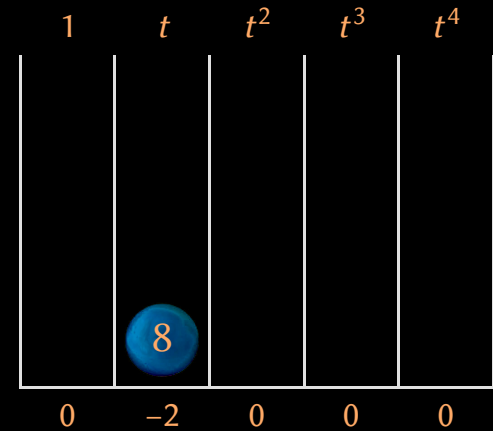
$$(x, y, z) = (t, t, t)$$



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



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



1

2

3

4

5

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

6

7

8

9

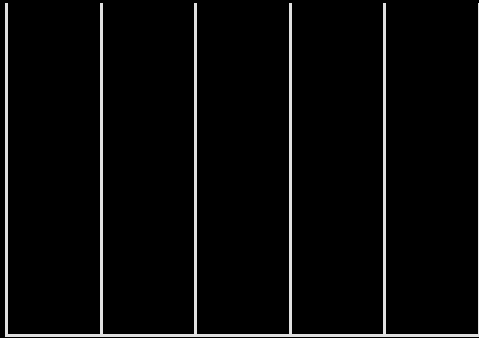
10

$$\overbrace{3xy^7z^2} + \overbrace{7xy^6z} + \overbrace{(-2)x^8y^{11}z} + \overbrace{2xy^5} + \overbrace{(-4)x^8y^{10}}$$

Jeux des boules mystères

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

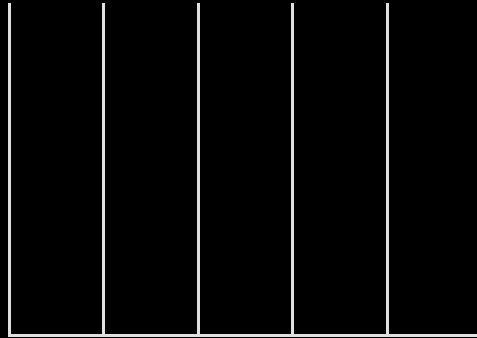
1 t t^2 t^3 t^4



0 0 0 0 0

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

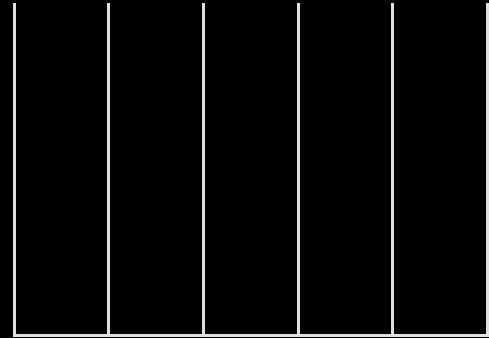
1 t t^2 t^3 t^4



0 0 0 0 0

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

1 t t^2 t^3 t^4



0 0 0 0 0

1

2

3

4

5

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

6

7

8

9

10

$$\overbrace{3xy^7z^2} + \overbrace{7xy^6z} + \overbrace{(-2)x^8y^{11}z} + \overbrace{2xy^5} + \overbrace{(-4)x^8y^{10}}$$

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

$$M_{\mathbb{K}}^{\text{sparse}}(s) \leq_{\text{heuristique}} \frac{3}{2} M_{\mathbb{K}}^{\circ}(s) + O(s)$$

$$0,407264 < \tau_{\text{crit}} < 0,407265$$

$$0,407264 < \tau_{\text{crit}} < 0,407265$$

$$M_{\mathbb{K}}^{\text{sparse}}(s) \stackrel{\text{heuristique}}{\leq} 1,221795 M_{\mathbb{K}}^{\circ}(s) + O(s)$$

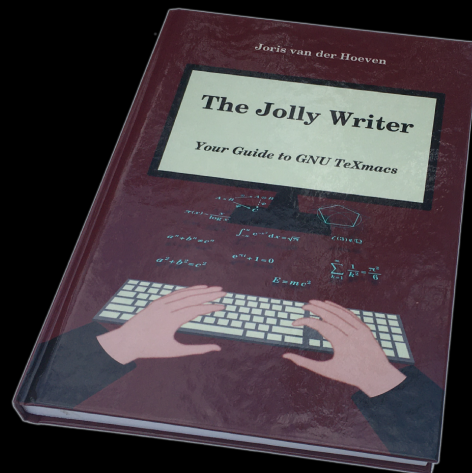
$$0,407264 < \tau_{\text{crit}} < 0,407265$$

$$M_{\mathbb{K}}^{\text{sparse}}(s) \leq_{\text{heuristique}} 1,221795 M_{\mathbb{K}}^{\circ}(s) + O(s)$$

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
3τ	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>