Multiplication rapide I

Joris van der Hoeven

CNRS, École polytechnique

JNCF, Luminy **28 février, 2022**

Motivation I

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

Motivation I

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

Inversion d'une série formelle

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

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

Inversion d'une série formelle

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

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

Inversion d'une série formelle

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

Motivation I

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

Inversion d'une série formelle

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

Motivation I

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

Inversion d'une série formelle

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

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

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

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

Inversion d'une série formelle

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

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

$$
\begin{aligned}
\mathrm{T}(n) &\leqslant \mathrm{T}(m) + 2\,\mathrm{M}(n) + O(n) \\
\mathrm{T}(n) &= O(\mathrm{M}(n))
\end{aligned}
$$

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

Inversion d'une matrice

$$\begin{array}{r|c|c|c|c|} \cline{2-5} r\left\{\vphantom{\Big|}\right. & A & B & 1 & 0 \\ \cline{2-5} & C & D & 0 & 1 \\ \cline{2-5} \end{array}$$

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

Motivation I

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

Inversion d'une matrice

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

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

Motivation I

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

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

Inversion d'une matrice

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

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

Motivation II

La multiplication comme étalon pour la complexité

La multiplication comme étalon pour la complexité

Complexités fondamentales

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

La multiplication comme étalon pour la complexité

Complexités fondamentales

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

La multiplication comme étalon pour la complexité

Complexités fondamentales

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

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

Motivation II

La multiplication comme étalon pour la complexité

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

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

Motivation II

La multiplication comme étalon pour la complexité

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

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

La multiplication comme étalon pour la complexité

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

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

Motivation II

La multiplication comme étalon pour la complexité

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

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

Motivation II

La multiplication comme étalon pour la complexité

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

opération	complexité
division euclidienne	$\sim 2\,\mathrm{I}(N)$
racine carrée	$\sim {}^4\!/\!_3\,\mathrm{I}(N)$
pgcd / ppcm	$O(\mathrm{I}(N)\log N)$
conversion de base	$O\left(\mathrm{I}(N)\,\frac{\log N}{\log\log N}\right)$
calcul de e, π, …	$O(\mathrm{I}(N)\log N)$
DFT, longueur n	$O(\mathrm{I}(n\,b))$
b $\log n$ bits	

Motivation II

La multiplication comme étalon pour la complexité

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

opération	complexité
division euclidienne	$\sim 2\,\mathsf{I}(N)$
racine carrée	$\sim {}^4\!/\!_3\,\mathsf{I}(N)$
pgcd / ppcm	$O(\mathsf{I}(N)\log N)$
conversion de base	$O\left(\mathsf{I}(N)\frac{\log N}{\log\log N}\right)$
calcul de e, π, ...	$O(\mathsf{I}(N)\log N)$
DFT, longueur n	$O(\mathsf{I}(n\,b))$
$b \geqslant \log n$ bits	

Mieux saisir des objects algébriques à travers la multiplication

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

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

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

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

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

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

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

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

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

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

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

Motivation III

Mieux saisir des objects algébriques à travers la multiplication

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

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

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

I Multiplication des entiers jusqu'à 1971

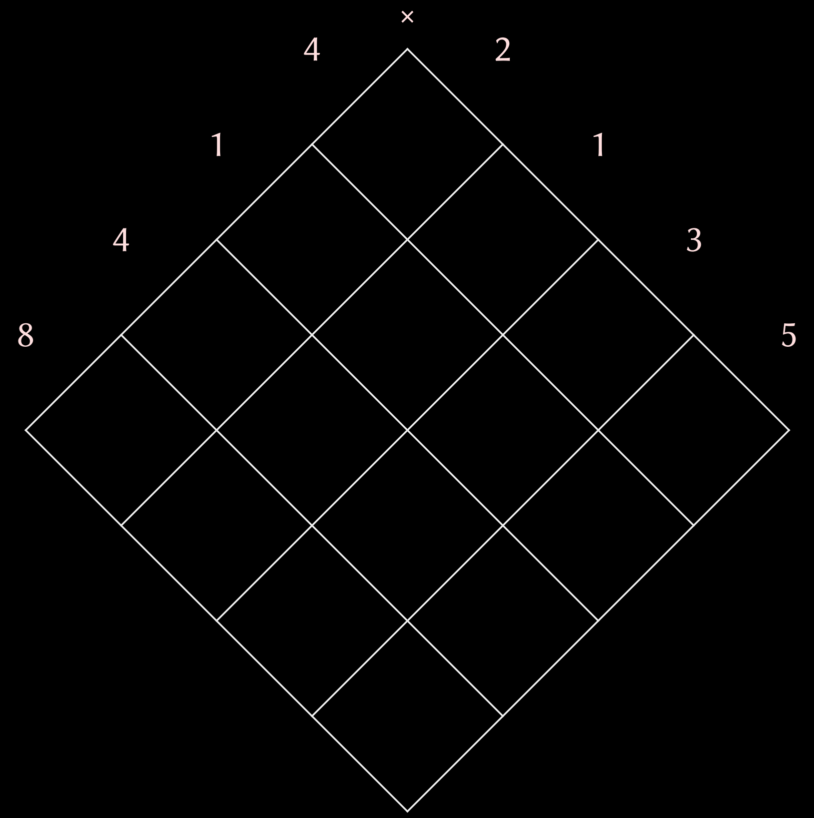
II Boîte à outils pour les FFTs

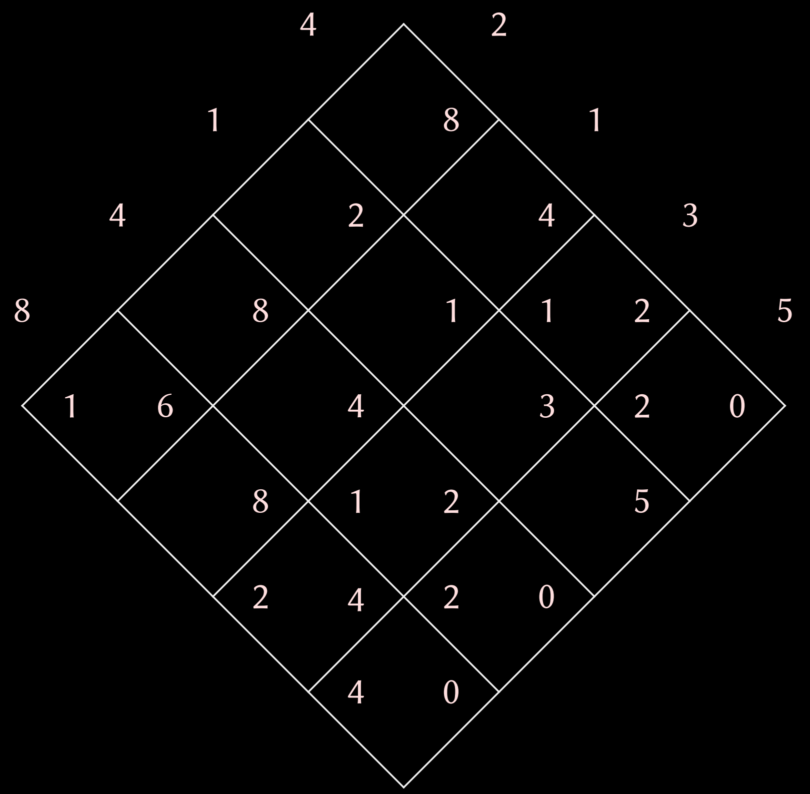
III Multiplication des entiers en temps $O(N \log N)$

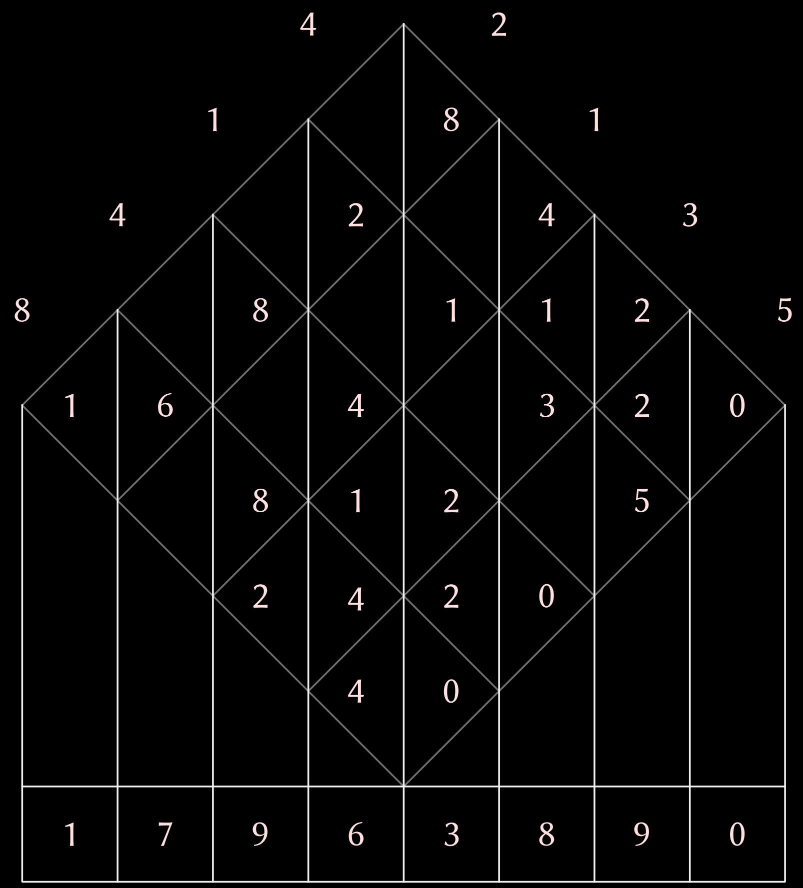
PARTIE I

Multiplication des entiers jusqu'à 1971

8 4 1 4 × 2 1 3 5


×
4
1
4
8
2
1
3
5


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

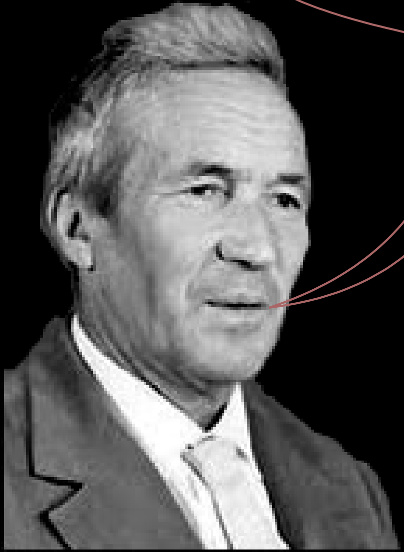

4 2
1 8 1
4 2 4 3
8 8 1 1 2 5
1 6 4 3 2 0
8 1 2 5
2 4 2 0
4 0
1 7 9 6 3 8 9 0

Peut-on faire mieux ?

Peut-on faire mieux ?

$$\mathrm{I}(N) = \Theta(N^2)$$

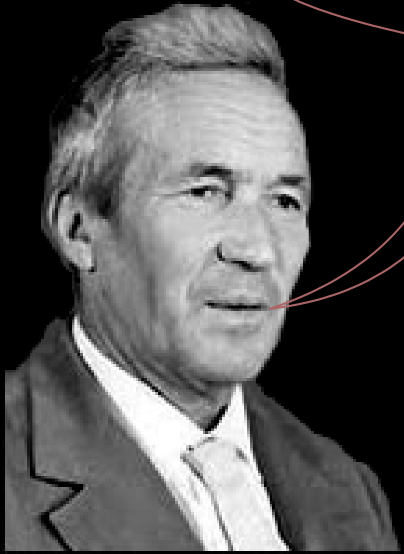
! ?



Peut-on faire mieux ?

$$I(N) = \Theta(N^2)$$

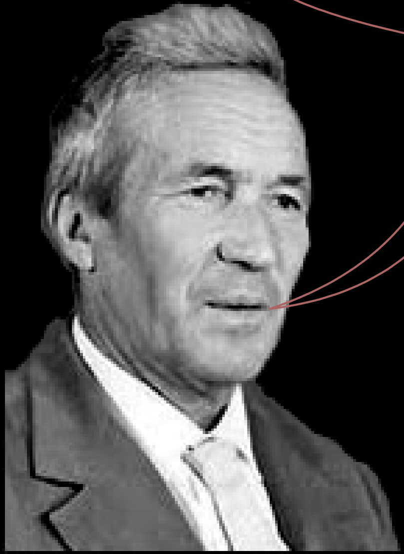
! ?



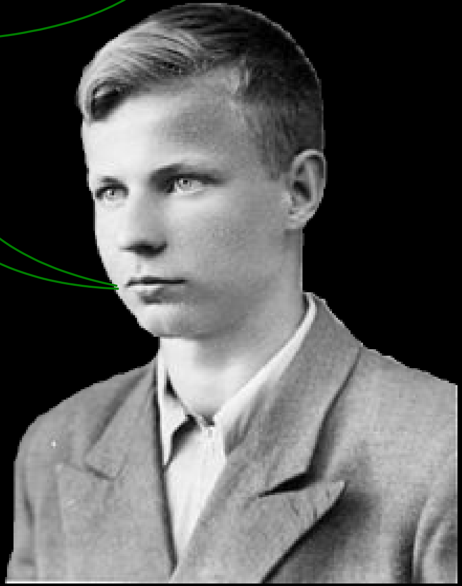
Peut-on faire mieux ?

$$\mathrm{I}(N) = \Theta(N^2)$$

! ?



$$\mathrm{I}(N) = O(N^{\log_2 3})$$



1962

Historique

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

$$13022020 \quad \times \quad 31415926$$

Multiplication de Karatsuba

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

Multiplication de Karatsuba

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

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

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

Multiplication de Karatsuba

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

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

Multiplication de Karatsuba

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

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

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

Multiplication de Karatsuba

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

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

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

Complexité

$$\mathsf{I}(N) \leqslant 3\,\mathsf{I}(N/2) + C\,N$$

Multiplication de Karatsuba

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

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

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

Complexité

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

Multiplication de Karatsuba

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

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

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

Complexité

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

Multiplication de Karatsuba

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

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

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

Complexité

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

Segmentation de Kronecker

$$4627579679788114 \quad \times \quad 4519170871966234$$

$$\rightsquigarrow$$

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

Segmentation de Kronecker

$$4627579679788114 \quad \times \quad 4519170871966234$$

$$\wr$$

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

Substitution de Kronecker

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

$$\wr$$

$$4627000005796000007978000008114 \quad \times \quad 4519000001708000007196000006234$$

Segmentation de Kronecker

$$4627579679788114 \quad \times \quad 4519170871966234$$

$$\wr$$

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

Substitution de Kronecker

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

$$\wr$$

$$4627000005796000007978000008114 \quad \times \quad 4519000001708000007196000006234$$

$$1004003 \quad \times \quad 2001005 \quad = \quad 2009015023015$$

Polynômes cycliques

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

n : longueur de cycle

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

Polynômes cycliques

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

n : longueur de cycle

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

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

Polynômes cycliques

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

n : longueur de cycle

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

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

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

Polynômes cycliques

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

n : longueur de cycle

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

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

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

Résumé jusqu'à présent

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

Transformation de Fourier discrète (DFT)

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

n : longueur de cycle

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

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

n : longueur de cycle

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

Théorème des restes chinois

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

Transformation de Fourier discrète (DFT)

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

n : longueur de cycle

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

Théorème des restes chinois

$$\begin{aligned} (x^n - 1) &= \prod_{0 \leqslant k < n} (x - \omega^k) \\ \mathbb{K}[x]/(x^n - 1) &\cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \end{aligned}$$

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

n : longueur de cycle

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

Théorème des restes chinois

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

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

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

n : longueur de cycle

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

Théorème des restes chinois

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

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

Transformation de Fourier discrète

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

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

n : longueur de cycle

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

Théorème des restes chinois

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

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

Transformation de Fourier discrète

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

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

Application à la multiplication

$$
\begin{tikzcd}
P \in \mathbb{K}[x]/(x^n-1) \arrow[d, "\mathrm{DFT}"] & & Q \in \mathbb{K}[x]/(x^n-1) \arrow[d, "\mathrm{DFT}"] \\
\hat{P} \in \bigoplus_{0\leqslant k<n} \mathbb{K}[x]/(x-\omega^k) \arrow[dr] & & \hat{Q} \in \bigoplus_{0\leqslant k<n} \mathbb{K}[x]/(x-\omega^k) \arrow[dl] \\
& \hat{P}\hat{Q} \in \bigoplus_{0\leqslant k<n} \mathbb{K}[x]/(x-\omega^k) \arrow[d, "\mathrm{DFT}^{-1}"] & \\
& PQ \in \mathbb{K}[x]/(x^n-1) &
\end{tikzcd}
$$

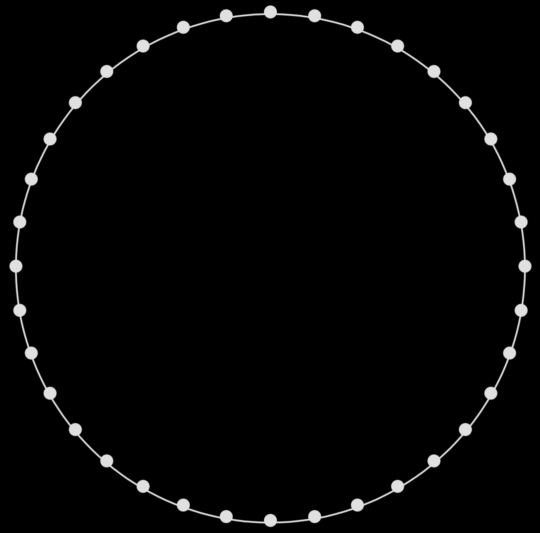
Application à la multiplication

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

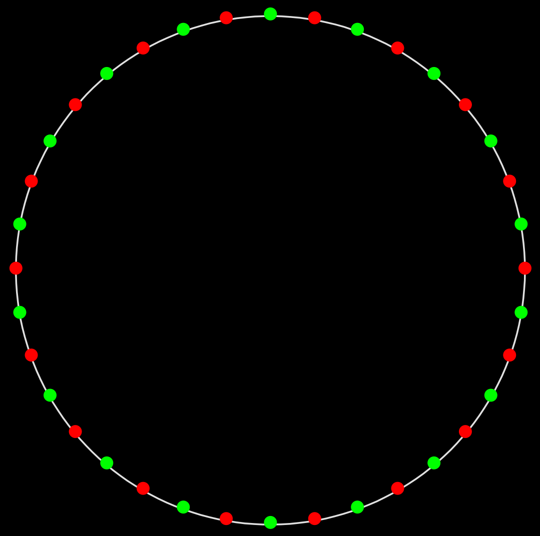
Résumé jusqu'à présent

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

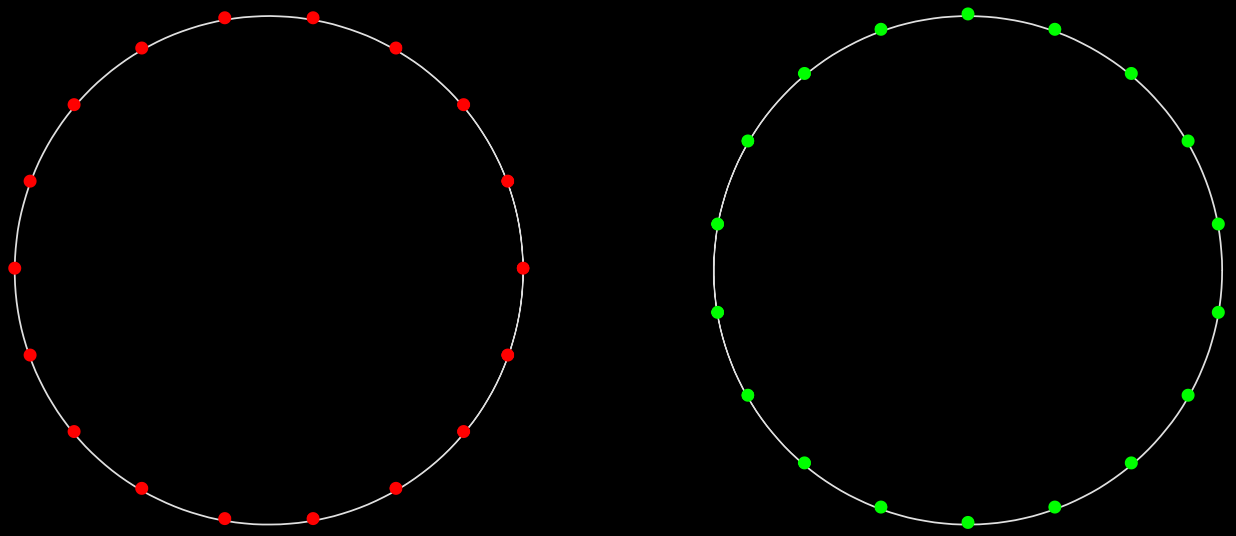
Rendre les DFTs efficaces : FFT



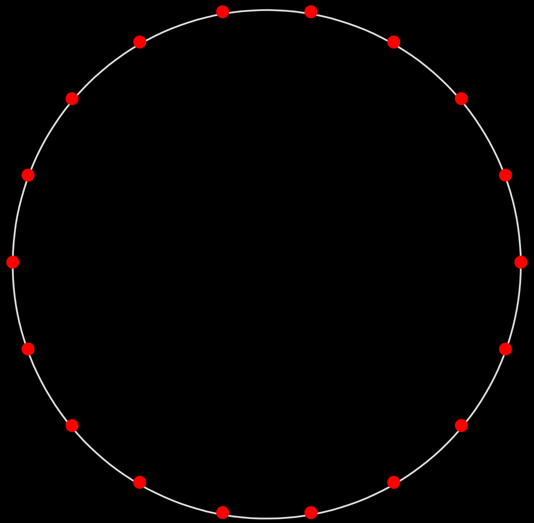
Rendre les DFTs efficaces : FFT

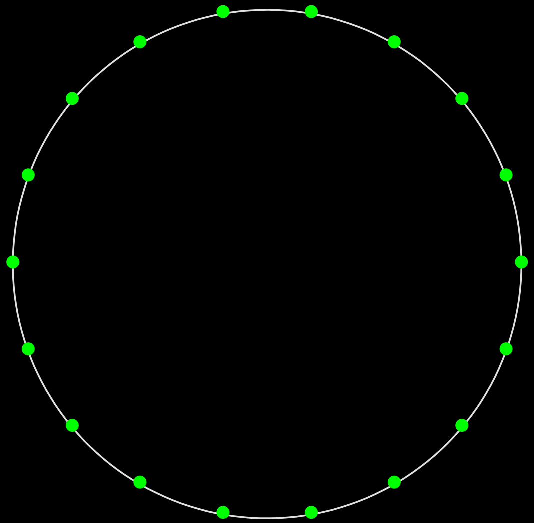


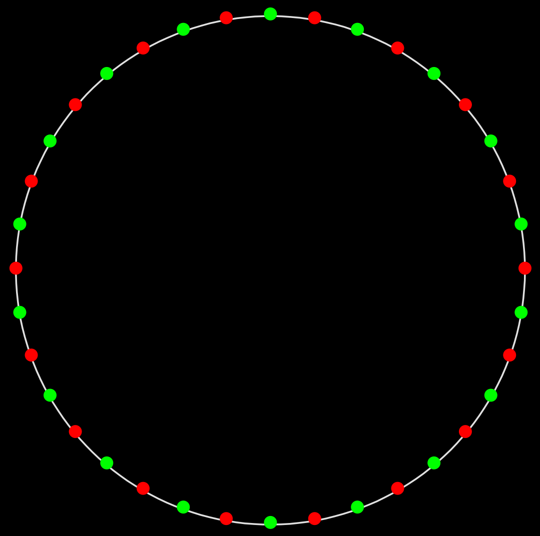
Rendre les DFTs efficaces : FFT



Rendre les DFTs efficaces : FFT

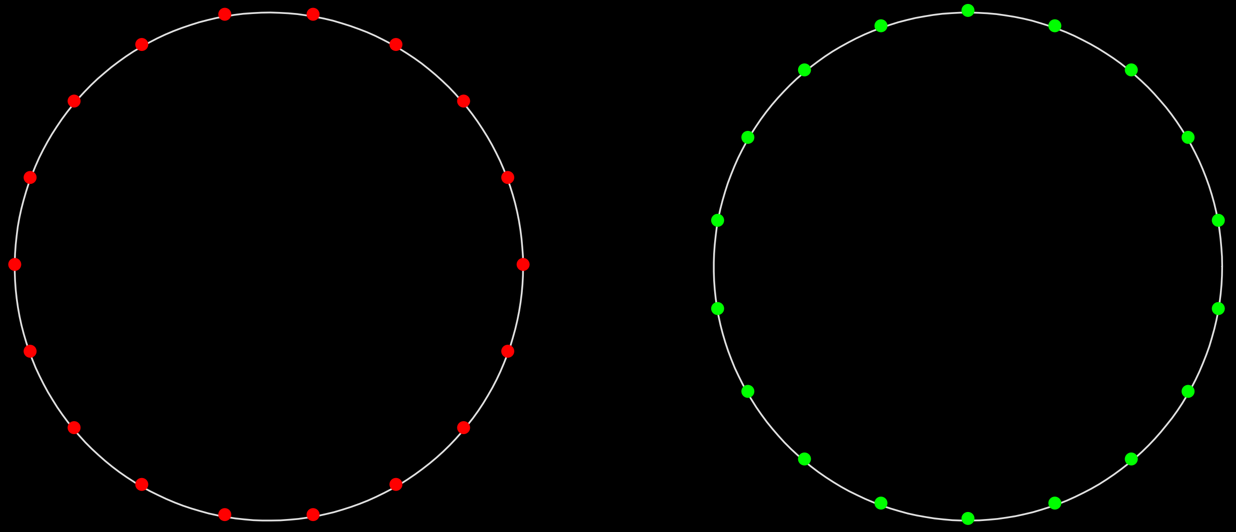






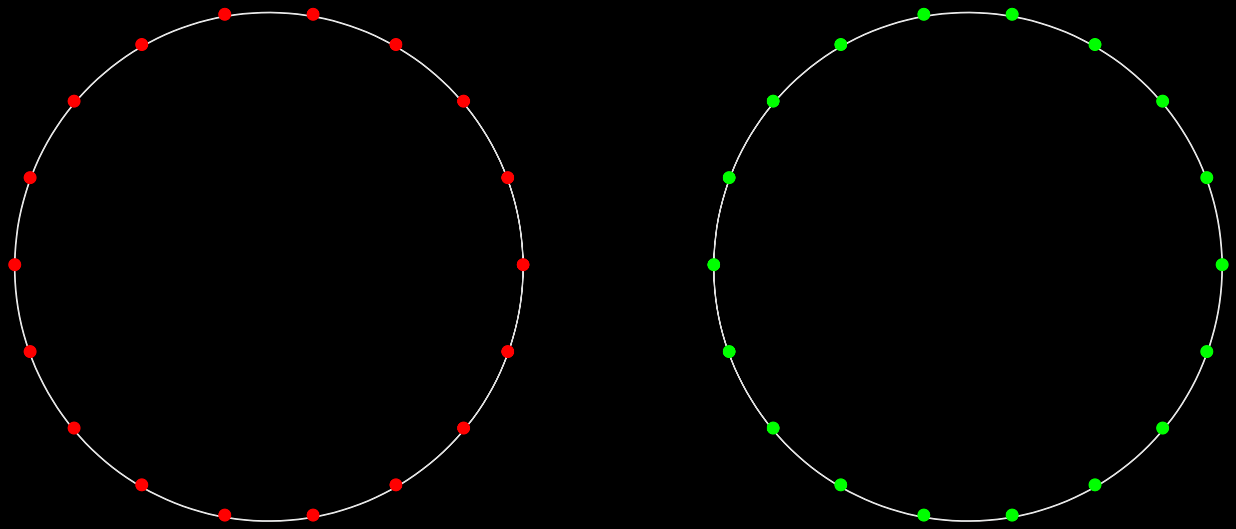
$$\mathbb{K}[x]/(x^{2n}-1)$$

Rendre les DFTs efficaces : FFT



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

Rendre les DFTs efficaces : FFT



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

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

$$\tilde{x} = \omega x$$

$$\omega^n = -1$$

Analyse de complexité

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

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

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

$$\cong$$

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

Analyse de complexité

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

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

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

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

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

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

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

Comment choisir $\mathbb{K}$?

Comment choisir $\mathbb{K}$?

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

Comment choisir $\mathbb{K}$?

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

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

Comment choisir $\mathbb{K}$?

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

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

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

Comment choisir $\mathbb{K}$?

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

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

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

Analyse de complexité

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

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

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

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

Analyse de complexité

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

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

Retour à la multiplication des entiers

Comment choisir $\mathbb{K}$?

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

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

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

Analyse de complexité

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

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

Comment choisir $\mathbb{K}$?

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

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

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

Analyse de complexité

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

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

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

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

PARTIE II

Boîte à outils pour les FFTs

FFT de Cooley–Tukey généralisée

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

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

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

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

n_2 DFTs de longueur n_1

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

FFT de Cooley–Tukey généralisée

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

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

n_2 DFTs de longueur n_1

n multiplications par des puissances de ω

FFT de Cooley–Tukey généralisée

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

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

n_2 DFTs de longueur n_1

n multiplications par des puissances de ω

n_1 DFTs de longueur n_2

FFT de Cooley–Tukey généralisée

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

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

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

FFT de Good

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

FFT de Good

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

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

FFT de Good

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

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

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

FFT de Good

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

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

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

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

FFT de Good

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

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

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

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

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

FFT de Good

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

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

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

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

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

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

DFT de longueur $p=5$

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

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

Réduction de Rader

DFT de longueur $p = 5$

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

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

Réduction de Rader

DFT de longueur $p = 5$

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

$$1 = 2^0, \qquad 2 = 2^1, \qquad 3 = 2^3, \qquad 4 = 2^2 \qquad \pmod 5$$

DFT de longueur $p = 5$

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

Réduction de Rader

DFT de longueur $p = 5$

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

DFT de longueur $p = 5$

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

Réduction de Rader

DFT de longueur $p = 5$

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

$$\Updownarrow$$

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

$$\text{modulo } x^4 - 1$$

Réduction de Rader

DFT de longueur $p = 5$

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

$$\Updownarrow$$

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

$$\text{modulo } x^4 - 1$$

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

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

$\mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(n)$: quand un argument est fixe

Réduction de Rader

DFT de longueur $p = 5$

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

$$\Updownarrow$$

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

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

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

Réduction de Bluestein

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

Réduction de Bluestein

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

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

Réduction de Bluestein

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

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

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

Réduction de Bluestein

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

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

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

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

Réduction de Bluestein

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

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

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

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

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

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

Réduction de Bluestein

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

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

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

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

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

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

Résumé

$$
\begin{aligned}
\mathrm{M}^{\circ}_{\mathbb{K}}(n) &\leqslant 3\,\mathrm{F}_{\mathbb{K}}(n) + n\,\mathrm{mul}_{\mathbb{K}} && \text{(multiplication FFT)}\\
\mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(n) &\leqslant 2\,\mathrm{F}_{\mathbb{K}}(n) + n\,\mathrm{mul}_{\mathbb{K}} && \\
\mathrm{F}_{\mathbb{K}}(n) &\leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(n) + 2\,n\,\mathrm{mul}_{\mathbb{K}} && \text{(Bluestein)}\\
\mathrm{F}_{\mathbb{K}}(p) &\leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixe}}(p-1) + 2\,n\,\mathrm{add}_{\mathbb{K}} && \text{(Rader)}
\end{aligned}
$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rader

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

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

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

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

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

Rader

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

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

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

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

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

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

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

Rader

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

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

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

FFT « de Frobenius »

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

FFT « de Frobenius »

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

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

FFT « de Frobenius »

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

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

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

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

FFT « de Frobenius »

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

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

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

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

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

FFT « de Frobenius »

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

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

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

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

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

Au final, on gagne un facteur 2

PARTIE III

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

Une construction soigneuse donne

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

Note sur la multiplication de Schönhage–Strassen

Une construction soigneuse donne

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

Une construction soigneuse donne

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

Une construction soigneuse donne

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

Et si…

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

Et si…

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

Et si...

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

Note sur la multiplication de Schönhage–Strassen

Et si…

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

Et si…

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

Objectif suivant :

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

Et si…

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

Objectif suivant :

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

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

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

Schönhage–Strassen

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

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

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

Schönhage–Strassen

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

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

Nussbaumer

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

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

Transformations polynomiales de Nussbaumer

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

Schönhage–Strassen

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

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

Nussbaumer

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

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

Objectif suivant :

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

Restes chinois à la Good

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

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

FFT de Good

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

Restes chinois à la Good

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

FFT de Good

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

Cadre

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

Restes chinois à la Good

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

FFT de Good

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

Cadre

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

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

Première approche par Rader

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

Première approche par Rader

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

$$\searrow$$

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

Première approche par Rader

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

$$\searrow$$

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

Exemple

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

Première approche par Rader

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

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

Exemple

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

Constante de Linnik

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

Première approche par Rader

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

$$\searrow$$

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

Exemple

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

Constante de Linnik

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

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

Constante de Linnik

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

Théorème

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

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

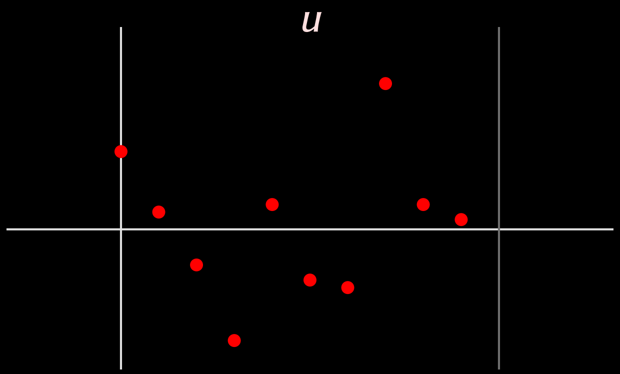
Théorème

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

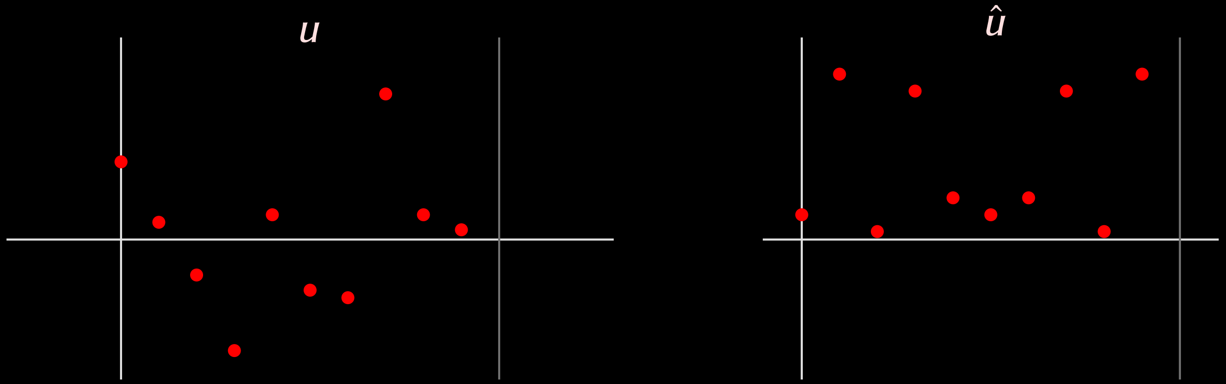
$$\mathsf{M}_{\mathbb{F}_q}(n) = O(n \log q \log(n \log q)),$$

uniformément en q.

Rééchantillonage gaussien

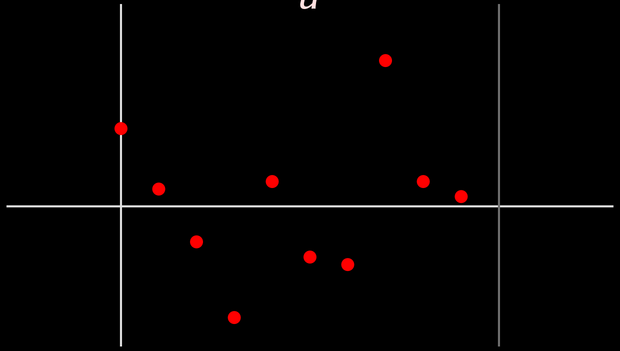


Rééchantillonage gaussien

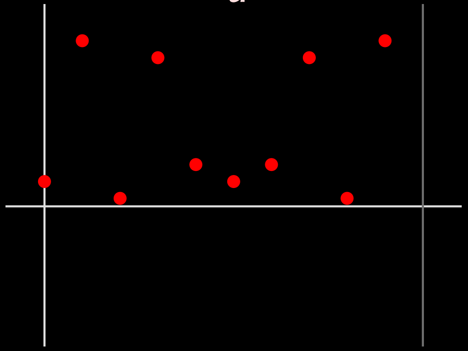


Rééchantillonage gaussien

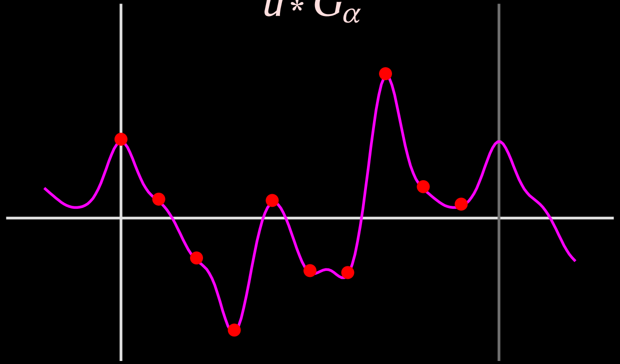
u



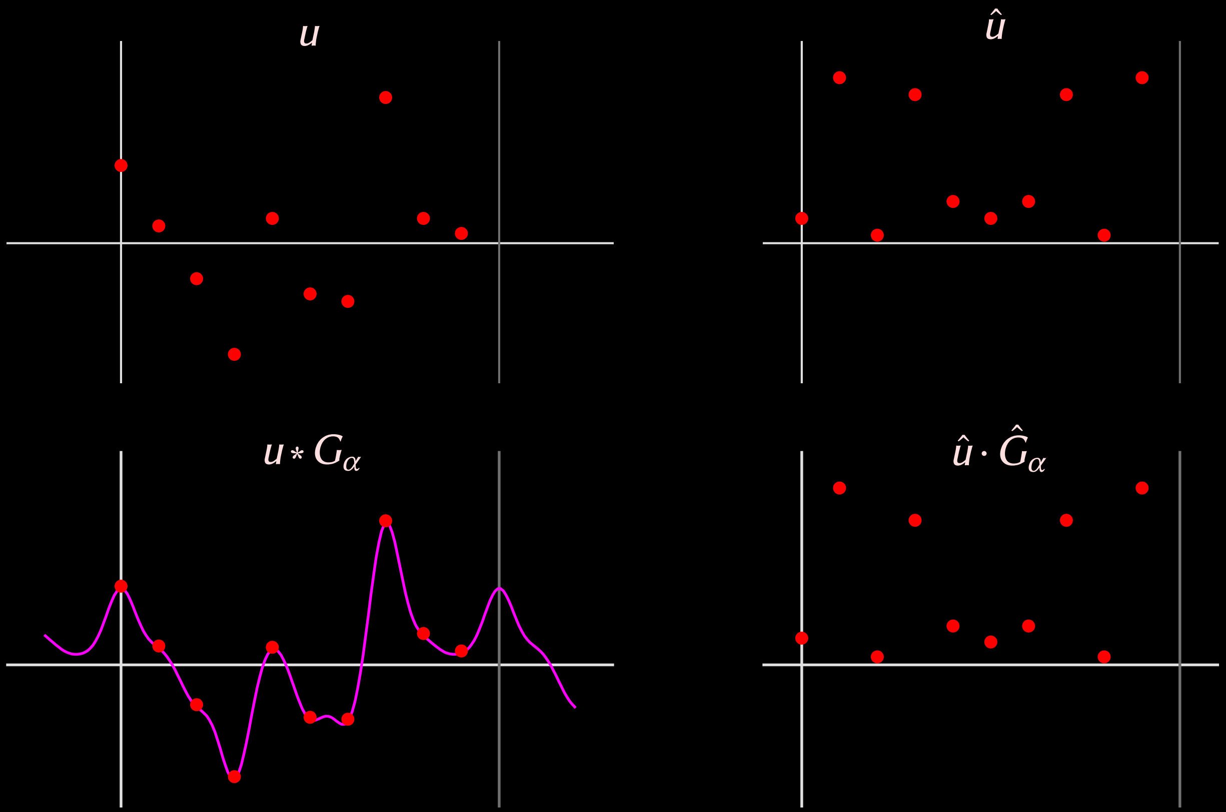
$\hat{u}$



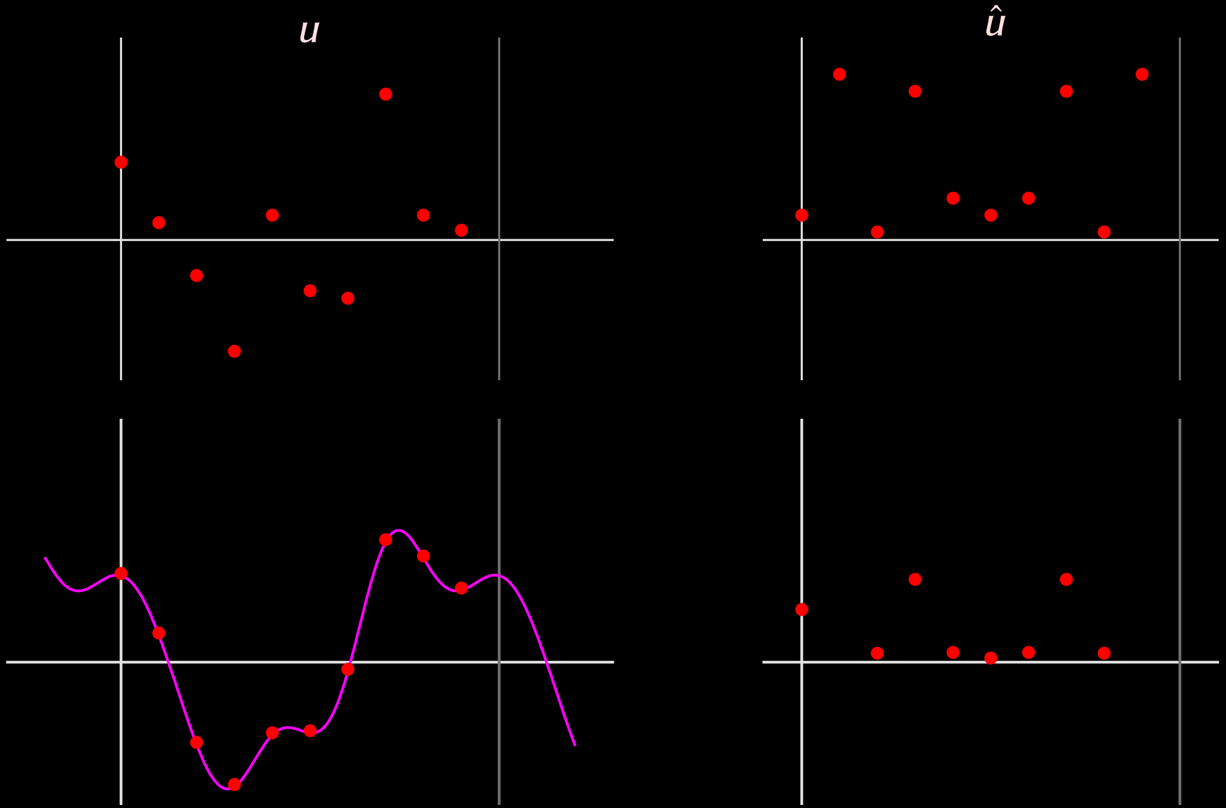
$u * G_\alpha$



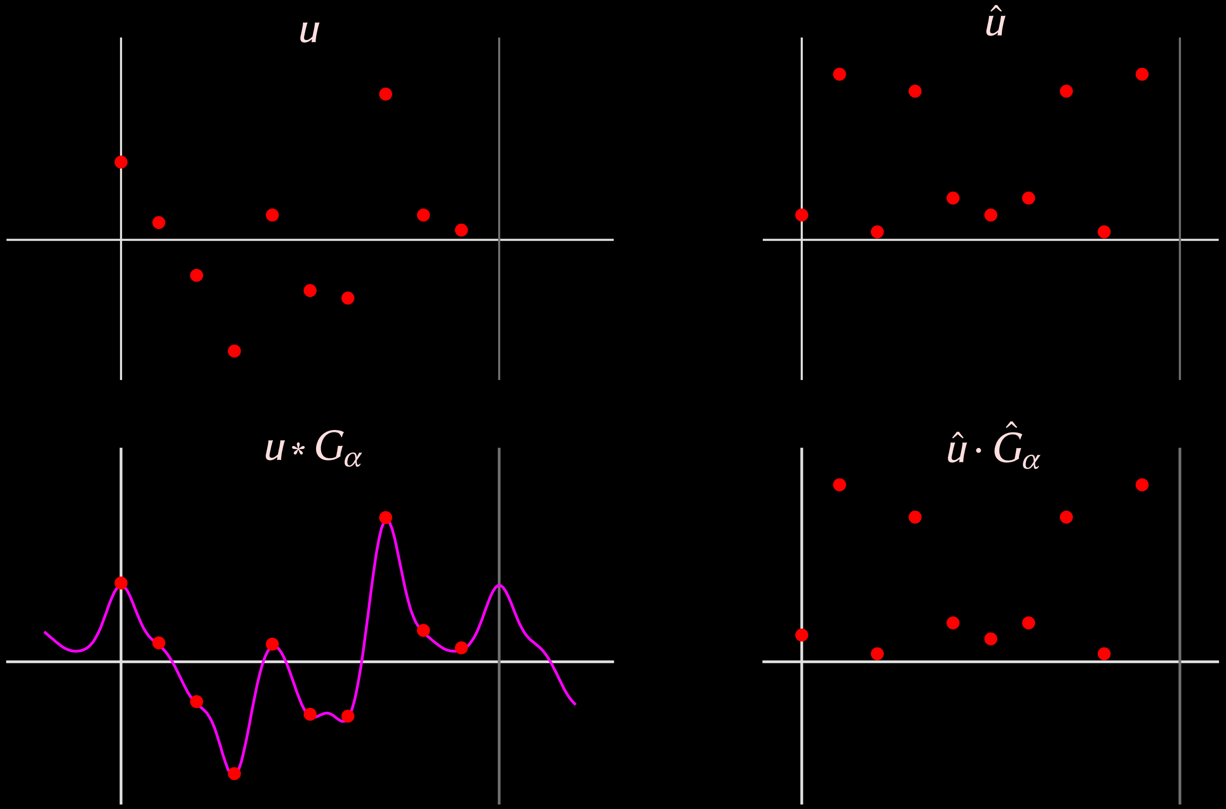
Rééchantillonage gaussien



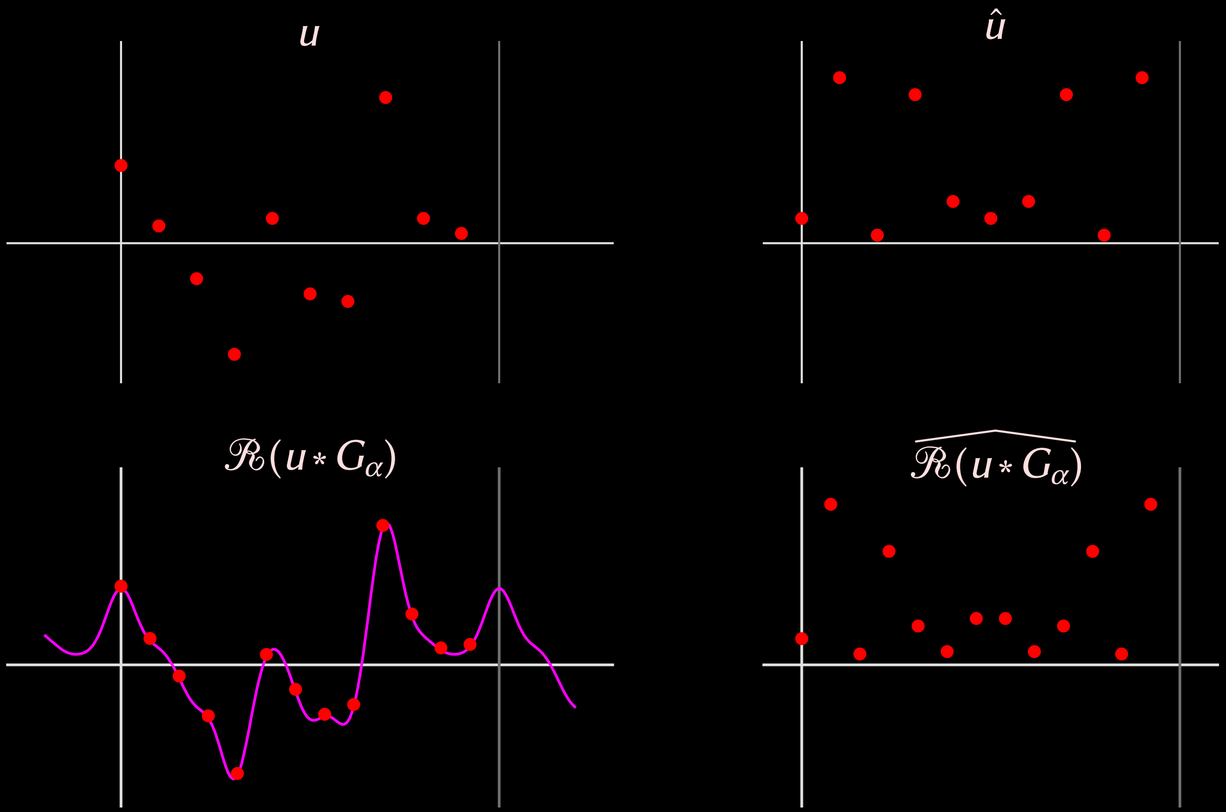
Rééchantillonage gaussien



Rééchantillonage gaussien



Rééchantillonage gaussien



Rééchantillonage gaussien

$$
\begin{tikzcd}
\mathbb{C}^s \arrow[r, "\mathrm{DFT}_s"] \arrow[d, "\mathscr{S}"'] & \mathbb{C}^s \arrow[r, "\text{Permutation}"] & \mathbb{C}^s \arrow[d, "\mathscr{T}"] \\
\mathbb{C}^t \arrow[r, "\mathrm{DFT}_t"] & \mathbb{C}^t \arrow[r, "\text{Permutation}"] & \mathbb{C}^t
\end{tikzcd}
$$

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

Rééchantillonage gaussien

$$\begin{tikzcd}
\mathbb{C}^s \arrow[r, "\mathrm{DFT}_s"] \arrow[d, "\mathscr{S}"'] & \mathbb{C}^s \arrow[r, "\text{Permutation}"] & \mathbb{C}^s \arrow[d, "\mathscr{T}"] \\
\mathbb{C}^t \arrow[r, "\mathrm{DFT}_t"] & \mathbb{C}^t \arrow[r, "\text{Permutation}"] & \mathbb{C}^t
\end{tikzcd}$$

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

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

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

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

Matrices de rééchantillonage

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

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

Matrices de rééchantillonage

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

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

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

Conclusion

$$\begin{array}{c} \mathbb{Z} \\ \big\downarrow \\ \mathbb{C}[x]/(x^{r_1\cdots r_d}-1) \\ \big\downarrow \\ \mathbb{C}[u_1,\ldots,u_d]/(u_1^{r_1}-1,\ldots,u_d^{r_d}-1) \\ \big\downarrow \\ \mathrm{DFT}(r_2,\ldots,r_d)\ \text{ sur }\ \mathbb{C}[u_1]/(u_1^{r_1}-1) \\ \big\downarrow \\ \mathrm{DFT}(r_1,\ldots,r_1)\ \text{ sur }\ \mathbb{C}[u_1]/(u_1^{r_1}-1) \\ \big\downarrow \\ \mathbb{C}[u_1,\ldots,u_d]/(u_1^{r_1}-1,\ldots,u_d^{r_1}-1) \end{array}$$

$\longrightarrow$ Plongement

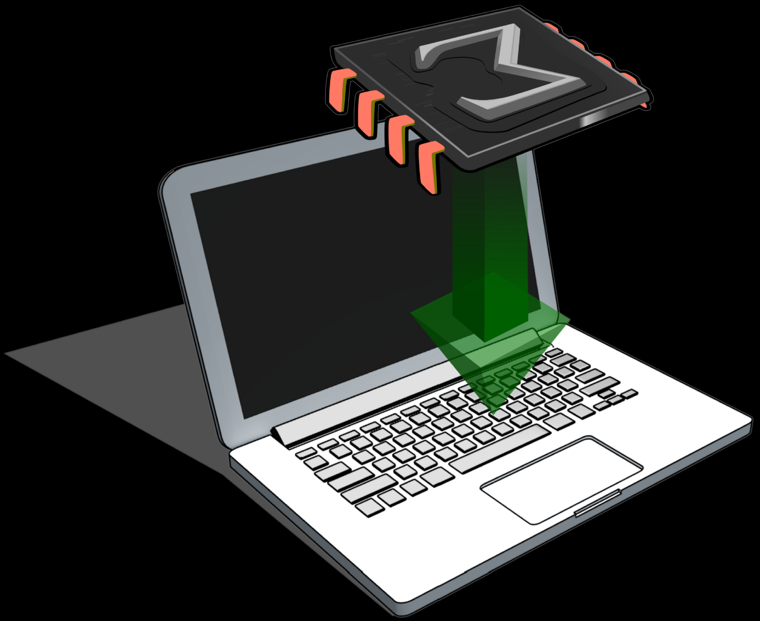
$\longrightarrow$ Restes chinois à la Good

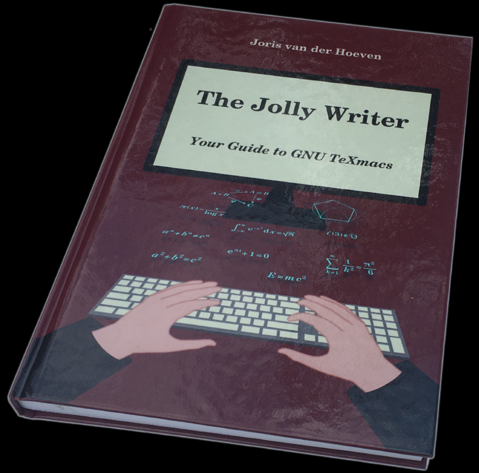
$\longrightarrow$ Multiplication FFT

$\longrightarrow$ Rééchantillonage gaussien

$\longrightarrow$ Réduction de Bluestein

Merci !





http://www.TeXmacs.org