The Truncated Fourier Transform

$\wedge$

Applications

BY

Joris van der Hoeven

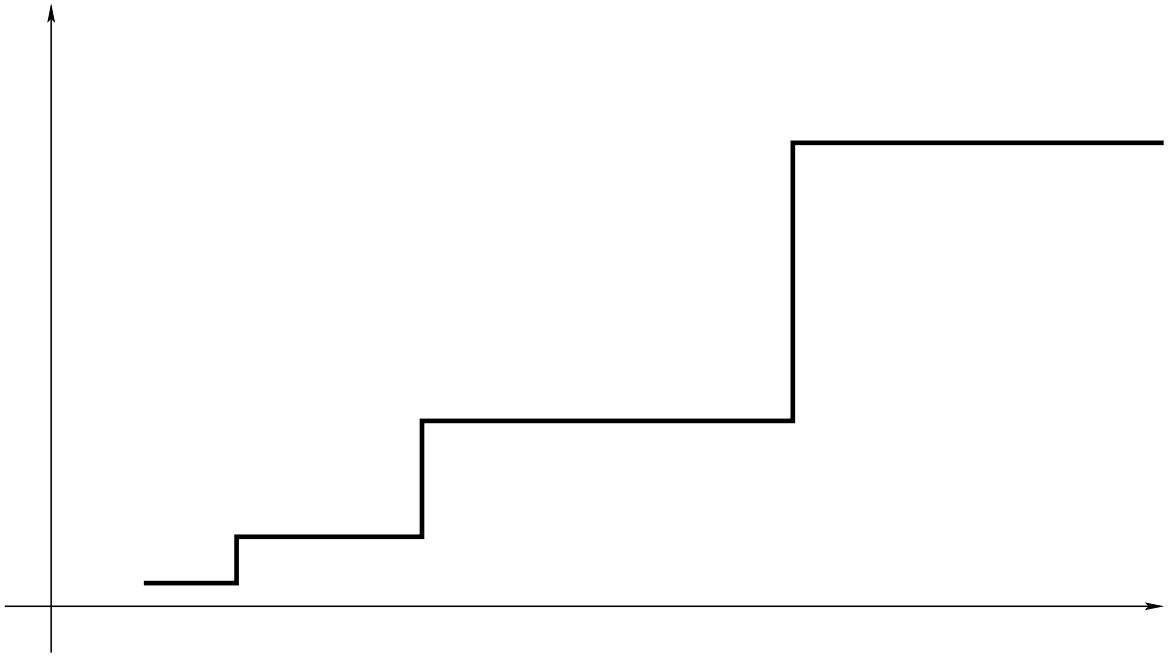
ISSAC 2004

Classical results

- Fast multiplication in $\mathbb{C}[X]$.
  - Cooley-Tuckey, Gauss.
  - Complexity: $O(n \log n)$ operations in $\mathbb{C}$.
- Fast multiplication in $\mathbb{Z}$ and $\mathcal{R}[X]$.
  - Shönhage-Straßen, Cantor-Kaltofen.
  - $\mathcal{R}[x]/(x^{n^2} \pm 1) \cong (\mathcal{R}[y]/(y^n \pm 1))[x]/(x^n - y)$
  - Complexity: $O(n \log n \log^2 n)$ operations in $\mathcal{R}$.
- Fast « sparse » multiplication in $\mathcal{R}[z_1, ..., z_d]$.
  - Canny-Kaltofen-Lakshman.
  - Complexity: $O(s \log^2 s \log \log s)$.
  - Formal power series: Lecerf-Schost, VdH.

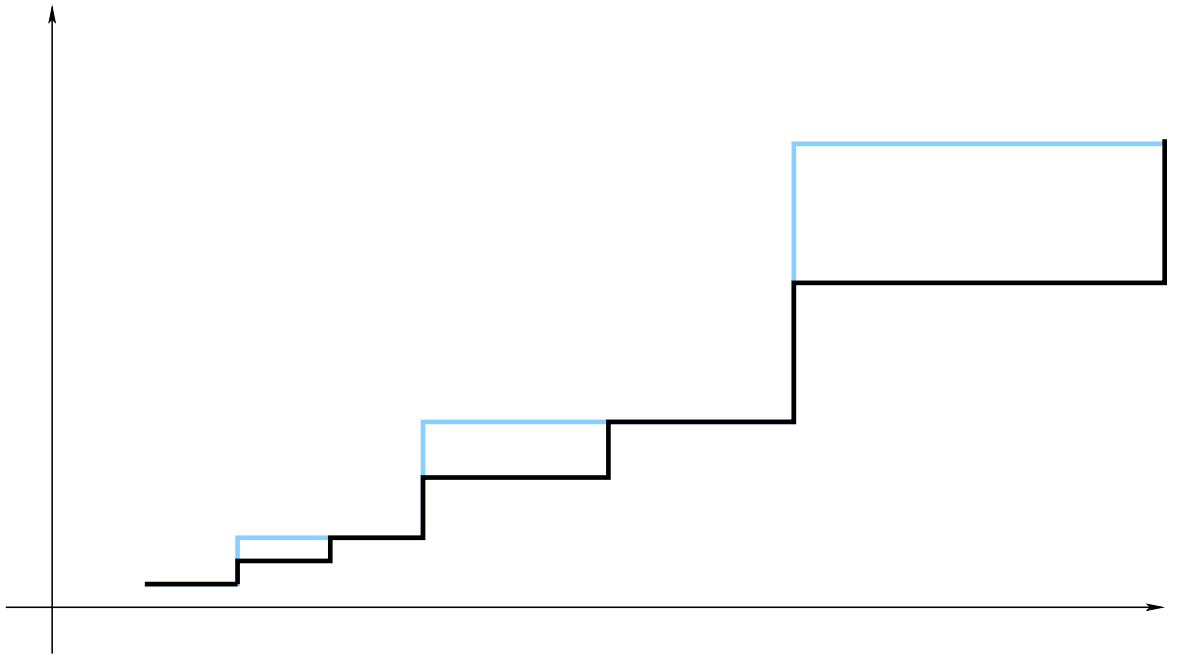
Classical drawbacks

- Jumps in the complexity.



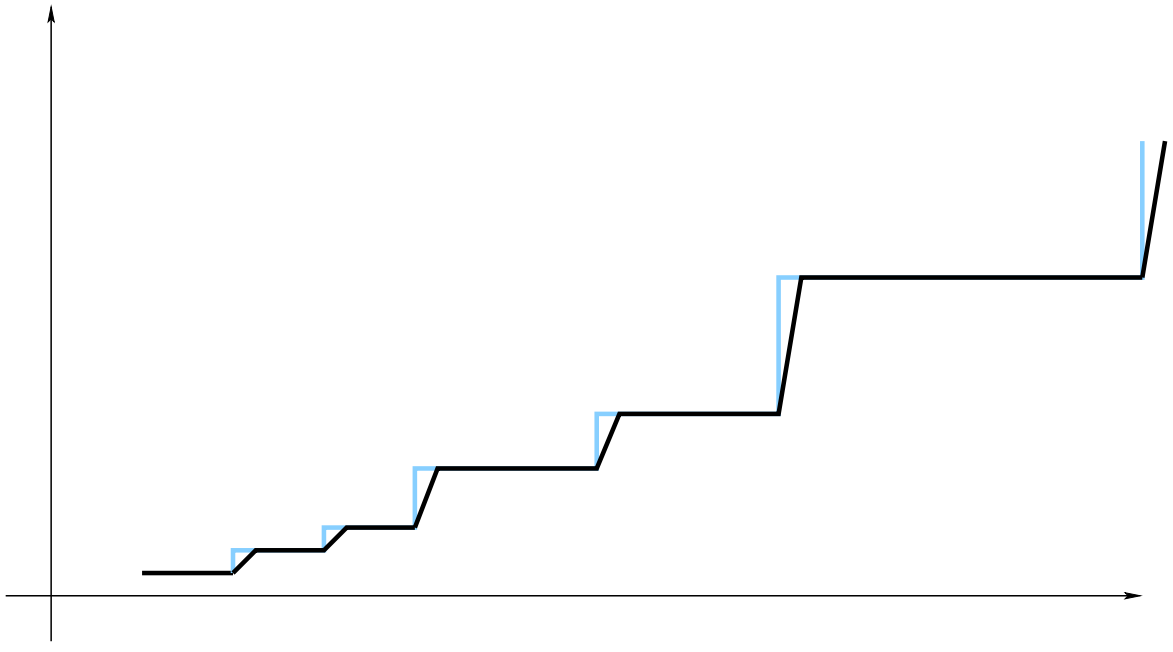
Classical drawbacks

- Jumps in the complexity.



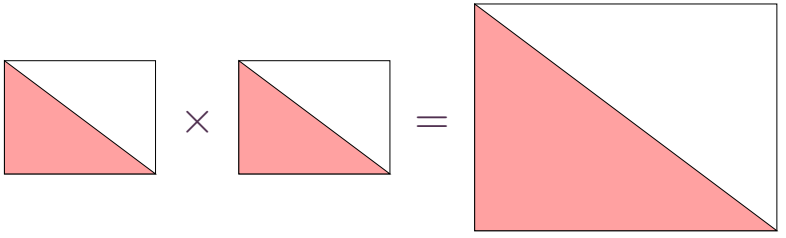
Classical drawbacks

- Jumps in the complexity.



Classical drawbacks

- Unefficiency in higher dimensions.



- Let $P, Q \in \mathbb{C}[z_1, ..., z_d]$ with $\deg P, \deg Q < n$.
- Input size: $s = O(\frac{n^d}{d!})$.
- Naive complexity: $O(d\, n^d \log n) \gg O(s \log s)$.

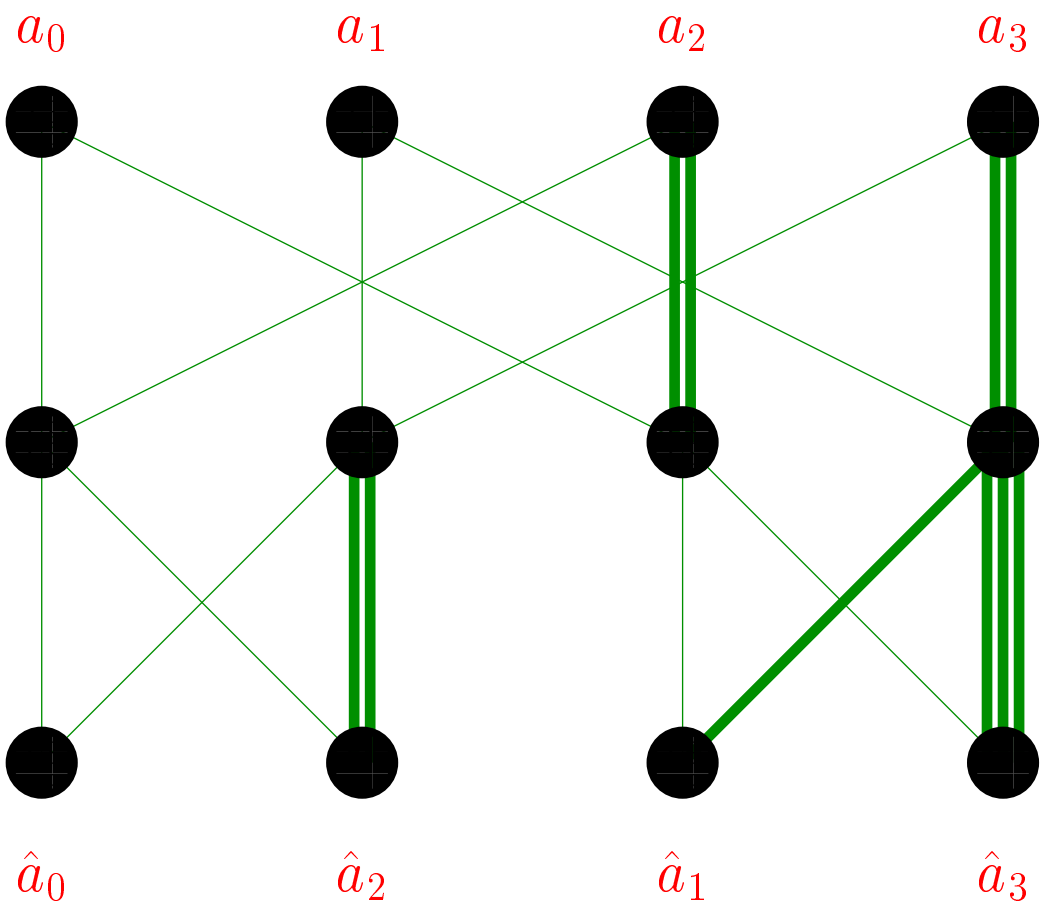
Notations

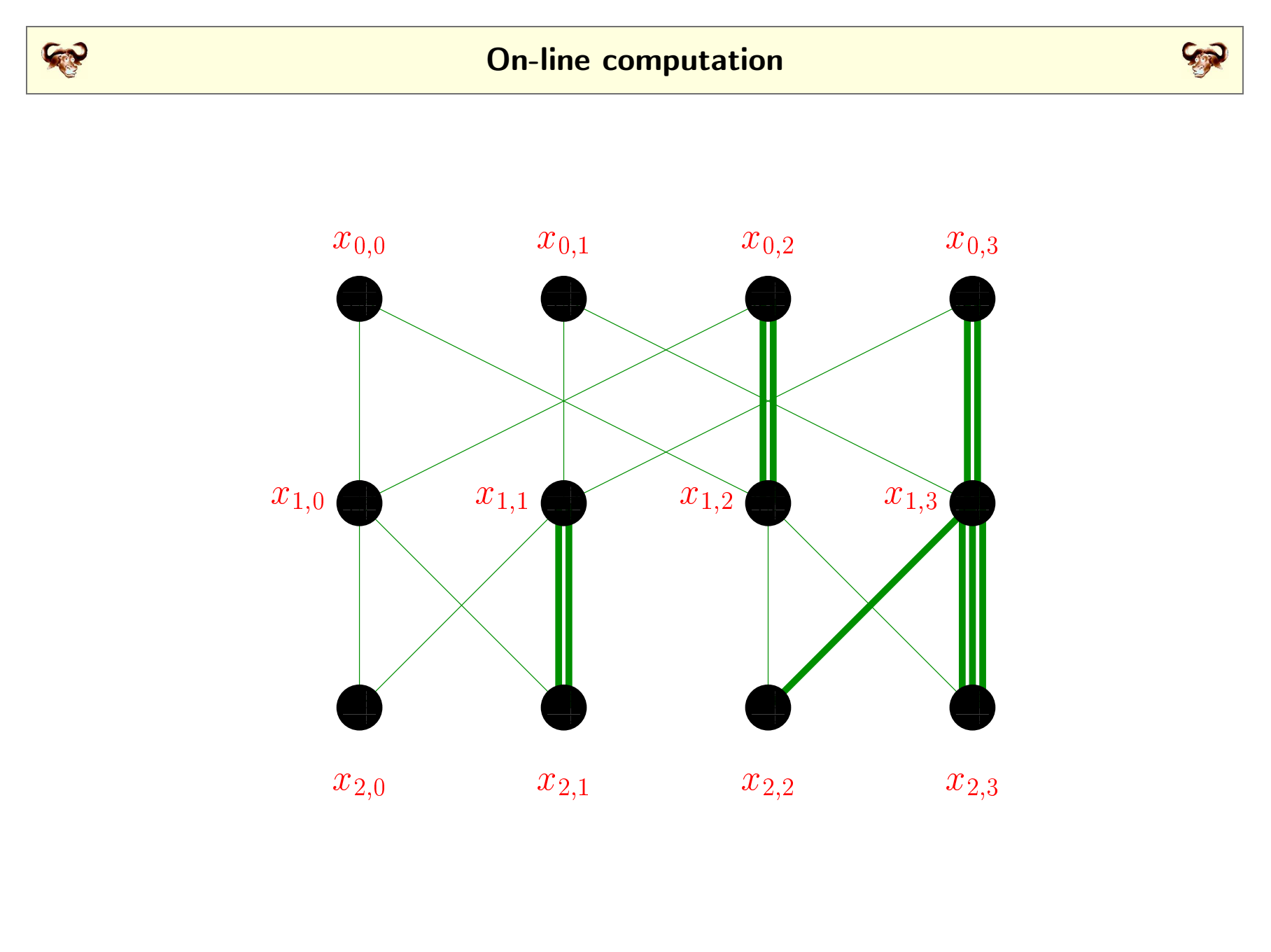
- Notations.
  - $\mathcal{R} \ni \frac{1}{2}$: effective constant ring.
  - $n = 2^p$.
  - $\omega \in \mathcal{R}$ primitive n-th root of unity.
- Definition F.F.T.

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

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

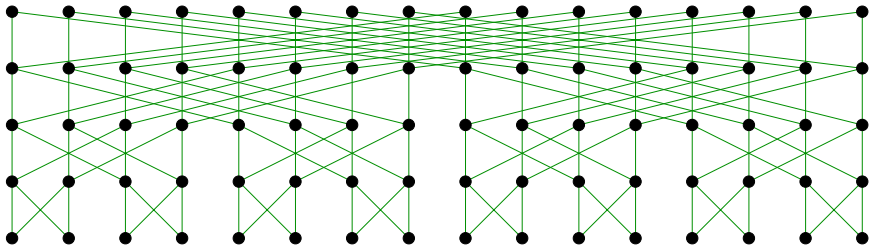
$$\begin{aligned} x_{s,im_s+j} &= (\mathrm{FFT}_{\omega^{m_s}}(a_j, a_{m_s+j}, \ldots, a_{n-m_s+j}))_{[i]_s} \\ x_{p,i} &= \hat{a}_{[i]_p} \\ \hat{a}_i &= x_{p,[i]_p} \end{aligned}$$

The Truncated Fourier Transform

- 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

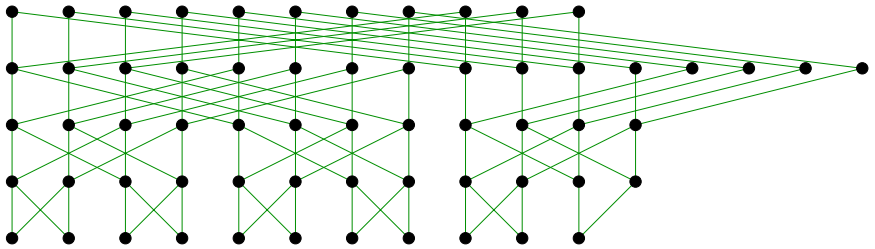
Theorem. *The T.F.T. of* $(a_0, \ldots, a_{l-1})$ *w.r.t.* ω *can be computed using* $l\,p + n$ *additions-subtractions and* $\lceil (l\,p + n)/2 \rceil$ *multiplications with powers of* ω.

The Truncated Fourier Transform

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

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

- Computation



- Complexity

Theorem. *The T.F.T. of* $(a_0, ..., a_{l-1})$ *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.

Inverse transformation

- Observation on the cross relation

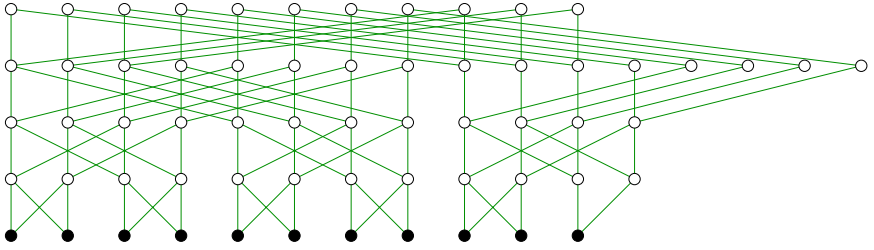
$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega^i \\ 1 & -\omega^i \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

$\forall \epsilon, \delta \in \{0,1\}$: (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 $y_0 = x_0 - 2\,\omega^i\, y_1$

Inverse transformation

- The inverse T.F.T.

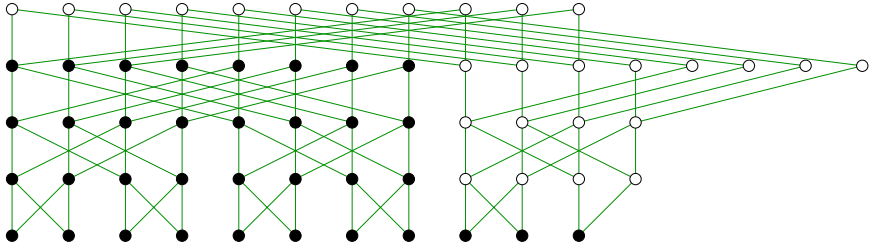


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

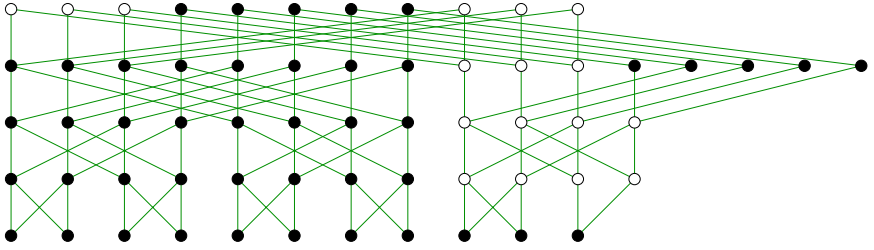


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

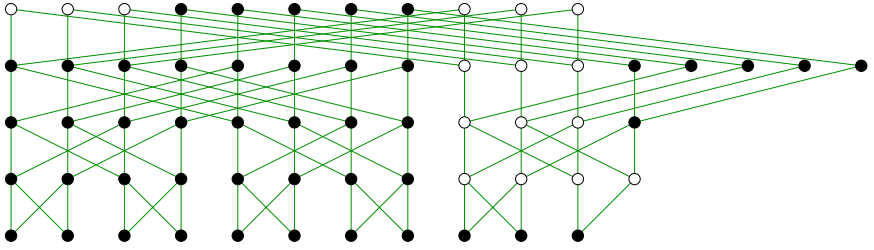


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

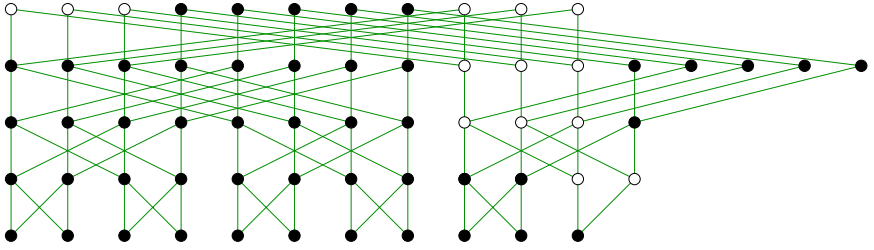


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

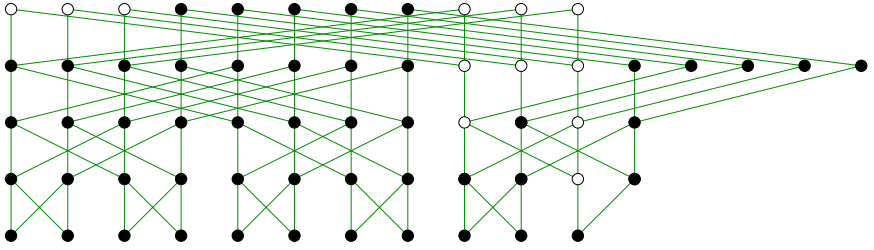


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

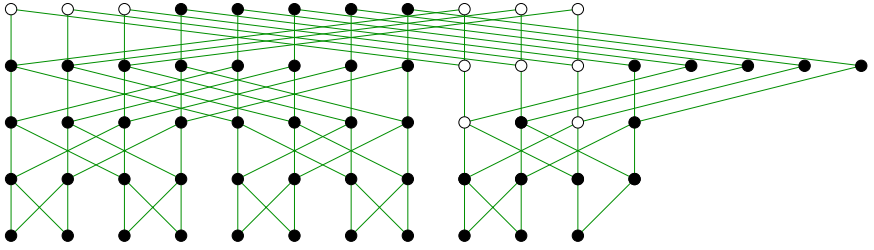


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

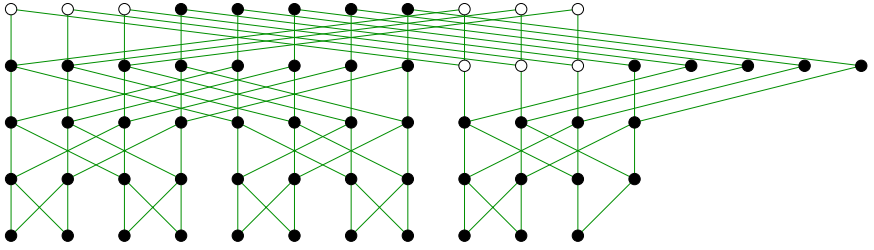


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

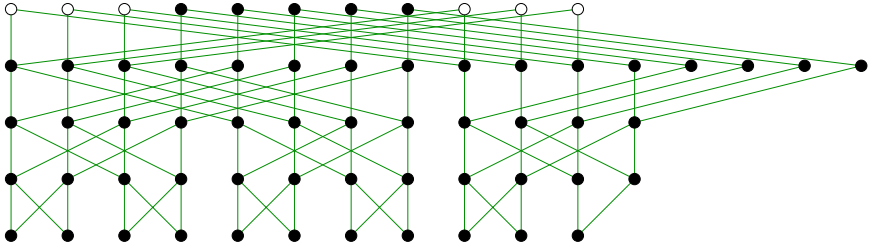


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.

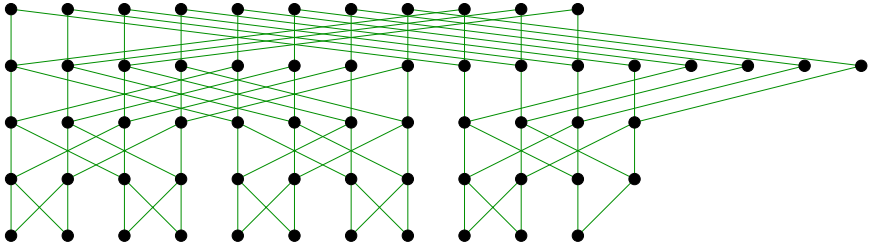


- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Inverse transformation

- The inverse T.F.T.



- Complexity

Theorem. *One may recover* $(a_0, ..., a_{l-1})$ *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.*

Remarks

- Compatibility with Schönhage-Strassen
  - All multiplications are by powers of ω.
- Generalization to the case $\frac{1}{2} \notin \mathcal{R}$

  For j with $j^3 = 1$, study:

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

Remarks

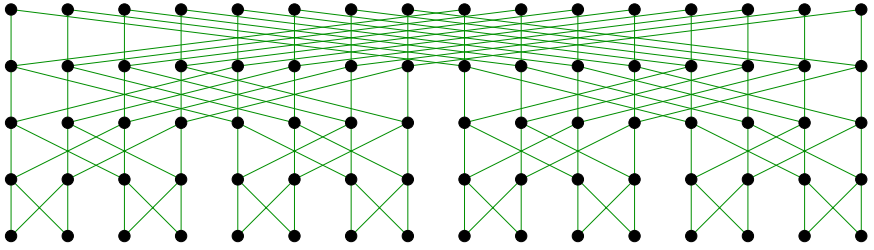
- Compatibility with Schönhage-Strassen
  - All multiplications are by powers of ω.
- Generalization to the case $\frac{1}{2} \notin \mathcal{R}$

  For j with $j^3 = 1$, study:

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

Remarks

- T.F.T. with respect to subsets $\{0, ..., n-1\}$

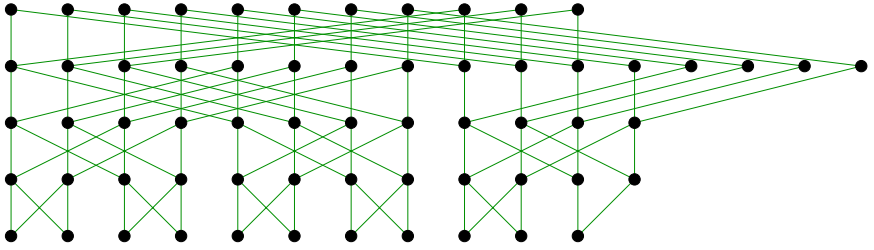


- Theoretical note for $n \to \infty$
  - Sequence $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ with $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2^\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ for all p with $i < 2^p$.
  - L.F.T. of $a_0, a_1, a_2, ...$ with $\rho(\sum_i a_i z^i) > 1$:

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

Remarks

- T.F.T. with respect to subsets $\{0, ..., n-1\}$

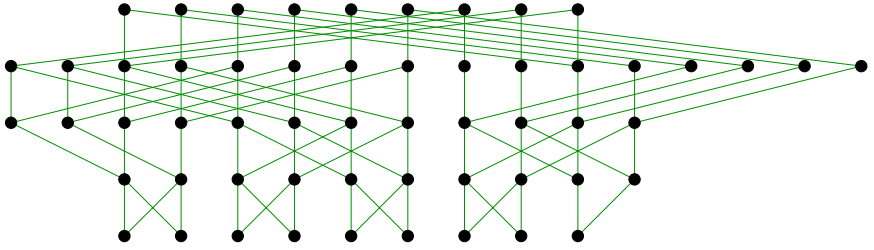


- Theoretical note for $n \to \infty$
  - Sequence $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ with $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2^\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ for all p with $i < 2^p$.
  - L.F.T. of $a_0, a_1, a_2, ...$ with $\rho(\sum_i a_i z^i) > 1$:

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

Remarks

- T.F.T. with respect to subsets $\{0, ..., n-1\}$

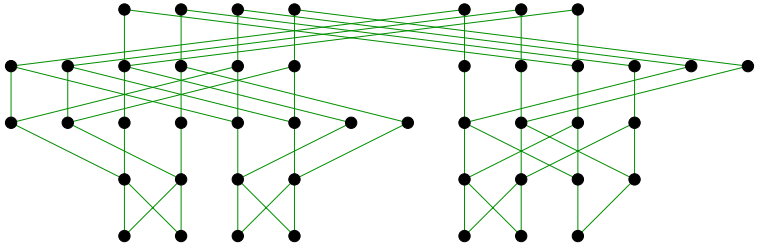


- Theoretical note for $n \to \infty$
  - Sequence $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ with $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2^\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ for all p with $i < 2^p$.
  - L.F.T. of $a_0, a_1, a_2, ...$ with $\rho(\sum_i a_i z^i) > 1$:

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

Remarks

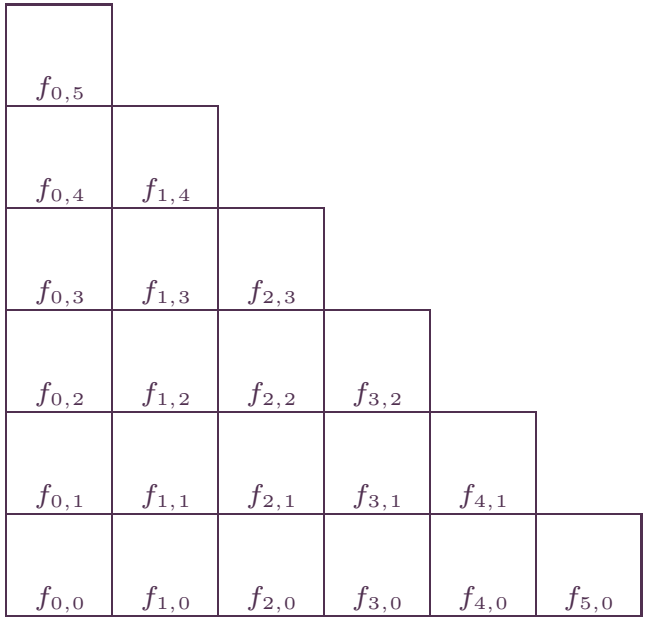
- T.F.T. with respect to subsets $\{0, ..., n-1\}$



- Theoretical note for $n \to \infty$
  - Sequence $\omega_1 = 1, \omega_2, \omega_4, ... \in \mathbb{C}$ with $\omega_{2p}^2 = \omega_p \rightsquigarrow \omega = \omega_{2^\infty}$
  - $\omega^{[i]} := \omega_{2^p}^{[i]_p}$ for all p with $i < 2^p$.
  - L.F.T. of $a_0, a_1, a_2, ...$ with $\rho(\sum_i a_i z^i) > 1$:

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

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



- Complexity if $\mathcal{S}=\{(i_1,\ldots,i_d)\in\mathbb{N}^d\colon i_1+\cdots+i_d<n\}$

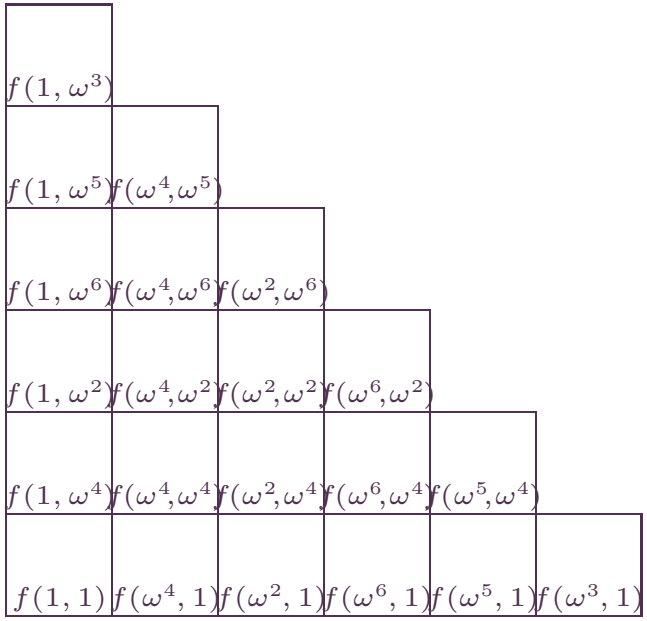
Theorem. *Assume that $\mathcal{R}$ admits « sufficiently many » primitive 2^p-th roots of unity. Let $f,g\in\mathcal{R}[z_1,\ldots,z_d]$ be polynomials with $\deg f+\deg g<r$ and $s=\binom{r+d-1}{r}$. Then the product fg can be computed using $O(s\log s)$ operations in $\mathcal{R}$.*

- Complexity in general

$$O(|\mathcal{S}|\log|\mathcal{S}|+|\delta\mathcal{S}||\partial\mathcal{S}|)$$

- Formal power series
  - Additional $O(\log s)$ overhead.

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



- Complexity if $\mathcal{S}=\{(i_1,\ldots,i_d)\in\mathbb{N}^d\colon i_1+\cdots+i_d<n\}$

Theorem. *Assume that $\mathcal{R}$ admits « sufficiently many » primitive 2^p-th roots of unity. Let $f,g\in\mathcal{R}[z_1,\ldots,z_d]$ be polynomials with $\deg f+\deg g<r$ and $s=\binom{r+d-1}{r}$. Then the product fg can be computed using $O(s\log s)$ operations in $\mathcal{R}$.*

- Complexity in general

$$O(|\mathcal{S}|\log|\mathcal{S}|+|\delta\mathcal{S}||\partial\mathcal{S}|)$$

- Formal power series
  - Additional $O(\log s)$ overhead.