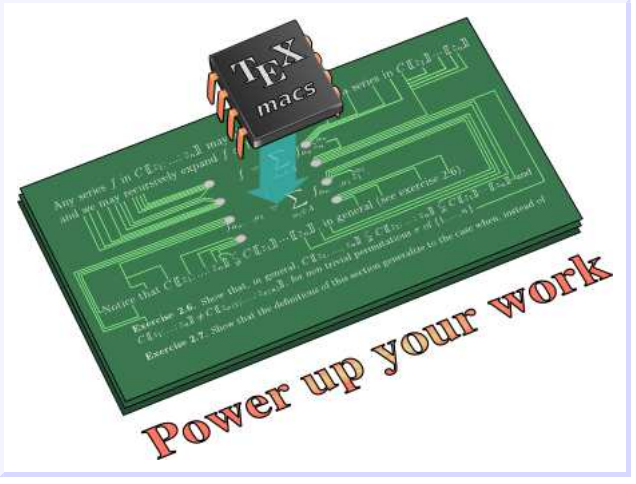
Algorithmes rapides pour calculer avec les séries formelles



Lyon 2007

http://www.TEXMACS.org

- **Intégration d'équations différentielles**

$$\boldsymbol{F}'(z) = \boldsymbol{\Phi}(\boldsymbol{F}(z), z)$$

$\boldsymbol{F}(z)$ convergent en 0. Calculer $\boldsymbol{F}(\varepsilon)$ avec beaucoup de décimales.

- **Intégration d'équations aux dérivées partielles**

$$\boldsymbol{F}_{z_n}(\boldsymbol{z}) = \boldsymbol{\Phi}(\boldsymbol{F}(\boldsymbol{z}), \boldsymbol{F}_{z_1}(\boldsymbol{z}), \ldots, \boldsymbol{z})$$

$\boldsymbol{F}(\boldsymbol{z})$ convergent en $\boldsymbol{0}$. Calculer $\boldsymbol{F}(\boldsymbol{\varepsilon})$ avec beaucoup de décimales.

- **Équations de la combinatoire**

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

Énumère les alccols de la forme $\mathrm{C}_n\mathrm{H}_{2n+1}\mathrm{OH}$.

Multiplication de séries formelles

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

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

Algorithmes classiques de multiplication

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

Exemple : la multiplication Karatsuba

Pour n pair, décomposer :

$$\begin{cases} f^{\downarrow} &= f_0 + \cdots + f_{\frac{n}{2}-1}\, z^{\frac{n}{2}-1} \\ f^{\uparrow} &= f_{\frac{n}{2}} + \cdots + f_{n-1}\, z^{\frac{n}{2}-1} \end{cases} \quad \begin{cases} g^{\downarrow} &= g_0 + \cdots + g_{\frac{n}{2}-1}\, z^{\frac{n}{2}-1} \\ g^{\uparrow} &= g_{\frac{n}{2}} + \cdots + g_{n-1}\, z^{\frac{n}{2}-1} \end{cases}$$

Appliquer récursivement :

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

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

$$\square = \left(f^{\downarrow}+f^{\uparrow}\right)\left(g^{\downarrow}+g^{\uparrow}\right) - f^{\downarrow}\,g^{\downarrow} - f^{\uparrow}\,g^{\uparrow}$$

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

$M(n)$: temps pour la multiplication

Logarithme

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

Exponentiation

Pour n pair, supposons

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

$$\text{avec} \quad \begin{cases} f = f_0 + \cdots + f_{n-1}\, z^{n-1}; \\ g = g_0 + \cdots + g_{n/2-1}\, z^{n/2-1} \end{cases}$$

Alors

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

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

Algorithme d'exponentiation en $O(M(n))$.

Principe

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

Implantation

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

Conséquence importante

On calcule le terme $h_n = (f\,g)_n$ du produit $h = f\,g$ dès que $f_0, \ldots, f_n$ et $g_0, \ldots, g_n$ sont connus. En particulier, f_{n+1} et g_{n+1} peuvent dépendre de $h_0, \ldots, h_n$.

Application

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

$$g = \int f' g \qquad\qquad (h = f' g)$$

En effet

$$\begin{aligned} g_n &= \left[\int f' g\right]_n \\ &= \frac{1}{n}(f' g)_{n-1} \\ &= \frac{1}{n}\left[(f')_0\, g_{n-1} + \cdots + (f')_{n-1}\, g_0\right] \end{aligned}$$

Inconvenient

Plus de multiplication rapide.

Anticipation $\Rightarrow$ Accélération

Anticipation ⇒ Accélération

Algorithme naïf

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

0 $h_0 = f_0\, g_0$.
1 $h_1 = f_0\, g_1 + f_1\, g_0$.
2 $h_2 = f_0\, g_2 + f_1\, g_1 + f_2\, g_0$.

Algorithme détendu

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

0 $h_0 = f_0\, g_0$.
1 $h_1 = (f_0 + f_1)\,(g_0 + g_1) - f_0\, g_0 - f_1\, g_1$
2 $h_2 = f_0\, g_2 + f_1\, g_1 + f_2\, g_0$.

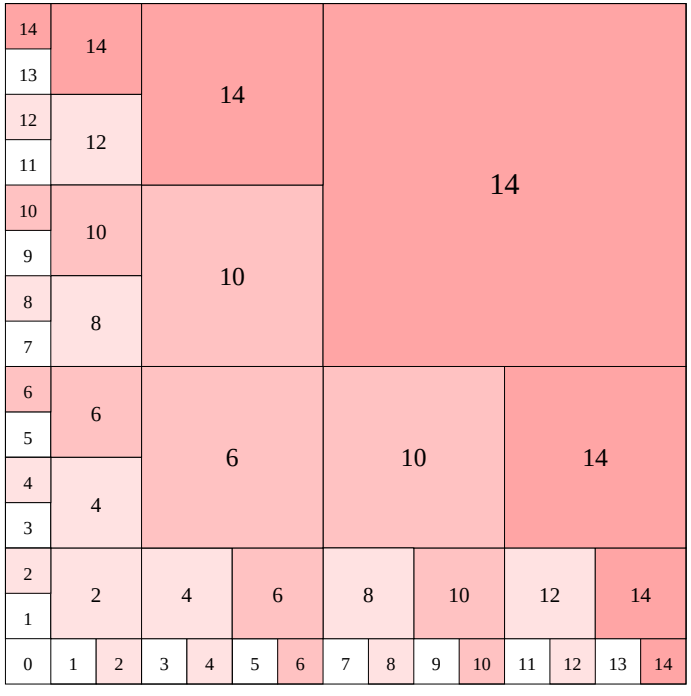
La formule pour h_k ne dépend que de $f_0, \ldots, f_k$ et $g_0, \ldots, g_k$.

Exemple : multiplication à l'ordre 4

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

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

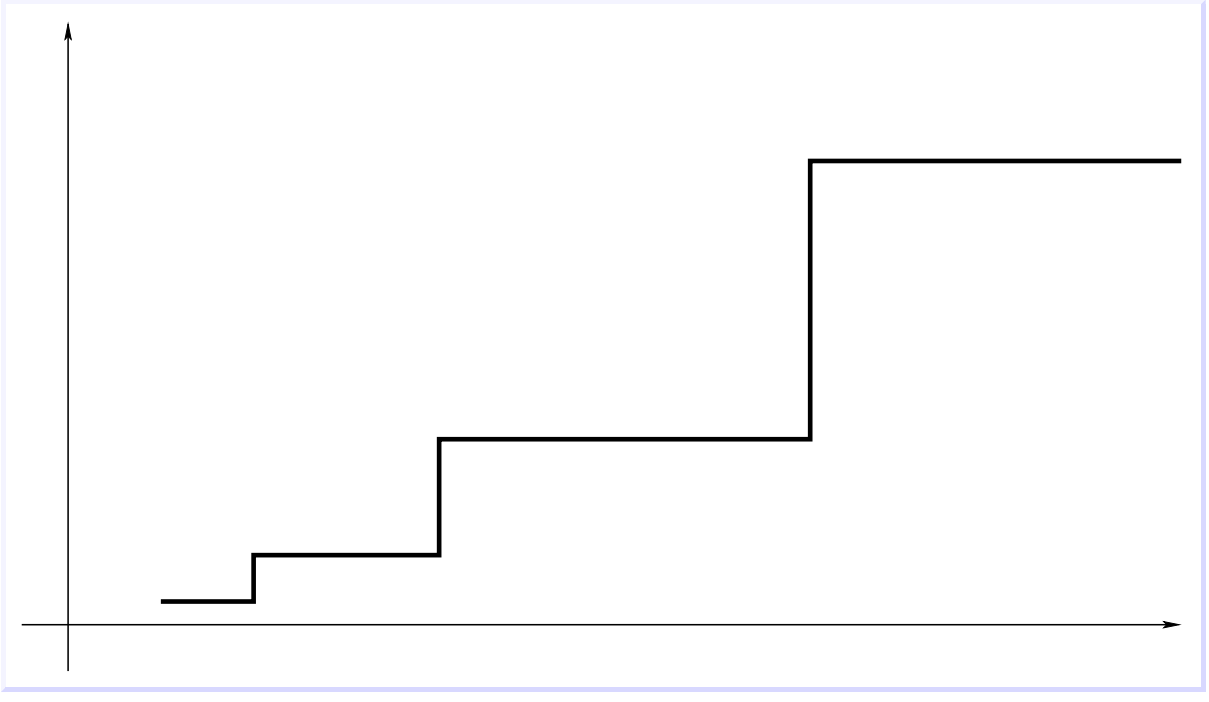
Multiplication détendue rapide



Algorithme en temps $O(M(n)\log n)$

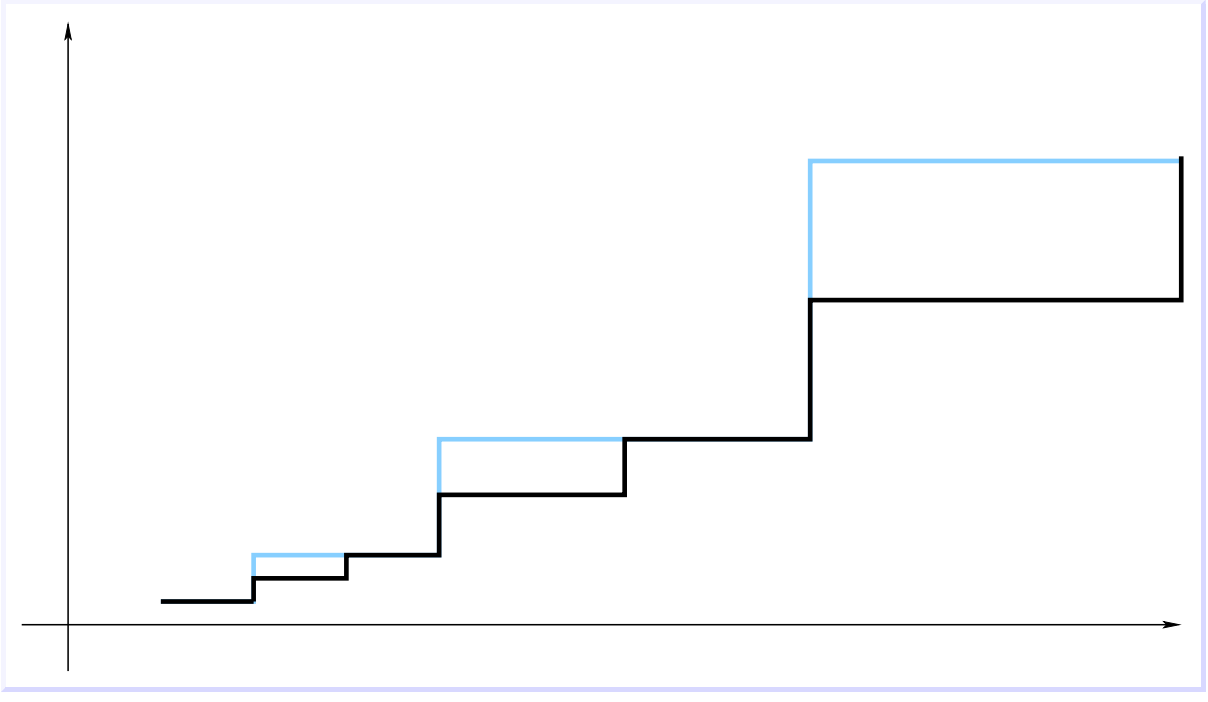
Peut-on améliorer la FFT ?

- La FFT présente des sauts de complexité.



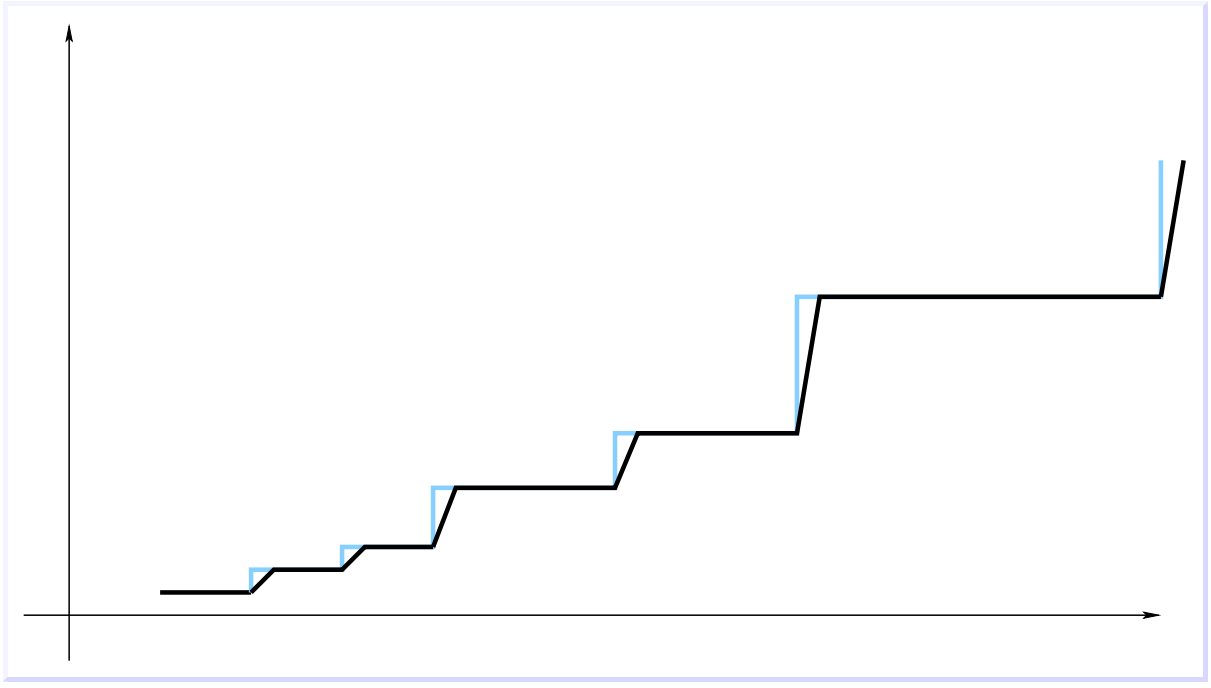
Peut-on améliorer la FFT ?

- La FFT présente des sauts de complexité.



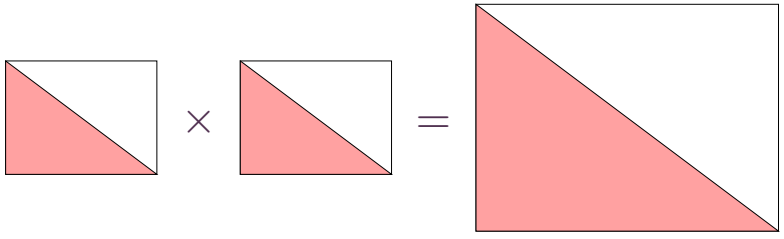
Peut-on améliorer la FFT ?

- La FFT présente des sauts de complexité.



Peut-on améliorer la FFT ?

- Inefficacité en dimension supérieure.



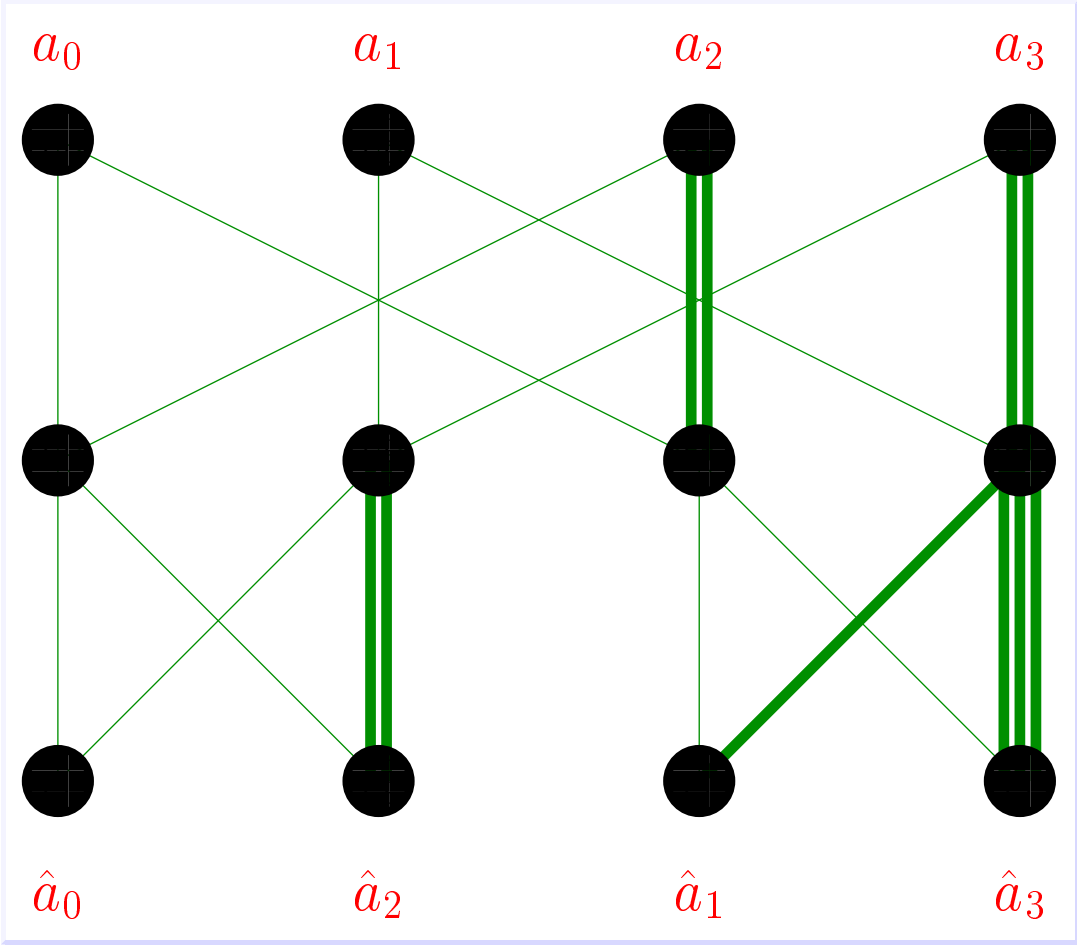
- Soient $P, Q \in \mathbb{C}[z_1, ..., z_d]$ avec $\deg P, \deg Q < n$.
- Taille des entrées : $s = O(\frac{n^d}{d!})$.
- Complexité naïve: $O(d\, n^d \log n) \gg O(s \log s)$.

- Notations.
  - $\mathcal{R} \ni \frac{1}{2}$: effective constant ring.
  - $n = 2^p$.
  - $\omega \in \mathcal{R}$ primitive n-th root of unity.
- Definition F.F.T.

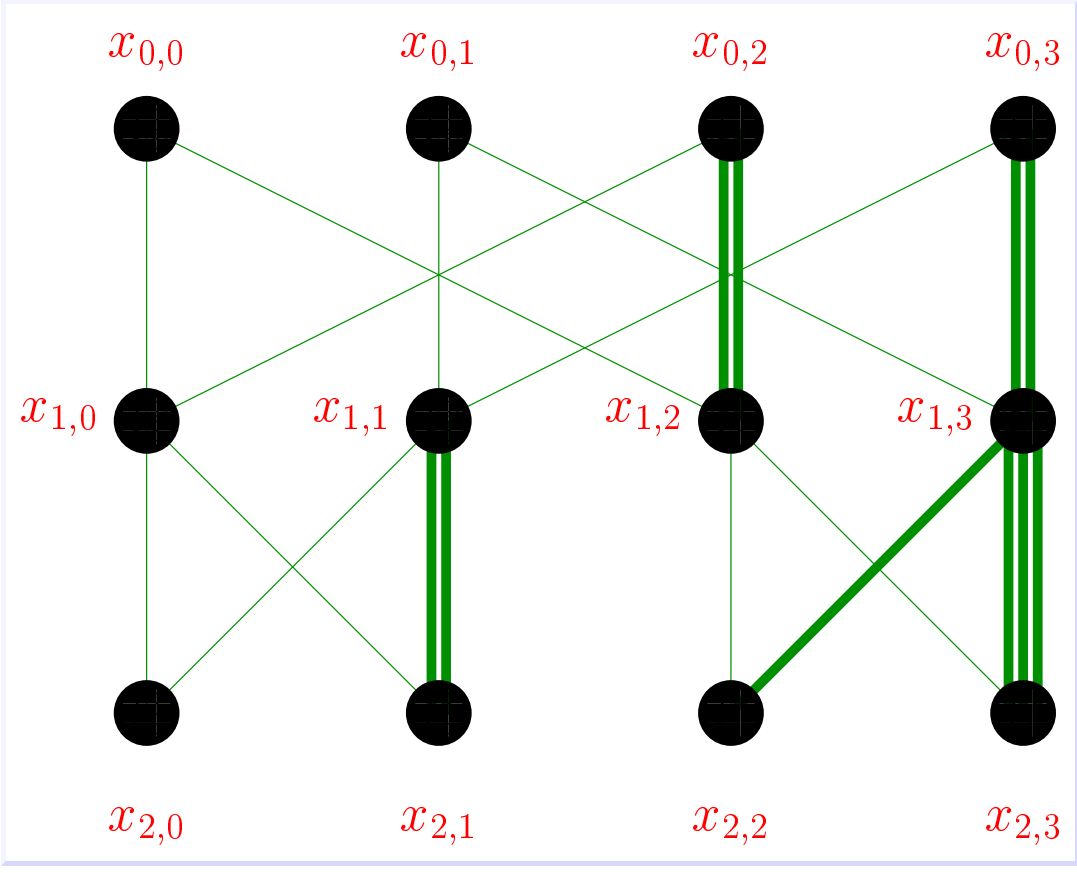
$$\begin{array}{ccc} \mathcal{R}^n & \longrightarrow & \mathcal{R}^n \\ (a_0, \ldots, a_{n-1}) & \overset{\text{FFT}}{\longmapsto} & (\hat{a}_0, \ldots, \hat{a}_{n-1}) \end{array}$$

with

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


a_0
a_1
a_2
a_3
$\hat{a}_0$
$\hat{a}_2$
$\hat{a}_1$
$\hat{a}_3$

On-line computation



The cross relation

- $[i]_p$: bitwise mirror of i at length p
  - $[3]_5 = [\overline{00011}]_5 = [\overline{11000}]_5 = 24$
  - $[26]_5 = [\overline{11010}]_5 = [\overline{01011}]_5 = 11$
- Cross relation

$$\begin{pmatrix} x_{s,im_s+j} \\ x_{s,(i+1)m_s+j} \end{pmatrix} = \begin{pmatrix} 1 & \omega^{[i]_s m_s} \\ 1 & -\omega^{[i]_s m_s} \end{pmatrix} \begin{pmatrix} x_{s-1,im_s+j} \\ x_{s-1,(i+1)m_s+j} \end{pmatrix}.$$

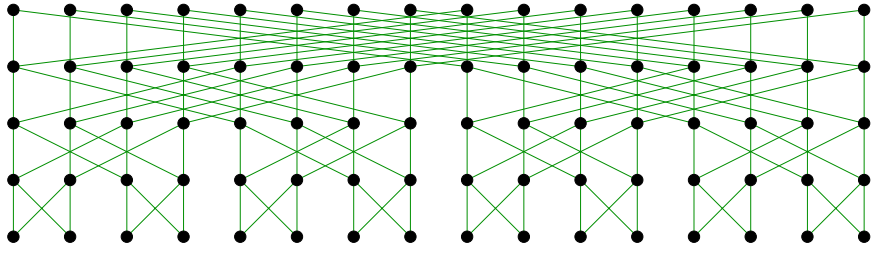
- Direct formulas

$$\begin{aligned} x_{s,im_s+j} &= (\mathrm{FFT}_{\omega^{m_s}}(a_j, a_{m_s+j}, \ldots, a_{n-m_s+j}))_{[i]_s} \\ x_{p,i} &= \hat{a}_{[i]_p} \\ \hat{a}_i &= x_{p,[i]_p} \end{aligned}$$

- Transformation at length $l \leqslant n = 2^p$

$$(a_0, a_1, \ldots, a_{l-1}) \longleftrightarrow (\hat{a}_{[0]_p}, \hat{a}_{[1]_p}, \ldots, \hat{a}_{[l-1]_p})$$

- Computation



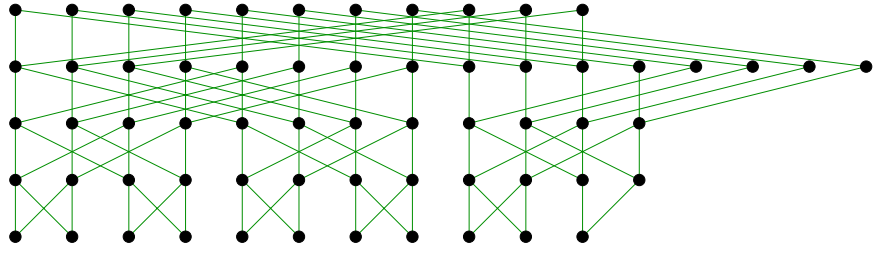
- Complexity

Theorem. *The T.F.T. of* $(a_0, \ldots, a_{l-1})$ *w.r.t.* ω *can be computed using* $l\,p + n$ *additions-subtractions and* $\lceil (l\,p + n)/2 \rceil$ *multiplications with powers of* ω.

- Transformation at length $l \leqslant n = 2^p$

$$(a_0, a_1, \ldots, a_{l-1}) \longleftrightarrow (\hat{a}_{[0]_p}, \hat{a}_{[1]_p}, \ldots, \hat{a}_{[l-1]_p})$$

- Computation



- Complexity

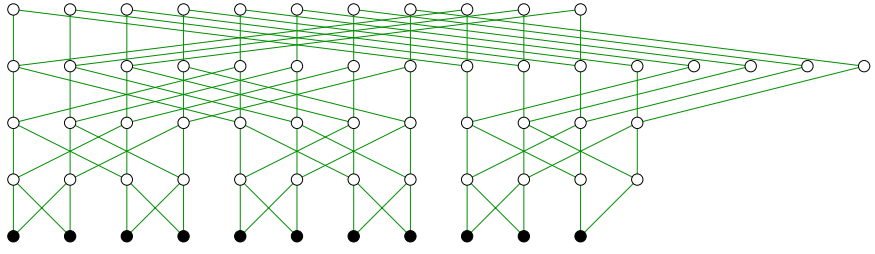
Theorem. *The T.F.T. of* $(a_0, \ldots, a_{l-1})$ *w.r.t.* ω *can be computed using* $l\,p + n$ *additions-subtractions and* $\lceil (l\,p + n)/2 \rceil$ *multiplications with powers of* ω.

- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

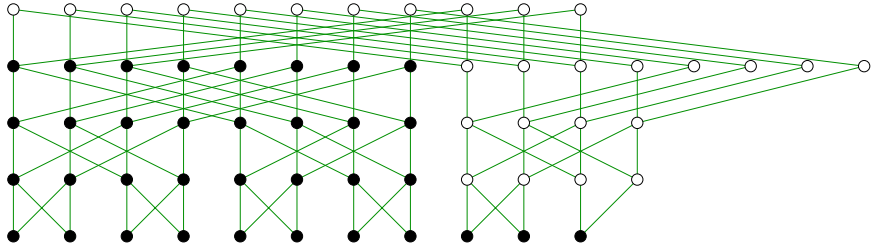


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

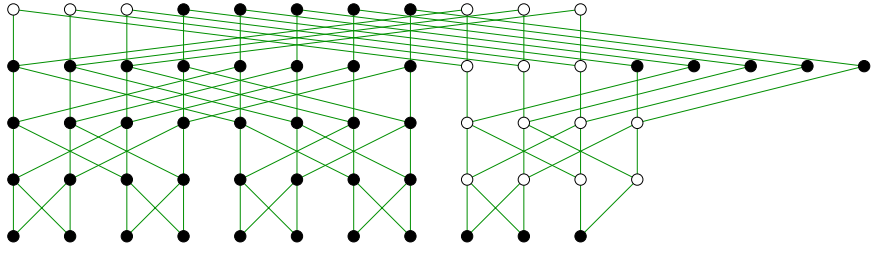


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i\, y_1$ et $y_0 = x_1 - \omega^i\, y_1$
  - $x_1 = \frac{1}{2}\,(x_0 + y_0)$ et $y_1 = \frac{1}{2}\,\omega^{-i}\,(x_0 - y_0)$
  - $x_0 = 2\,x_1 - y_0$ et $y_1 = \omega^{-i}\,(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i\, y_1$ et $y_0 = x_0 - 2\,\omega^i\, y_1$
- The inverse T.F.T.



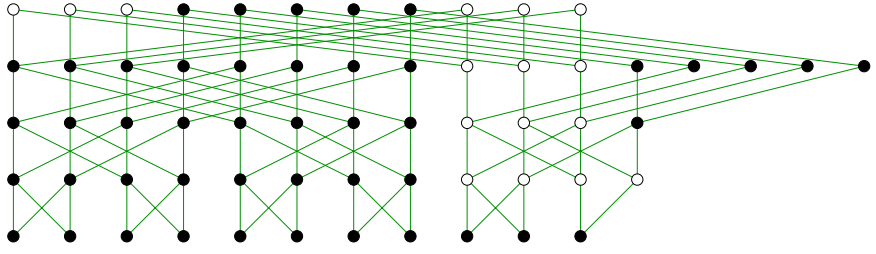
- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i\, y_1$ et $y_0 = x_1 - \omega^i\, y_1$
  - $x_1 = \frac{1}{2}\,(x_0 + y_0)$ et $y_1 = \frac{1}{2}\,\omega^{-i}\,(x_0 - y_0)$
  - $x_0 = 2\,x_1 - y_0$ et $y_1 = \omega^{-i}\,(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i\, y_1$ et $y_0 = x_0 - 2\,\omega^i\, y_1$

- The inverse T.F.T.

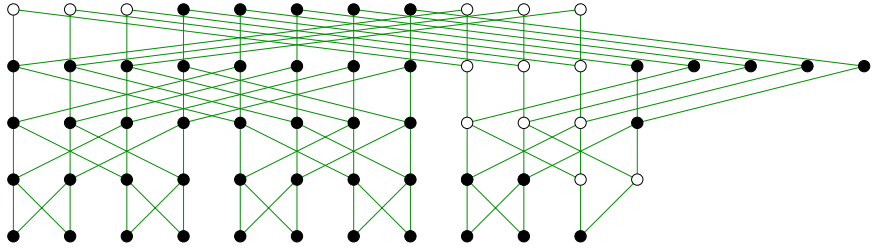


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

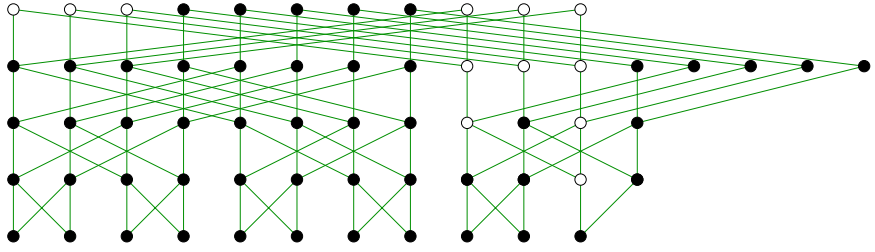


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

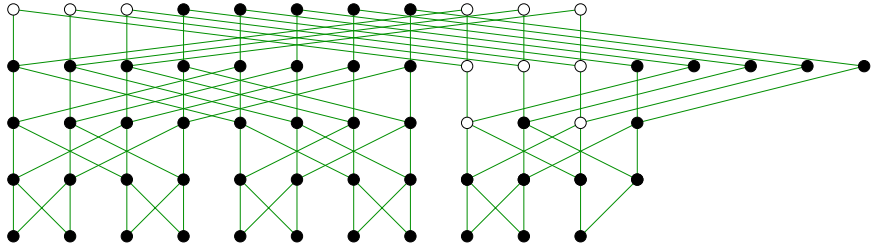


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

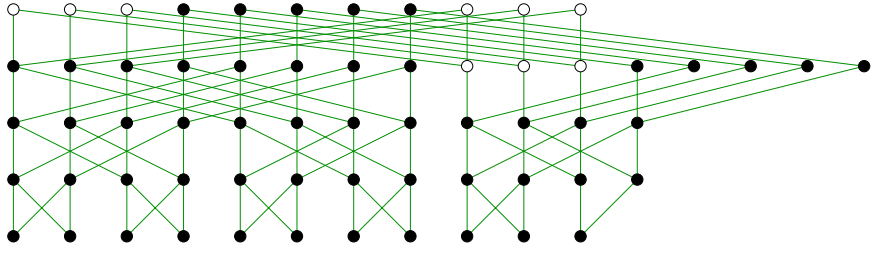


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

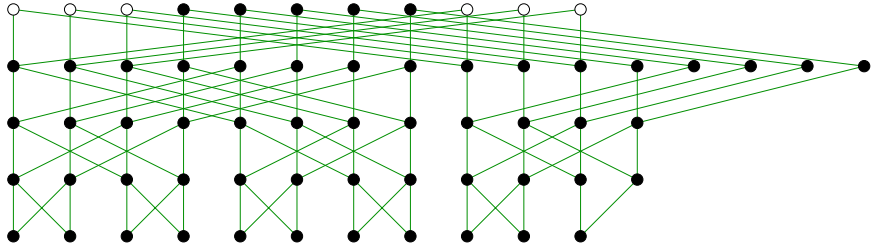


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

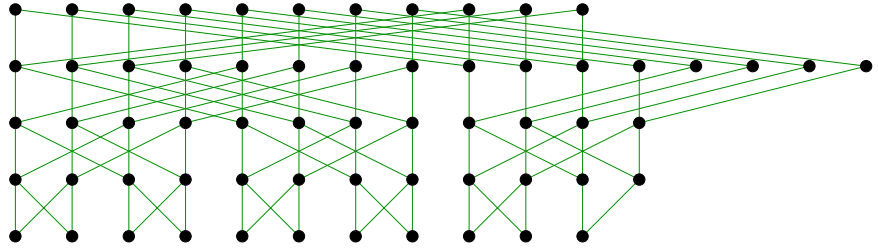


- Observation on the cross relation

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (x_ϵ, y_δ) determines $(x_{1-\epsilon}, y_{1-\delta})$

  - $x_0 = x_1 + \omega^i y_1$ et $y_0 = x_1 - \omega^i y_1$
  - $x_1 = \frac{1}{2}(x_0 + y_0)$ et $y_1 = \frac{1}{2}\omega^{-i}(x_0 - y_0)$
  - $x_0 = 2x_1 - y_0$ et $y_1 = \omega^{-i}(x_1 - y_0)$
  - $x_1 = x_0 - \omega^i y_1$ et $y_0 = x_0 - 2\omega^i y_1$
- The inverse T.F.T.

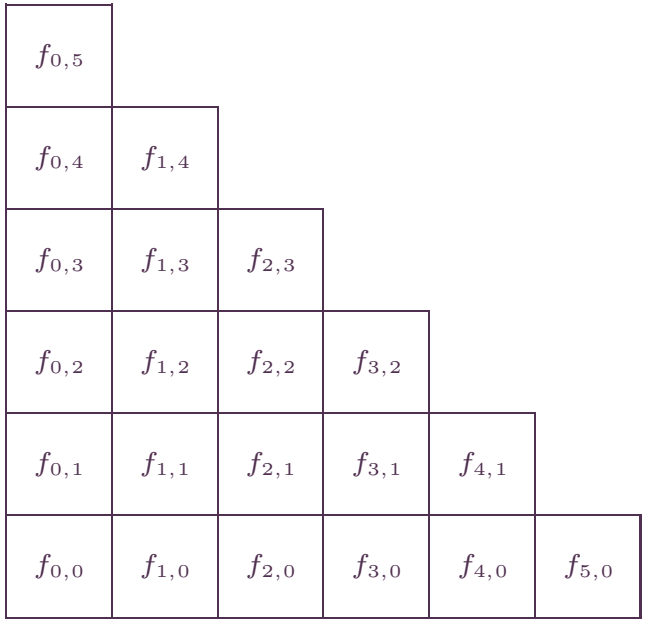


- Complexity

Theorem. *One may recover* $(a_0, \ldots, a_{l-1})$ *from its T.F.T. w.r.t.* ω *using* $l\ p + n$ *additions-subtractions,* $\lceil (l\,p + n)/2 \rceil$ *multiplications with powers of* ω *and* $2\,n$ *shifts.*

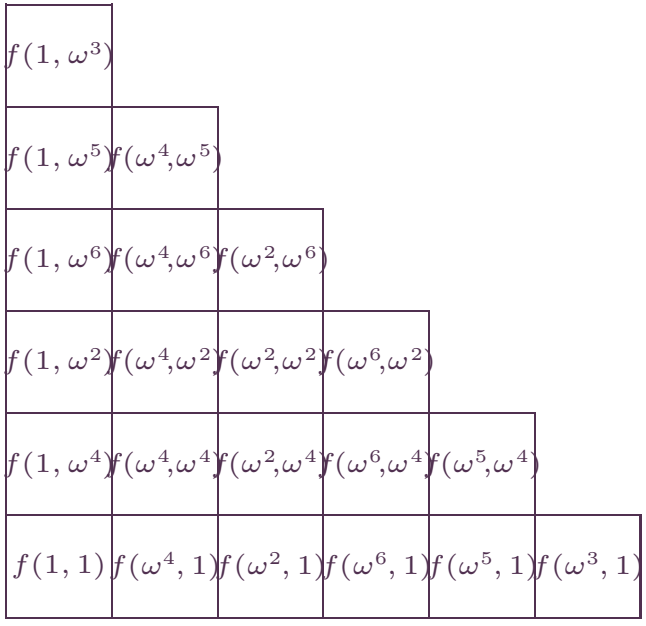
Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



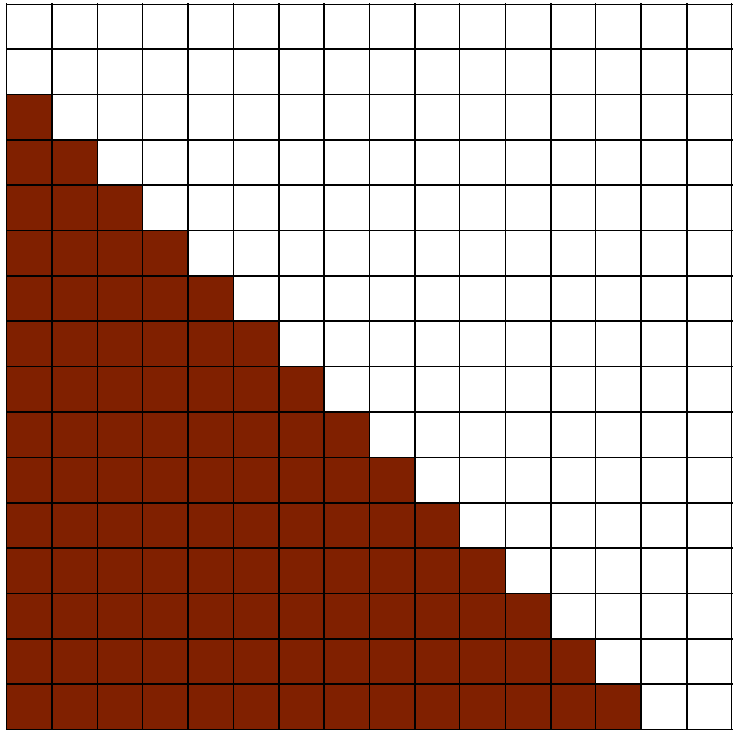
Multivariate case

- T.F.T. of $(f_{i_1,\dots,i_d})_{(i_1,\dots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



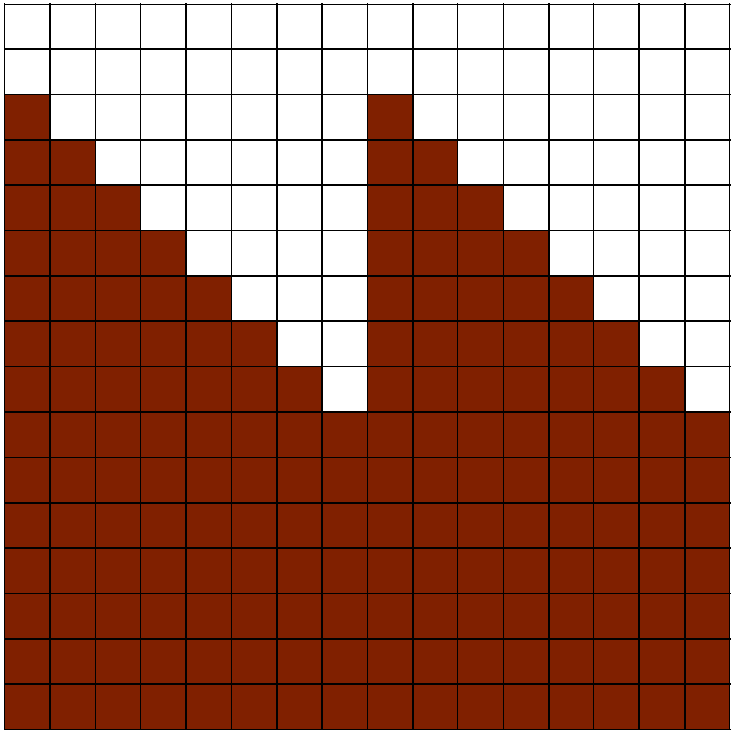
Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



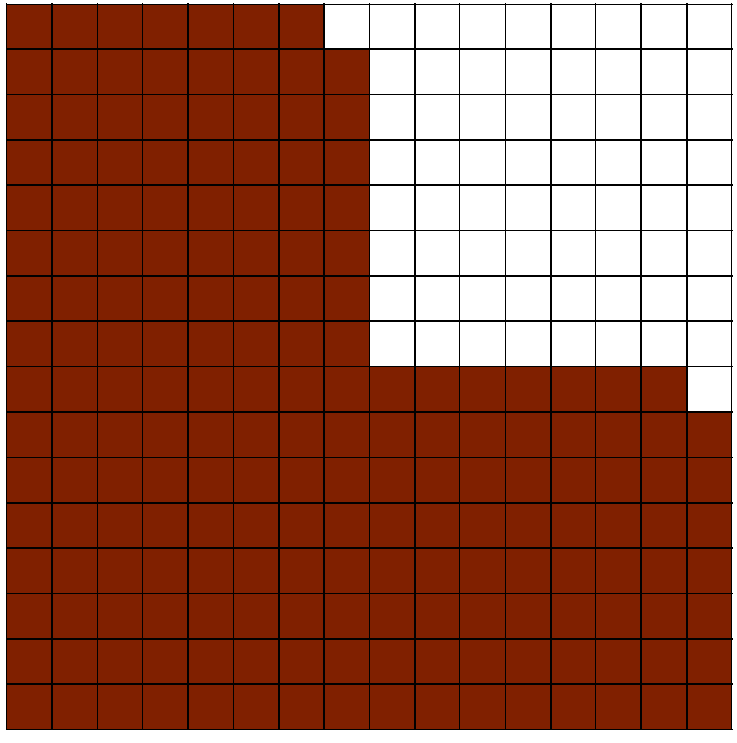
Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



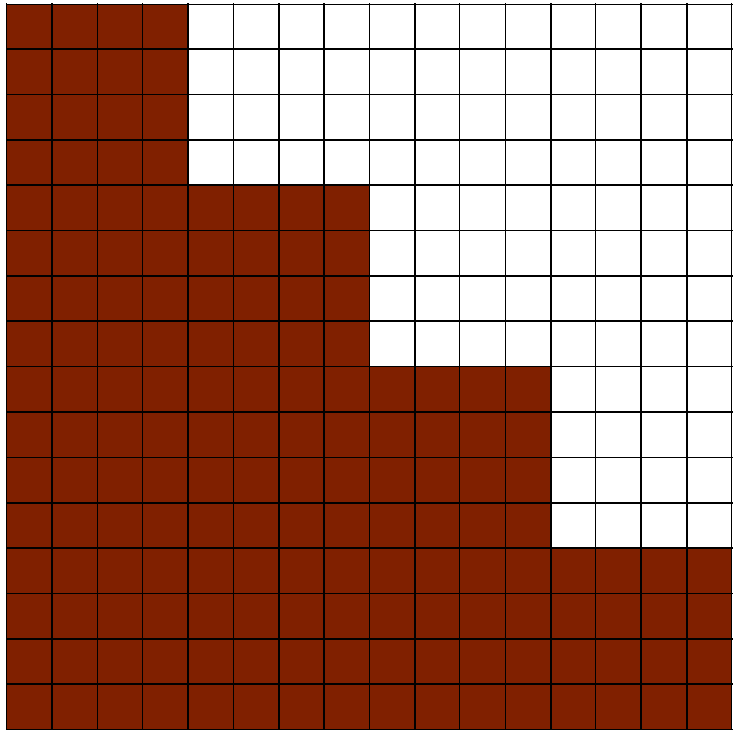
Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



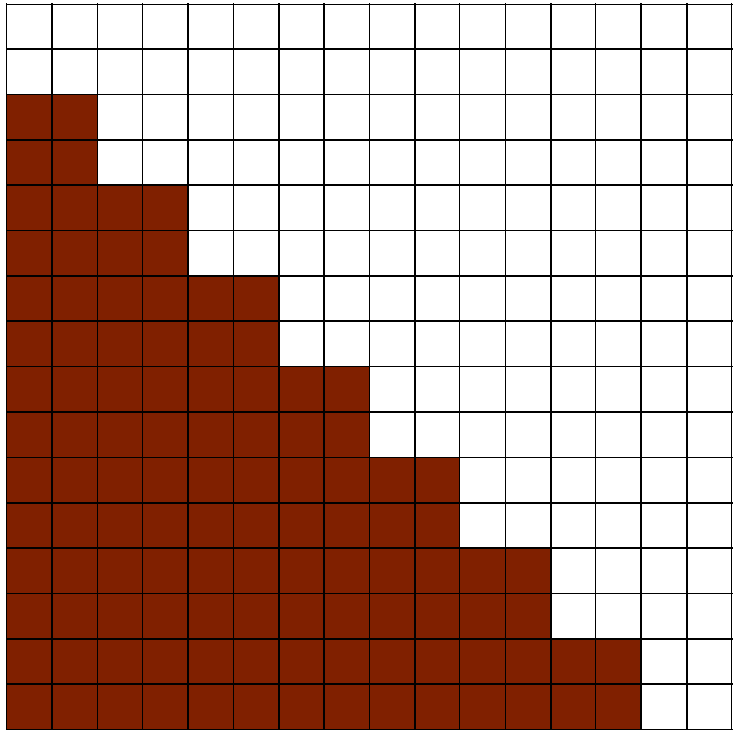
Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$



Multivariate case

- T.F.T. of $(f_{i_1,\ldots,i_d})_{(i_1,\ldots i_d)\in\mathcal{S}}$ with finite $\mathcal{S}\subseteq\mathbb{N}^d$