La Transformée de Fourier Tronquée

PAR

Joris van der Hoeven

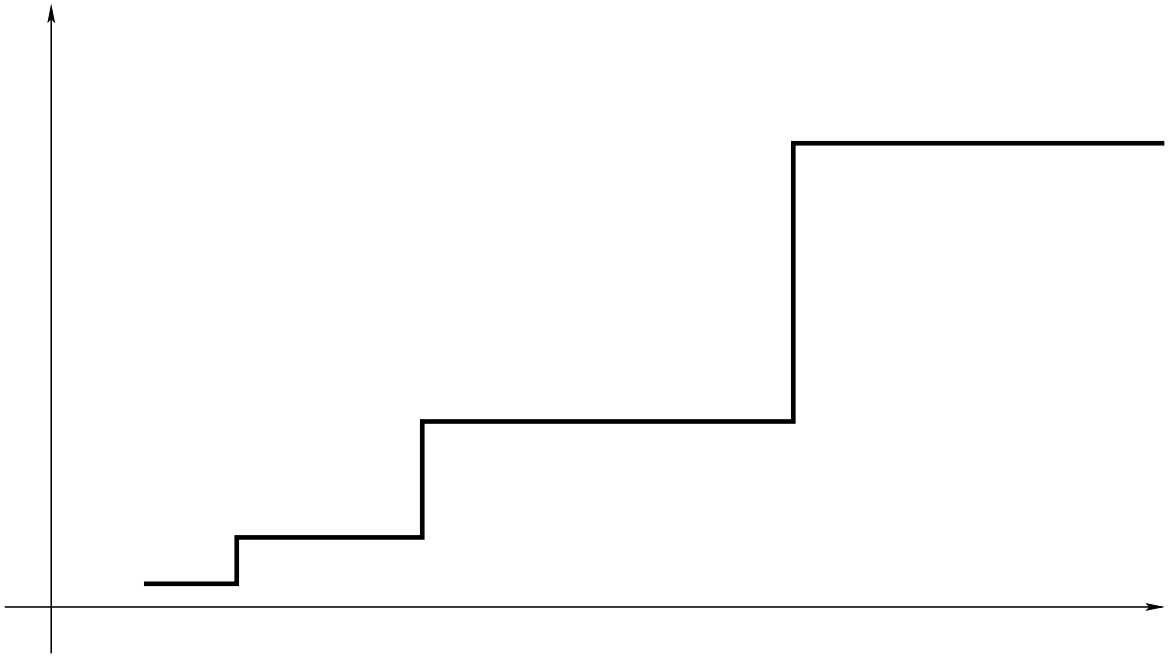
INRIA 2004

Résultats classiques

- Multiplication rapide dans $\mathbb{C}[X]$.
  - Cooley-Tuckey / Gauss.
  - Complexité : $O(n \log n)$ opérations dans $\mathbb{C}$.
- Multiplication rapide dans $\mathbb{Z}$ et $\mathcal{R}[X]$.
  - Shönhage-Straßen / Cantor-Kaltofen.
  - $\mathcal{R}[x]/(x^{n^2} \pm 1) \cong (\mathcal{R}[y]/(y^n \pm 1))[x]/(x^n - y)$
  - Complexité : $O(n \log n \log^2 n)$ opérations dans $\mathcal{R}$.
- Multiplication « creuse » rapide dans $\mathcal{R}[z_1, ..., z_d]$.
  - Canny-Kaltofen-Lakshman.
  - Complexité : $O(s \log^2 s \log \log s)$.
  - Séries formelles : Lecerf-Schost, VdH.

Inconvénients classiques

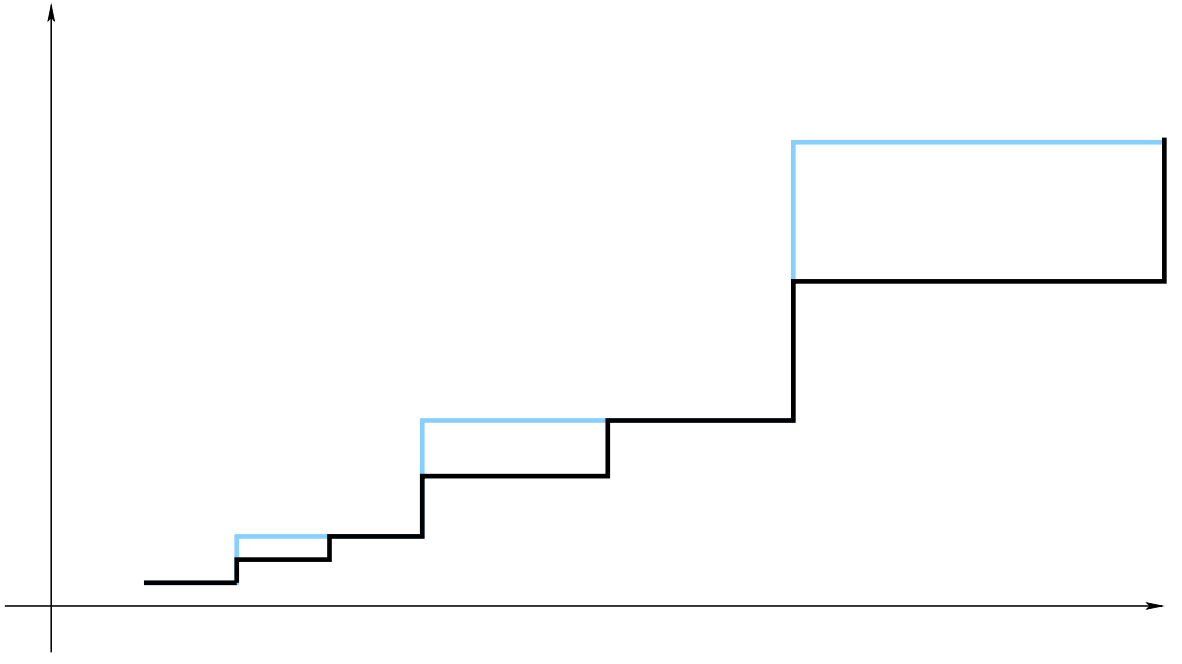
- Phénomène des sauts de complexité.



- Pas de F.F.T. dense efficace en dimension supérieure.
  - Soient $P, Q \in \mathbb{C}[z_1, ..., z_d]$ avec $\deg P, \deg Q < n$.
  - Taille des donnés : $s = O(\frac{n^d}{d!})$.
  - Complexité naïf : $O(d\, n^d \log n) \gg O(s \log s)$.

Inconvénients classiques

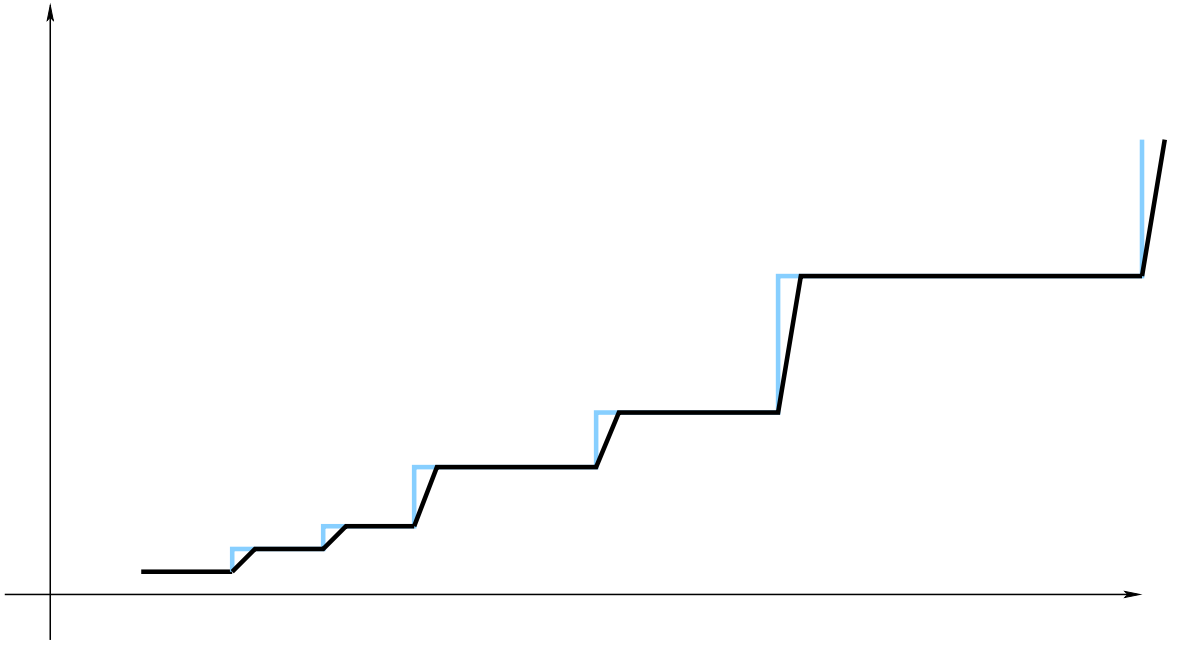
- Phénomène des sauts de complexité.



- Pas de F.F.T. dense efficace en dimension supérieure.
  - Soient $P, Q \in \mathbb{C}[z_1, ..., z_d]$ avec $\deg P, \deg Q < n$.
  - Taille des donnés : $s = O(\frac{n^d}{d!})$.
  - Complexité naïf : $O(d\, n^d \log n) \gg O(s \log s)$.

Inconvénients classiques

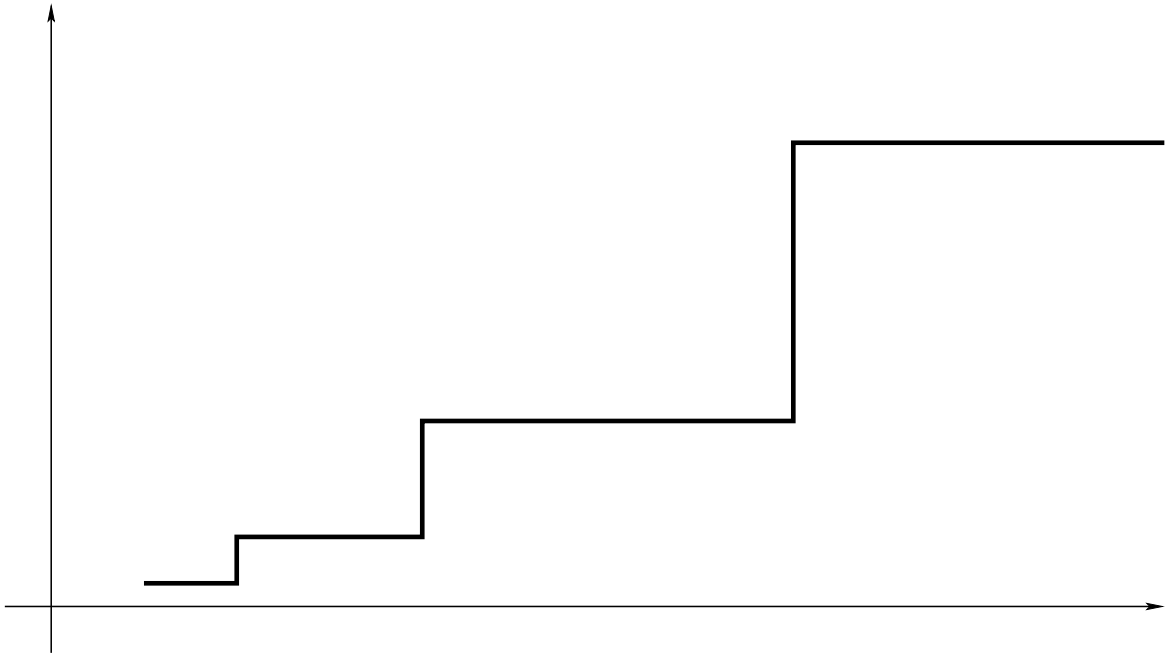
- Phénomène des sauts de complexité.



- Pas de F.F.T. dense efficace en dimension supérieure.
  - Soient $P, Q \in \mathbb{C}[z_1, ..., z_d]$ avec $\deg P, \deg Q < n$.
  - Taille des donnés : $s = O(\frac{n^d}{d!})$.
  - Complexité naïf : $O(d\, n^d \log n) \gg O(s \log s)$.

La Transformée de Fourier Tronquée

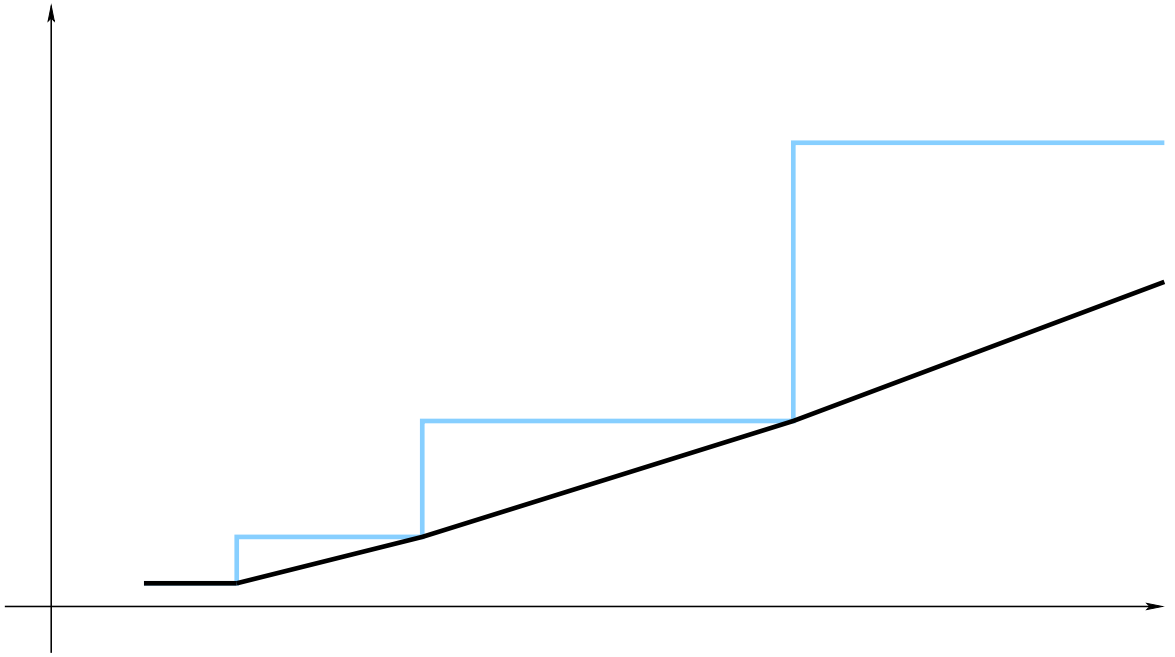
- Plus de phénomène des sauts de complexité.



- F.F.T. dense efficace en dimension supérieure.
  - Algorithme en $O(s \log s)$.

La Transformée de Fourier Tronquée

- Plus de phénomène des sauts de complexité.



- F.F.T. dense efficace en dimension supérieure.
  - Algorithme en $O(s \log s)$.

Rappels I

- Notations.
  - $\mathcal{R} \ni \frac{1}{2}$: anneau effectif de constantes et $n = 2^p$.
  - $\omega \in \mathcal{R}$ racine n-ième primitive de l'unité.
- Définition F.F.T.

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

avec

$$\hat{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij}$$

- Formule d'inversion.

$$\mathrm{FFT}_{\omega^{-1}} \circ \mathrm{FFT}_{\omega} = n\,\mathrm{Id}$$

- Multiplication F.F.T.
  - $A = a_0 + \cdots + a_{n-1} X^{n-1}$, $B = b_0 + \cdots + b_{n-1} X^{n-1}$.

- $C = A\,B = c_0 + \cdots + c_{n-1}\,X^{n-1}$ $(\deg C < n)$.

$$\begin{aligned}
(A(1), ..., A(\omega^{n-1})) &= \mathrm{FFT}_\omega(a_0, ..., a_{n-1}) \\
(B(1), ..., B(\omega^{n-1})) &= \mathrm{FFT}_\omega(b_0, ..., b_{n-1}) \\
(C(1), ..., C(\omega^{n-1})) &= (A(1)\,B(1), ..., A(\omega^{n-1})\,B(\omega^{n-1})) \\
(c_0, ..., c_{n-1}) &= \tfrac{1}{n}\,\mathrm{FFT}_{\omega^{-1}}(C(1), ..., C(\omega^{n-1}))
\end{aligned}$$

- Formule récursif de calcul.
  - Écrire

$$(a_0, \ldots, a_{n-1}) = (b_0, c_0, \ldots, b_{n/2-1}, c_{n/2-1}).$$

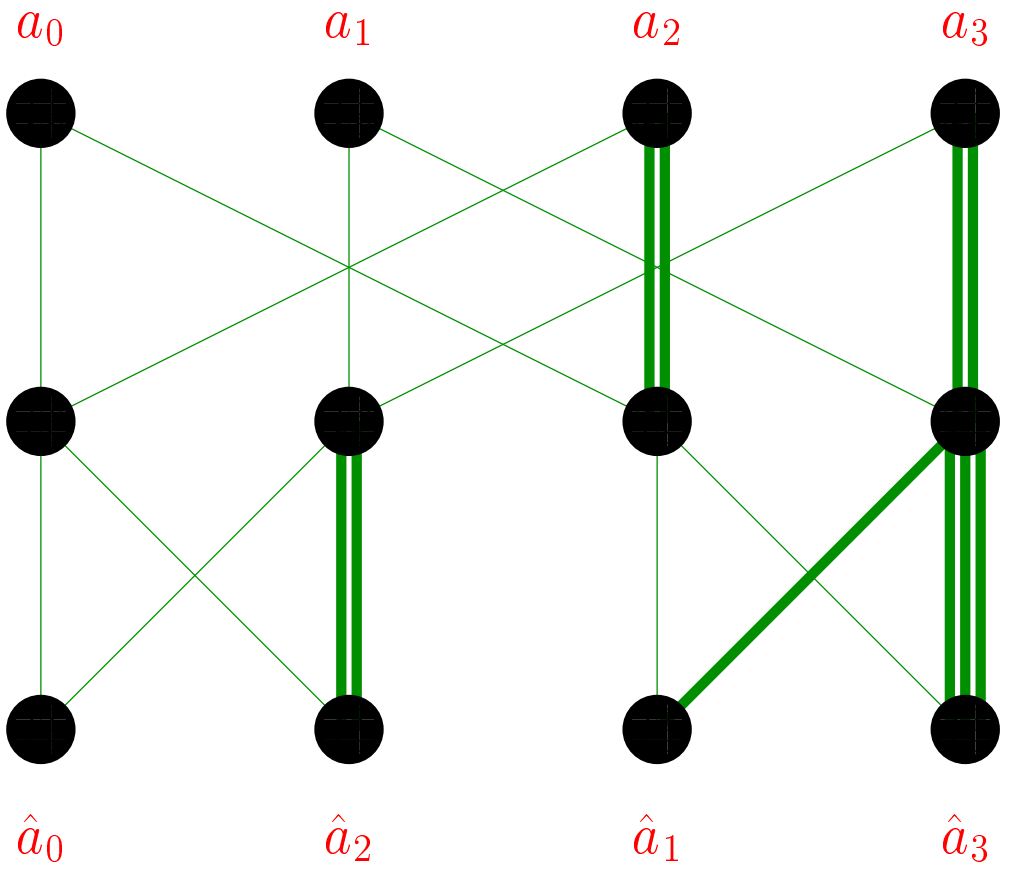
  - Calculer

$$\begin{aligned} \mathrm{FFT}_{\omega^2}(b_0, \ldots, b_{n/2-1}) &= (\hat{b}_0, \ldots, \hat{b}_{n/2-1}) \,; \\ \mathrm{FFT}_{\omega^2}(c_0, \ldots, c_{n/2-1}) &= (\hat{c}_0, \ldots, \hat{c}_{n/2-1}). \end{aligned}$$

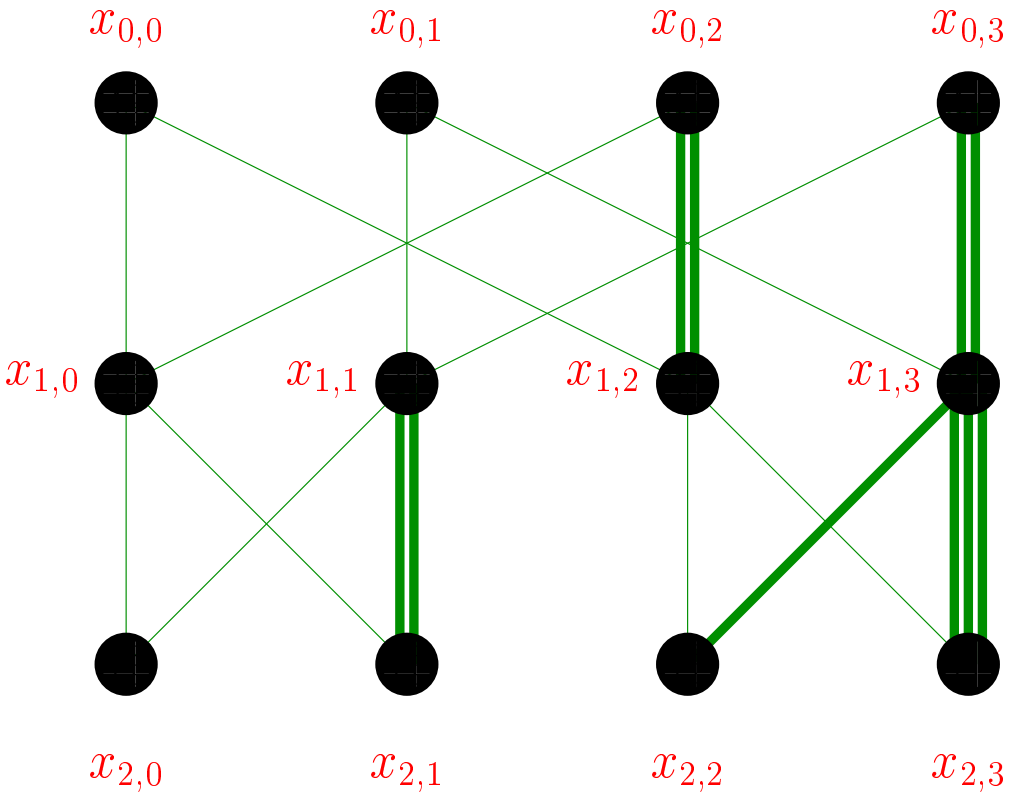
  - On a

$$\begin{aligned} (\hat{a}_0, \ldots, \hat{a}_{n-1}) = (&\hat{b}_0 + \hat{c}_0, \ldots, \hat{b}_{n/2-1} + \hat{c}_{n/2-1}\,\omega^{n/2-1} \\ &\hat{b}_0 - \hat{c}_0, \ldots, \hat{b}_{n/2-1} - \hat{c}_{n/2-1}\,\omega^{n/2-1}). \end{aligned}$$

- Variante en-ligne.



- Variante en-ligne.



- $[i]_p$: miroir binaire de i pour la longueur p
  - $[3]_5 = [\overline{00011}]_5 = [\overline{11000}]_5 = 24$
  - $[26]_5 = [\overline{11010}]_5 = [\overline{01011}]_5 = 11$
- Relation de croisement

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

- Formules directes

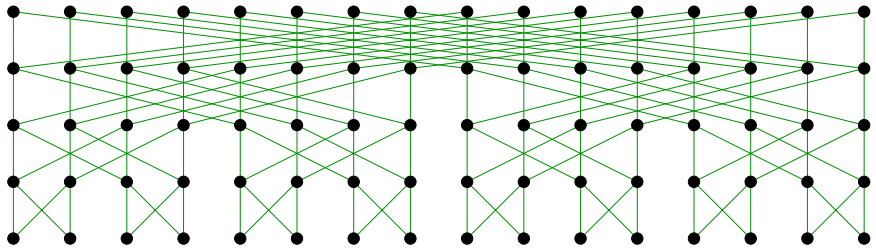
$$\begin{aligned} x_{s,im_s+j} &= (\mathrm{FFT}_{\omega^{m_s}}(a_j, a_{m_s+j}, \ldots, a_{n-m_s+j}))_{[i]_s} \\ x_{p,i} &= \hat{a}_{[i]_p} \\ \hat{a}_i &= x_{p,[i]_p} \end{aligned}$$

Transformation de Fourier Tronquée

- La transformation à longueur $l \leqslant n = 2^p$

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

- Calcul



- Complexité

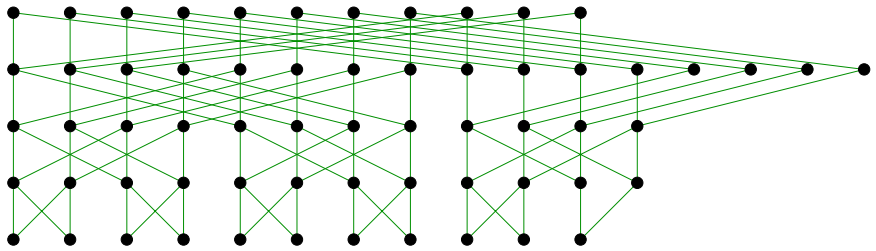
Théorème. *La T.F.T. de* $(a_0, \ldots, a_{l-1})$ *par rapport à* ω *se calcule utilisant* $l\,p + n$ *additions-soustractions et* $\lceil (l\,p+n)/2 \rceil$ *multiplications avec des puissances de* ω.

Transformation de Fourier Tronquée

- La transformation à longueur $l \leqslant n = 2^p$

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

- Calcul



- Complexité

Théorème. *La T.F.T. de* $(a_0, \ldots, a_{l-1})$ *par rapport à* ω *se calcule utilisant* $l\,p + n$ *additions-soustractions et* $\lceil (l\,p+n)/2 \rceil$ *multiplications avec des puissances de* ω.

Transformation inverse

- Observation fondamentale sur la relation de croisement

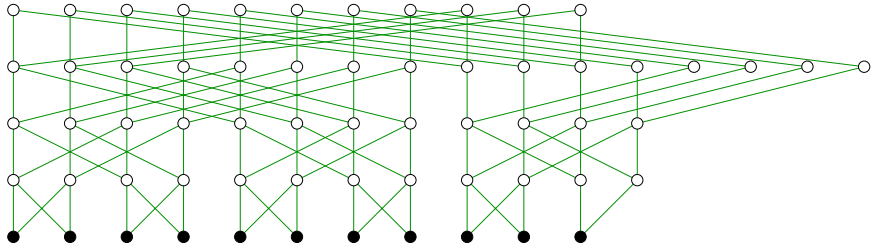
$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

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

- $x_0 = x_1 + \omega^i\, y_1$ 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 $y_0 = x_0 - 2\,\omega^i\, y_1$

Transformation inverse

- Le retour de la T.F.T.

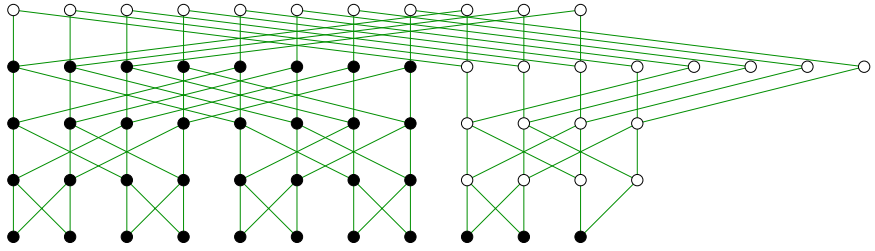


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

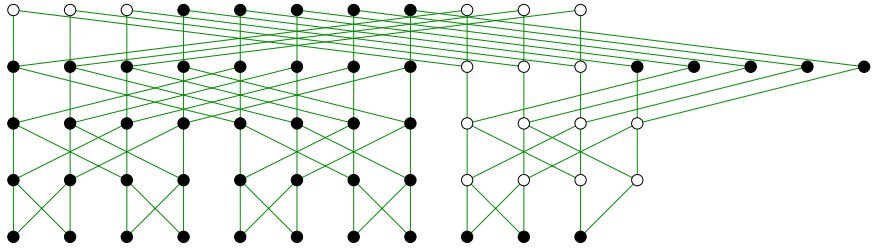


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

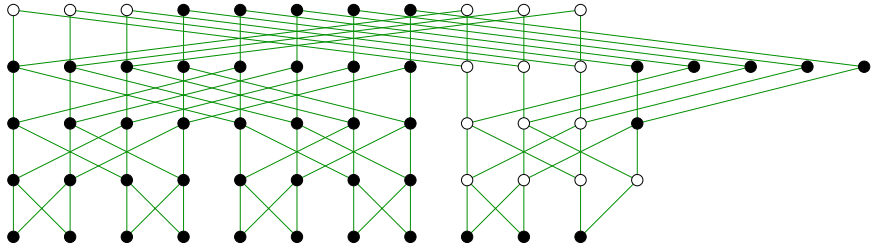


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

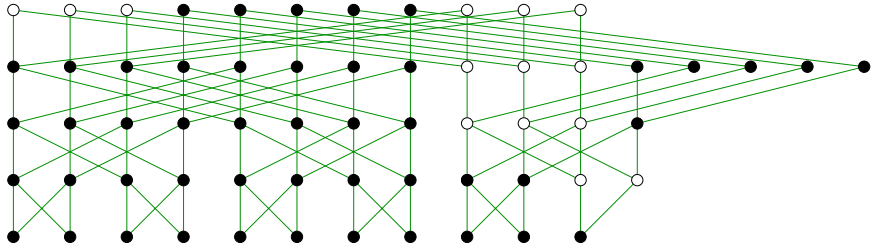


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

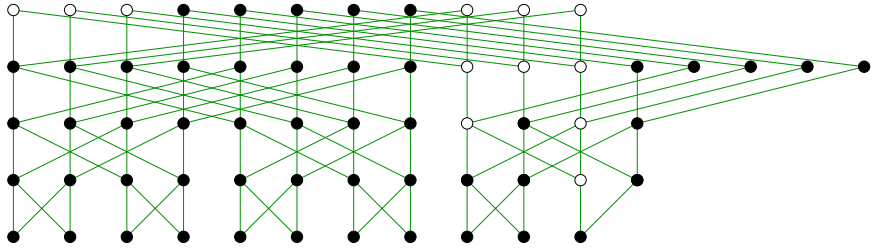


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

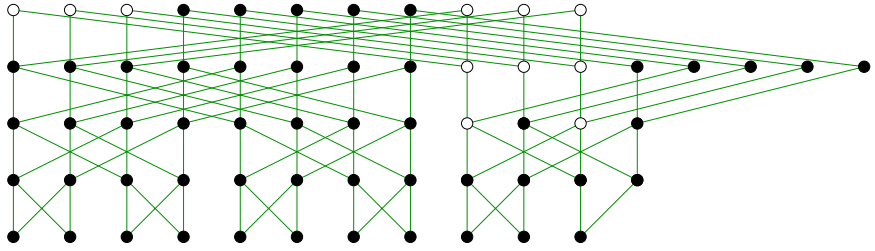


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

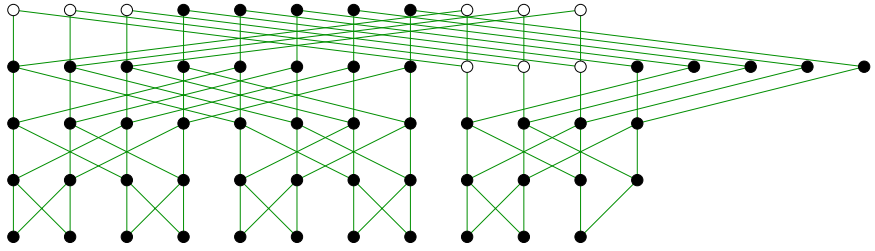


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

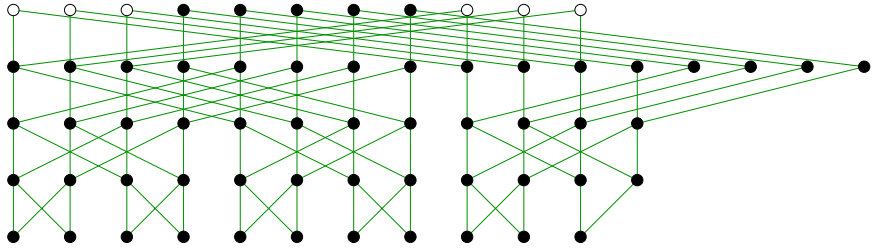


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.

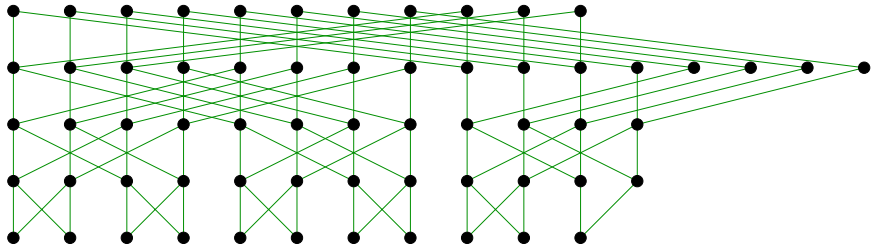


- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Transformation inverse

- Le retour de la T.F.T.



- Complexité

Théorème. *On peut retrouver* $(a_0, ..., a_{l-1})$ *à partir de sa T.F.T. par rapport à* ω *en utilisant* $l\ p + n$ *additions-soustractions,* $\lceil (l\ p + n)\ /\ 2 \rceil$ *multiplications avec des puissances de* ω *et* $2\,n$ *décalages.*

Remarques

- Compatibilité avec Schönhage-Strassen
  - Toutes les multiplications par des puissances de ω.
- Généralisation au cas $\frac{1}{2} \notin \mathcal{R}$

  Pour j avec $j^3 = 1$, étudier :

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & j & j^2 \\ 1 & j^2 & j \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \\ c_0 \end{pmatrix}$$

Remarques

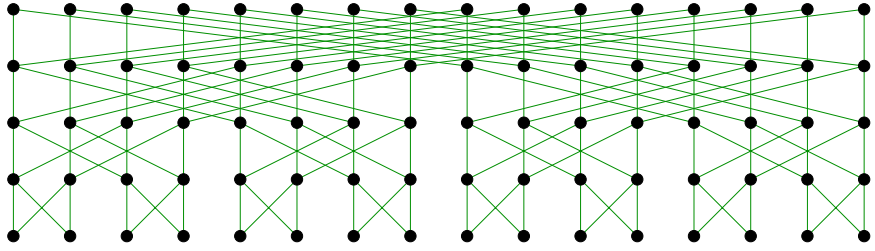
- Compatibilité avec Schönhage-Strassen
  - Toutes les multiplications par des puissances de ω.
- Généralisation au cas $\frac{1}{2} \notin \mathcal{R}$

  Pour j avec $j^3 = 1$, étudier :

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & j & j^2 \\ 1 & j^2 & j \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^i & 0 \\ 0 & 0 & \omega^{2i} \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \\ c_0 \end{pmatrix}$$

Remarques

- T.F.T. par rapport à sous-ensembles $\{0, ..., n-1\}$

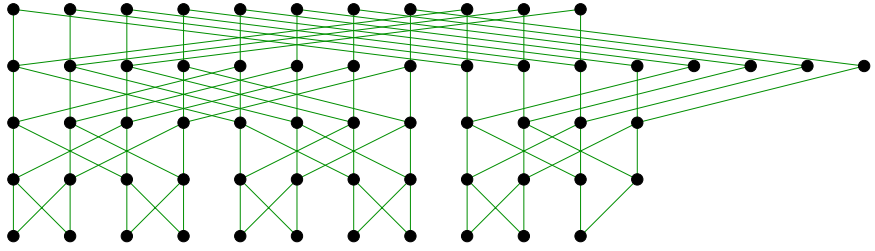


- Note théorique pour $n \to \infty$
  - Suite $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ avec $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ pour tout p avec $i < 2^p$.
  - T.F.L. d'une suite $a_0, a_1, a_2, ...$ avec $\rho(\sum_i a_i z^i) > 1$:

$$a(\omega^{[0]}), a(\omega^{[1]}), a(\omega^{[2]}), ...$$

Remarques

- T.F.T. par rapport à sous-ensembles $\{0, ..., n-1\}$

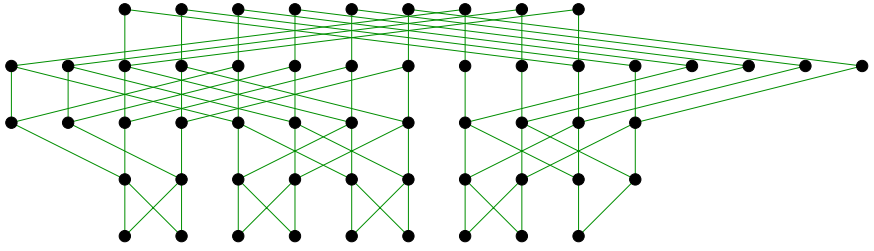


- Note théorique pour $n \to \infty$
  - Suite $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ avec $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ pour tout p avec $i < 2^p$.
  - T.F.L. d'une suite $a_0, a_1, a_2, ...$ avec $\rho(\sum_i a_i z^i) > 1$:

$$a(\omega^{[0]}), a(\omega^{[1]}), a(\omega^{[2]}), ...$$

Remarques

- T.F.T. par rapport à sous-ensembles $\{0, ..., n-1\}$

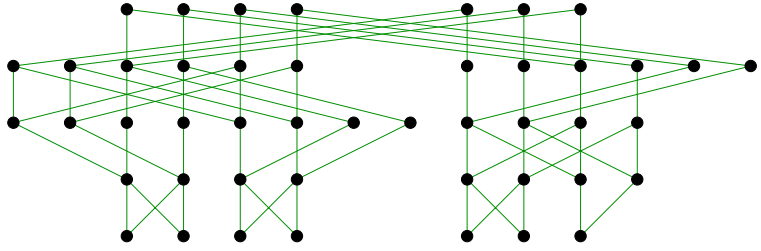


- Note théorique pour $n \to \infty$
  - Suite $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ avec $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2^\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ pour tout p avec $i < 2^p$.
  - T.F.L. d'une suite $a_0, a_1, a_2, ...$ avec $\rho(\sum_i a_i z^i) > 1$:

$$a(\omega^{[0]}), a(\omega^{[1]}), a(\omega^{[2]}), ...$$

Remarques

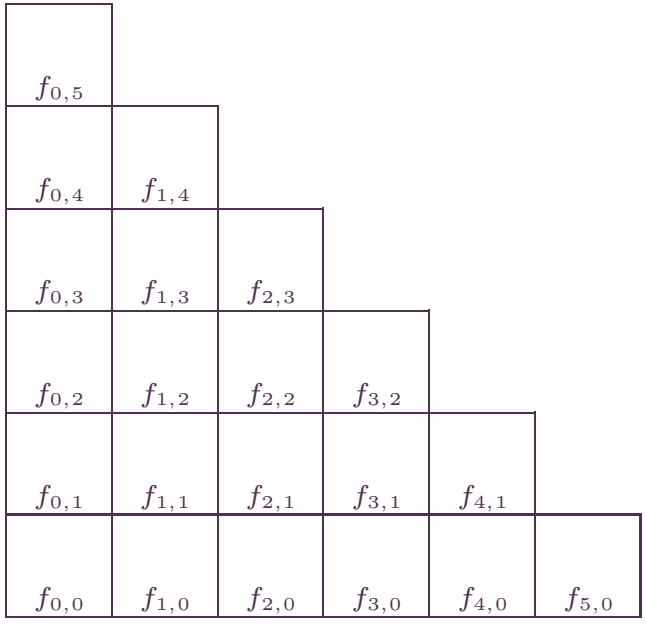
- T.F.T. par rapport à sous-ensembles $\{0, ..., n-1\}$



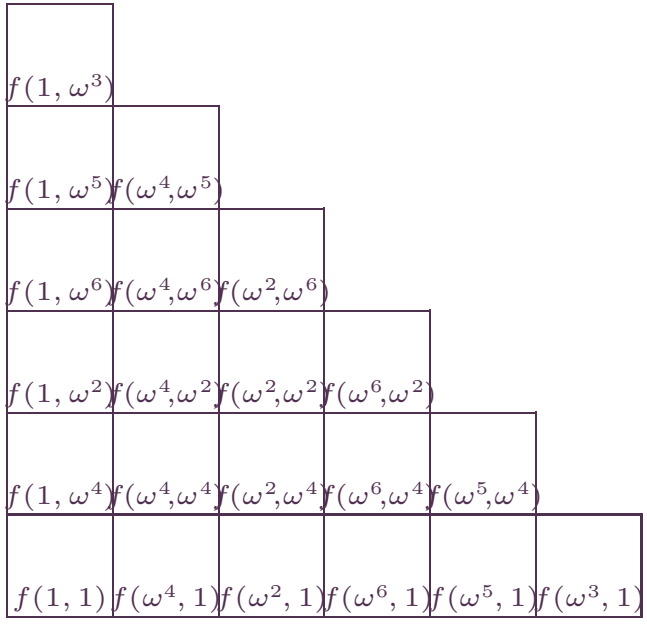
- Note théorique pour $n \to \infty$
  - Suite $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ avec $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2^\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ pour tout p avec $i < 2^p$.
  - T.F.L. d'une suite $a_0, a_1, a_2, ...$ avec $\rho(\sum_i a_i z^i) > 1$:

$$a(\omega^{[0]}), a(\omega^{[1]}), a(\omega^{[2]}), ...$$

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



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



- Complexité si $\mathcal{S} = \{(i_1, \ldots, i_d) \in \mathbb{N}^d : i_1 + \cdots + i_d < n\}$
  - Analyser complexité T.F.T. par rapport à 1 var.
  - $f_{0,i_2,\ldots i_d} \to f_{0,i_2,\ldots i_d}$

$$T_{d,r} \leqslant C\, d \sum_{l=2}^{r} \binom{r-l+d-2}{d-2} l \log l.$$

Théorème. *Supposant que $\mathcal{R}$ admet « sufissamment » de racines 2^p-ième d'unité. Soient $f, g \in \mathcal{R}[z_1, \ldots, z_d]$ des polynômes avec $\deg f + \deg g < r$ et $s = \binom{r+d-1}{r}$. Alors le produit $f\,g$ se calcule en utilisant $O(s \log s)$ opérations dans $\mathcal{R}$.*

- Complexité en général

$$C\,|\mathcal{S}|(\log|\mathcal{S}| + |\partial\mathcal{S}|)$$

- Séries formelles
  - Facteur $O(\log s)$ supplémentaire.