

# Integer multiplication in time $O(n \log n)$

**Joris van der Hoeven**

CNRS, École polytechnique

Joint work with **David Harvey** (UNSW, Sydney)



$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

**Division.**  $O(M(N))$

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

**Division.**  $O(M(N))$

**Gcd.**  $O(M(N) \log N)$

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

**Division.**  $O(M(N))$

**Gcd.**  $O(M(N) \log N)$

**Computing  $e, \pi$ .**  $O(M(N) \log N)$

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

**Division.**  $O(M(N))$

**Gcd.**  $O(M(N) \log N)$

**Computing  $e, \pi$ .**  $O(M(N) \log N)$

**Base conversion.**  $O\left(M(N) \frac{\log N}{\log \log N}\right)$  (FFT-model)

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

**Division.**  $O(M(N))$

**Gcd.**  $O(M(N) \log N)$

**Computing  $e$ ,  $\pi$ .**  $O(M(N) \log N)$

**Base conversion.**  $O\left(M(N) \frac{\log N}{\log \log N}\right)$  (FFT-model)

**FFT.**  $O(M(np))$ , length  $n$ , bit-precision  $p \geq \log n$



$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

**Why study the asymptotic behaviour of  $M(N)$  ?**

**Division.**  $O(M(N))$

**Gcd.**  $O(M(N) \log N)$

**Computing  $e, \pi$ .**  $O(M(N) \log N)$

**Base conversion.**  $O\left(M(N) \frac{\log N}{\log \log N}\right)$  (FFT-model)

**FFT.**  $O(M(np))$ , length  $n$ , bit-precision  $p \geq \log n$

$M(N)$  = speed of basic arithmetic

$M(N)$  : the complexity of multiplying two  $N$ -bit integers (Turing machine model)

## Why study the asymptotic behaviour of $M(N)$ ?

**Division.**  $O(M(N))$

**Gcd.**  $O(M(N) \log N)$

**Computing  $e$ ,  $\pi$ .**  $O(M(N) \log N)$

**Base conversion.**  $O\left(M(N) \frac{\log N}{\log \log N}\right)$  (FFT-model)

**FFT.**  $O(M(np))$ , length  $n$ , bit-precision  $p \geq \log n$

$M(N)$  = speed of basic arithmetic

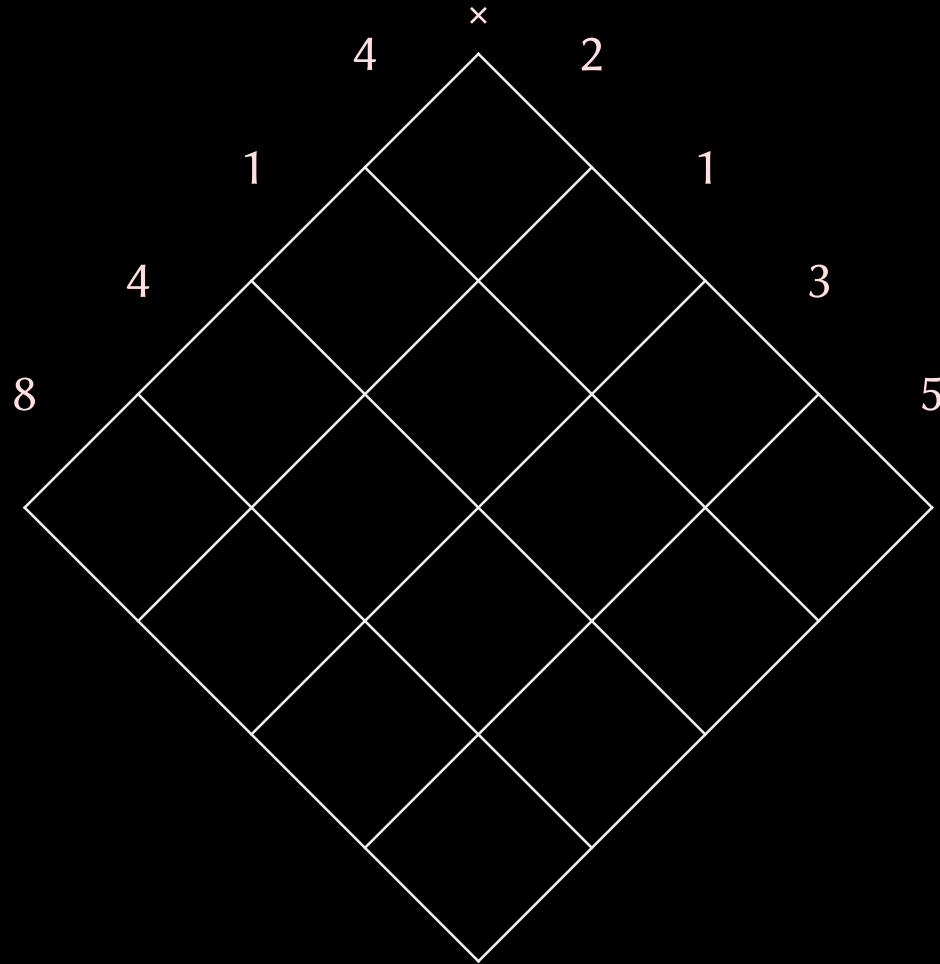
## Also

- Asymptotic complexity abstracts from concrete machines
- Better theoretical techniques  $\xrightarrow{\text{often}}$  faster practical implementations

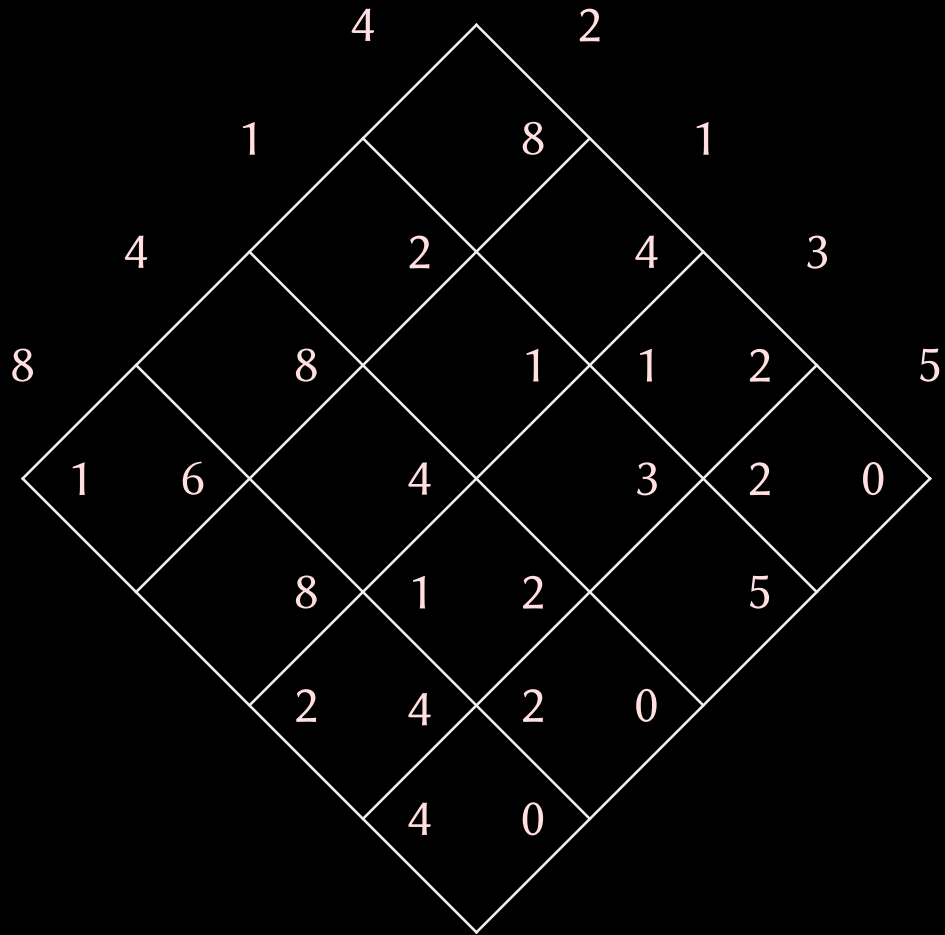
# Naive multiplication

$$8 \ 4 \ 1 \ 4 \ \times \ 2 \ 1 \ 3 \ 5$$

# Naive multiplication



# Naive multiplication





# Can we do better?



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

!

?





# Can we do better?


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

!

?



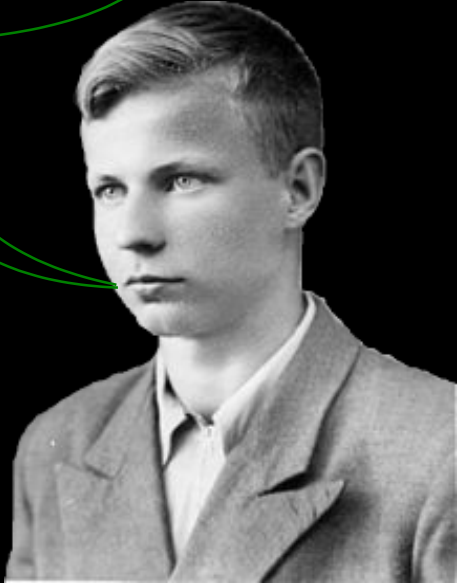
# Can we do better?



A black and white portrait of Donald Knuth, an older man with grey hair, wearing a suit and tie. A red speech bubble originates from his mouth.

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

! ?



A black and white portrait of Donald Knuth, a younger man with short hair, wearing a suit and tie. A green speech bubble originates from his mouth.

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

1962

1962	Karatsuba	$O(N^{\log 3 / \log 2})$
1963	Toom	$O(N 2^{5\sqrt{\log N / \log 2}})$
1966	Schönhage	$O(N 2^{\sqrt{2\log N / \log 2}} (\log N)^{3/2})$
1969	Knuth	$O(N 2^{\sqrt{2\log N / \log 2}} \log N)$
1971	Pollard	$O(N \log N \log \log N \log \log \log N \dots)$
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	$O(N \log N)$

# Karatsuba multiplication

$$13022020 \times 31415926$$

# Karatsuba multiplication

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

# Karatsuba multiplication

$$\underbrace{1302}_a \underbrace{2020}_b \times \underbrace{3141}_c \underbrace{5926}_d$$

# Karatsuba multiplication

$$\underbrace{1302}_a \underbrace{2020}_b \times \underbrace{3141}_c \underbrace{5926}_d$$

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

# Karatsuba multiplication

$$\underbrace{1302}_a \quad \underbrace{2020}_b \quad \times \quad \underbrace{3141}_c \quad \underbrace{5926}_d$$

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



# Karatsuba multiplication

$$\underbrace{1302}_a \quad \underbrace{2020}_b \quad \times \quad \underbrace{3141}_c \quad \underbrace{5926}_d$$

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

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

$$\underbrace{1302}_a \quad \underbrace{2020}_b \quad \times \quad \underbrace{3141}_c \quad \underbrace{5926}_d$$

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

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

## Complexity

$$M(n) \leq 3M(n/2) + Cn$$

$$\underbrace{1302}_a \quad \underbrace{2020}_b \quad \times \quad \underbrace{3141}_c \quad \underbrace{5926}_d$$

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

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

## Complexity

$$\begin{aligned} M(n) &\leq 3M(n/2) + Cn \\ &\leq 9M(n/4) + \frac{5}{2}Cn \end{aligned}$$

$$\underbrace{1302}_a \quad \underbrace{2020}_b \quad \times \quad \underbrace{3141}_c \quad \underbrace{5926}_d$$

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

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

## Complexity

$$\begin{aligned} M(n) &\leq 3M(n/2) + Cn \\ &\leq 9M(n/4) + \frac{5}{2}Cn \\ &\leq 27M(n/8) + \frac{19}{4}Cn \end{aligned}$$

$$\underbrace{1302}_a \quad \underbrace{2020}_b \quad \times \quad \underbrace{3141}_c \quad \underbrace{5926}_d$$

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

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

## Complexity

$$\begin{aligned} M(n) &\leq 3M(n/2) + Cn \\ &\leq 9M(n/4) + \frac{5}{2}Cn \\ &\leq 27M(n/8) + \frac{19}{4}Cn \\ &\leq \dots \\ &\leq O\left(n^{\frac{\log 3}{\log 2}}\right) \end{aligned}$$

## Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$

$$\Downarrow$$

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

## Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$

$$\Downarrow$$

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

## Kronecker substitution

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

$$\Downarrow$$

$$4627000005796000007978000008114 \times 4519000001708000007196000006234$$

## Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$

↵

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

## Kronecker substitution

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

↵

$$4627000005796000007978000008114 \times 4519000001708000007196000006234$$

$$1004003 \times 2001005 = 2009015023015$$



$\mathbb{K}$ : field (or suitable ring)

$n$ : cycle length

$\mathbb{K}[x]/(x^n - 1)$ : ring of cyclic polynomials of length  $n$

$\mathbb{K}$ : field (or suitable ring)

$n$ : cycle length

$\mathbb{K}[x]/(x^n - 1)$ : ring of cyclic polynomials of length  $n$

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

$\mathbb{K}$ : field (or suitable ring)

$n$ : cycle length

$\mathbb{K}[x]/(x^n - 1)$ : ring of cyclic polynomials of length  $n$

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

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

$\mathbb{K}$ : field (or suitable ring)

$n$ : cycle length

$\mathbb{K}[x]/(x^n - 1)$ : ring of cyclic polynomials of length  $n$

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

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

**Summary so far**

$$\begin{array}{c} \mathbb{Z} \\ \downarrow \\ \mathbb{K}[x] \\ \downarrow \\ \mathbb{K}[x]/(x^n - 1) \end{array}$$

$\mathbb{K}$ : a field (or a suitable ring)

$n$ : cycle or transform length

$\omega$ : primitive  $n$ -th root of unity in  $\mathbb{K}$ , say  $\omega = e^{\frac{2\pi i}{n}}$

$\mathbb{K}$ : a field (or a suitable ring)

$n$ : cycle or transform length

$\omega$ : primitive  $n$ -th root of unity in  $\mathbb{K}$ , say  $\omega = e^{\frac{2\pi i}{n}}$

## Chinese remainder theorem

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

$\mathbb{K}$ : a field (or a suitable ring)

$n$ : cycle or transform length

$\omega$ : primitive  $n$ -th root of unity in  $\mathbb{K}$ , say  $\omega = e^{\frac{2\pi i}{n}}$

## Chinese remainder theorem

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

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

$\mathbb{K}$ : a field (or a suitable ring)

$n$ : cycle or transform length

$\omega$ : primitive  $n$ -th root of unity in  $\mathbb{K}$ , say  $\omega = e^{\frac{2\pi i}{n}}$

## Chinese remainder theorem

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

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



$\mathbb{K}$ : a field (or a suitable ring)

$n$ : cycle or transform length

$\omega$ : primitive  $n$ -th root of unity in  $\mathbb{K}$ , say  $\omega = e^{\frac{2\pi i}{n}}$

## Chinese remainder theorem

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

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

## Discrete Fourier transform

$$\mathbb{K}[x]/(x^n - 1) \begin{array}{c} \xrightarrow{\text{DFT}_\omega} \\ \xleftarrow{\text{DFT}_\omega^{-1}} \end{array} \bigoplus_{0 \leq k < n} \mathbb{K}[x]/(x - \omega^k)$$

$\mathbb{K}$ : a field (or a suitable ring)

$n$ : cycle or transform length

$\omega$ : primitive  $n$ -th root of unity in  $\mathbb{K}$ , say  $\omega = e^{\frac{2\pi i}{n}}$

## Chinese remainder theorem

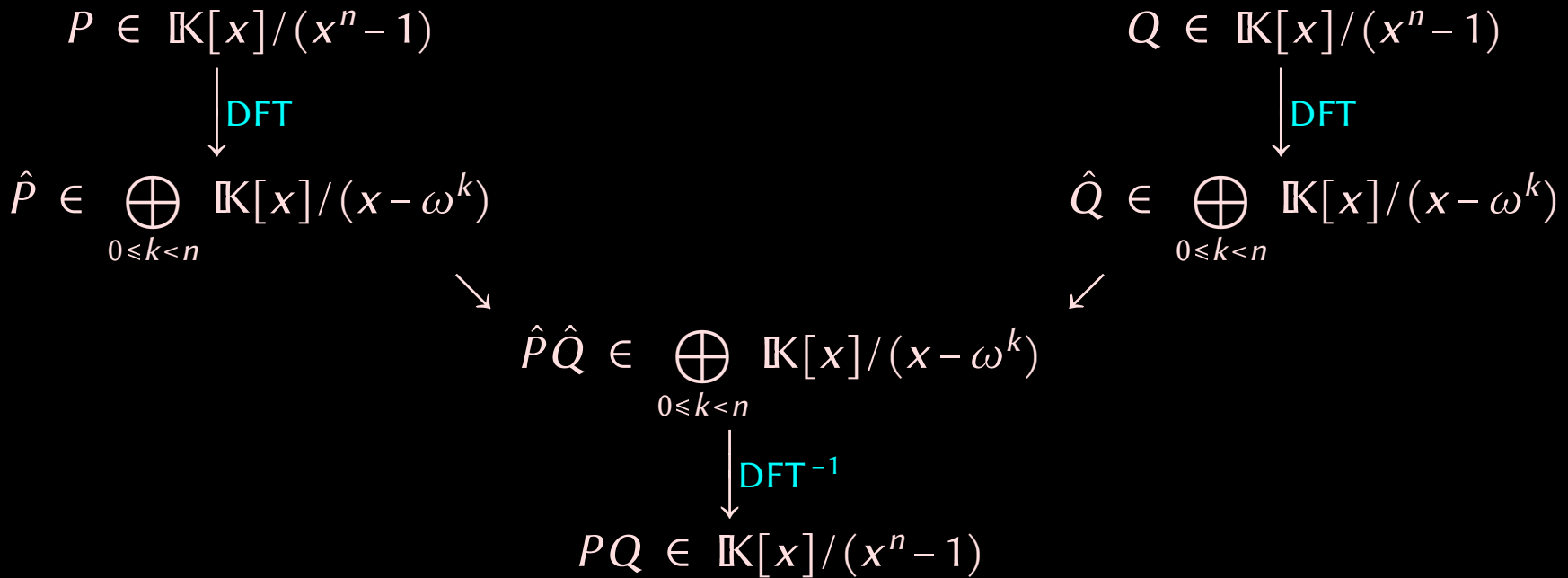
$$(x^n - 1) = \prod_{0 \leq k < n} (x - \omega^k)$$

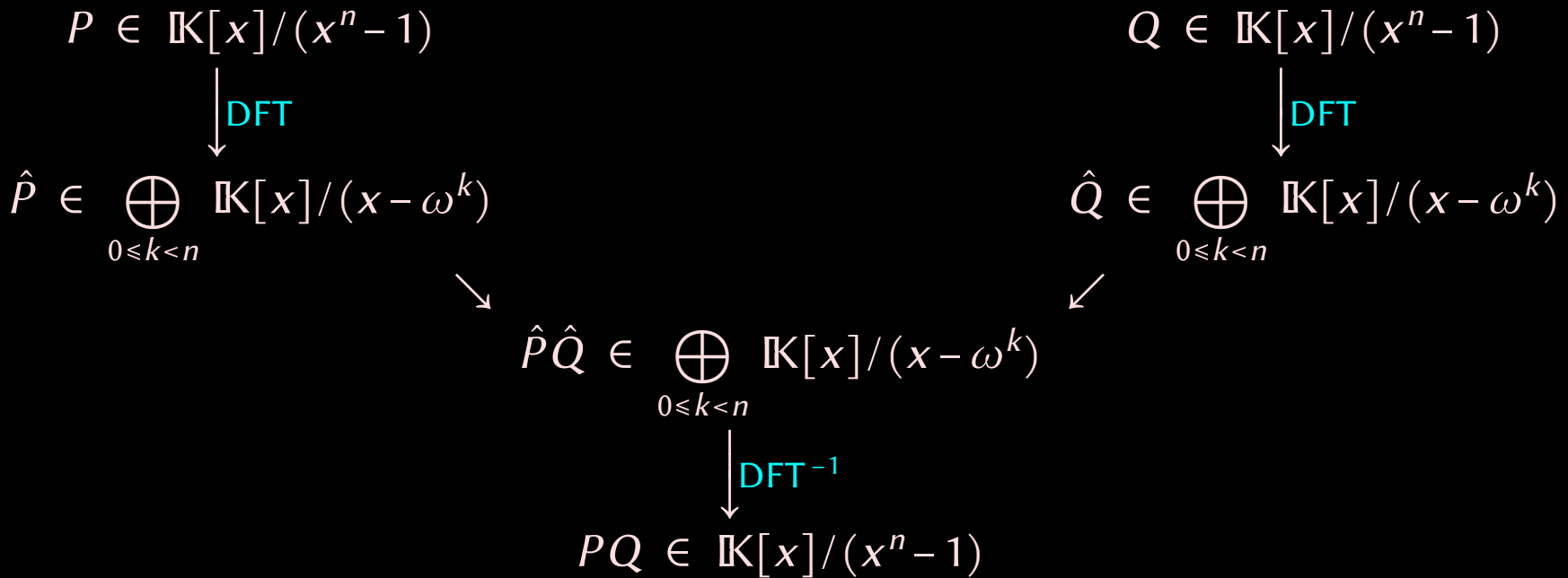
$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leq k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

## Discrete Fourier transform

$$\mathbb{K}[x]/(x^n - 1) \begin{array}{c} \xrightarrow{\text{DFT}_\omega} \\ \xleftarrow{\text{DFT}_\omega^{-1}} \end{array} \bigoplus_{0 \leq k < n} \mathbb{K}[x]/(x - \omega^k)$$

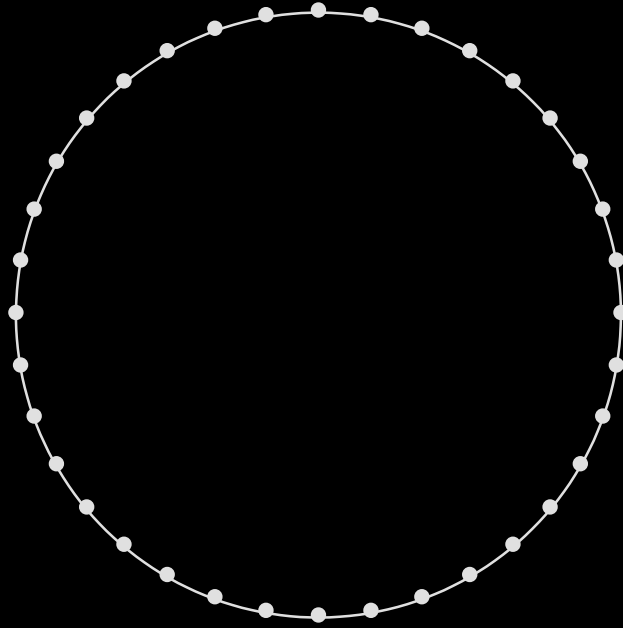
$$\text{DFT}_\omega^{-1} \rightsquigarrow \frac{1}{n} \text{DFT}_{\omega^{-1}}$$





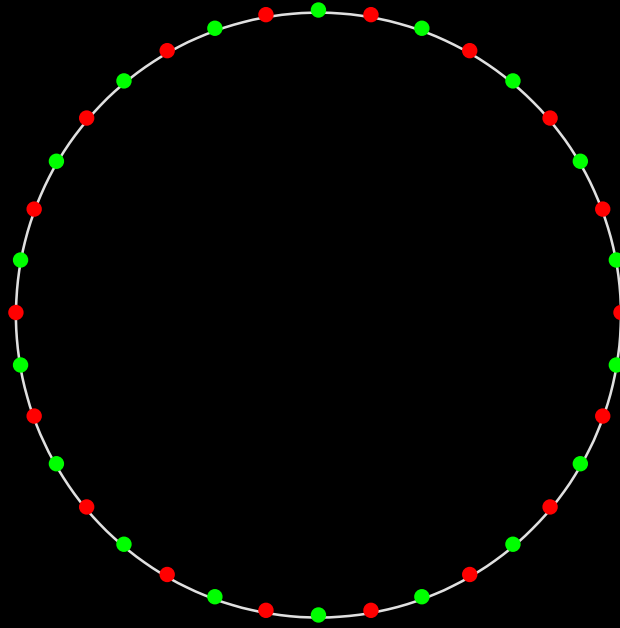
## Summary so far

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



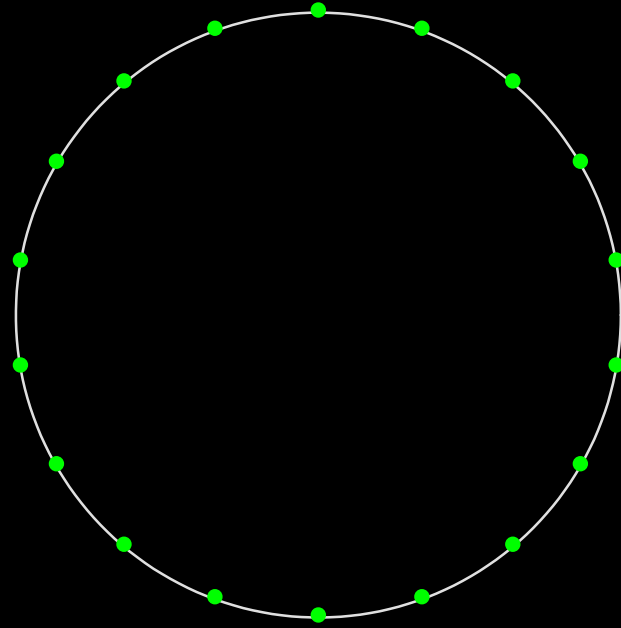
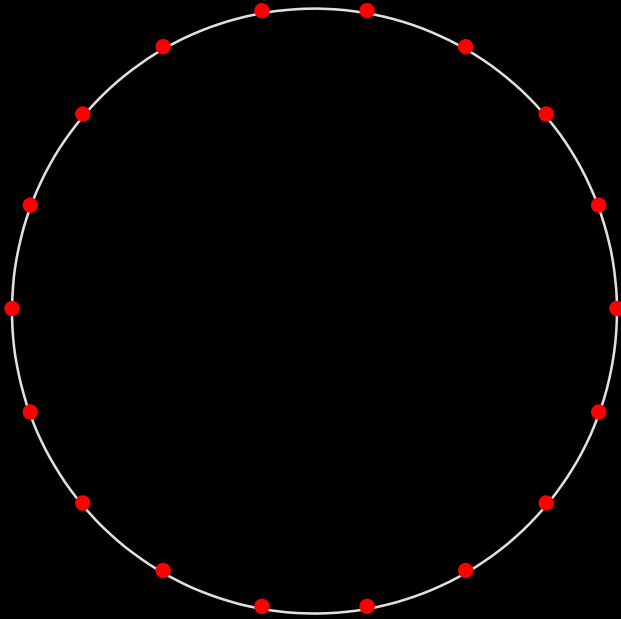
# Making the FFT fast

11/21

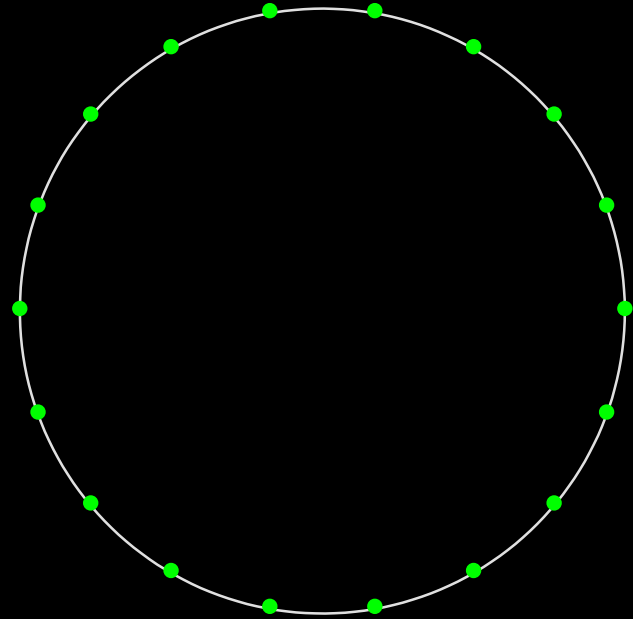
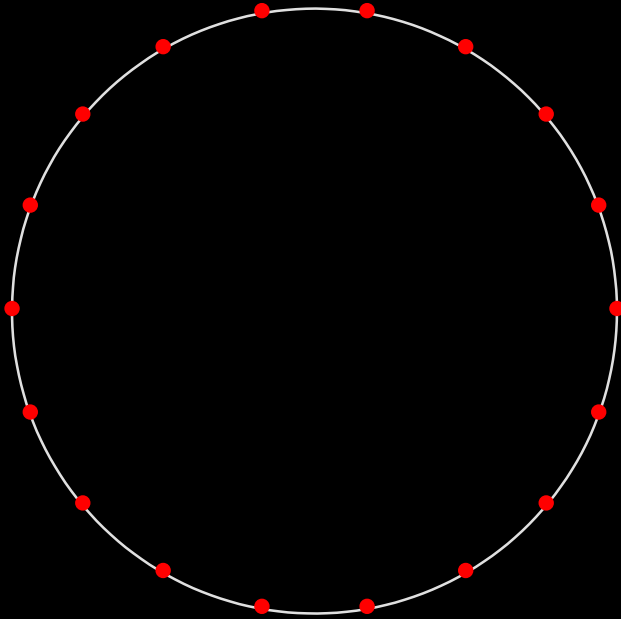


# Making the FFT fast

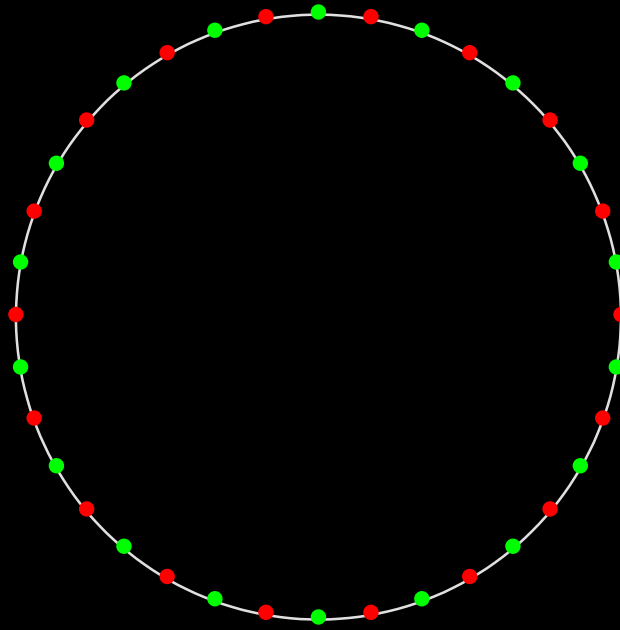
11/21



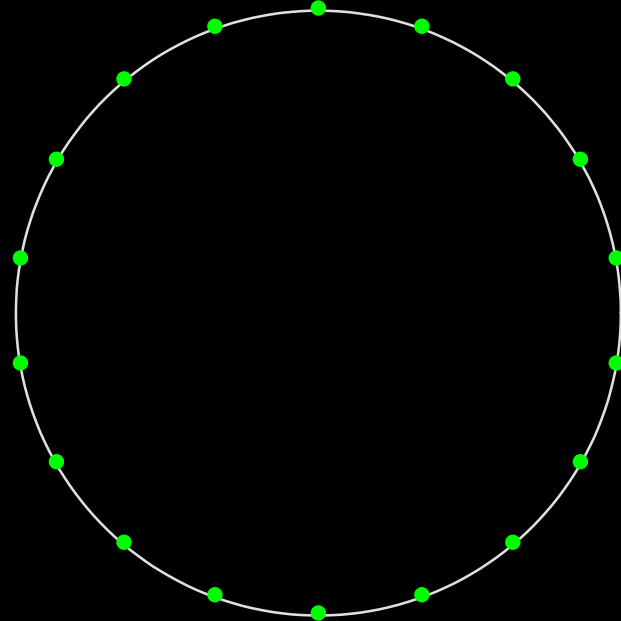
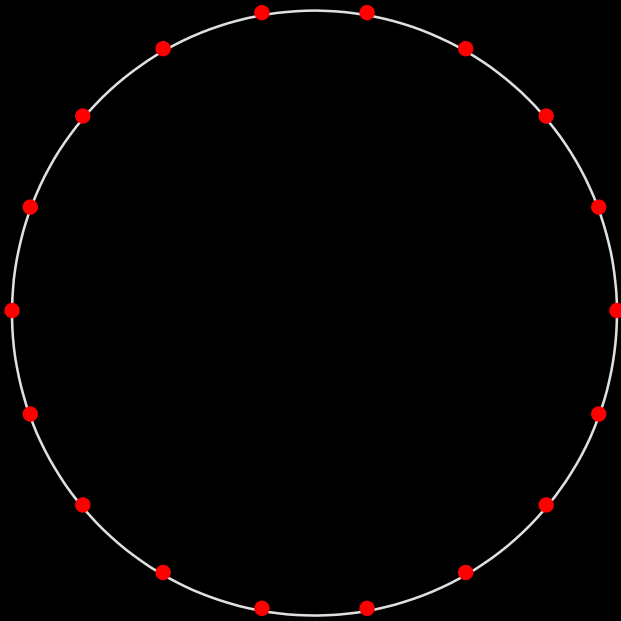
# Making the FFT fast



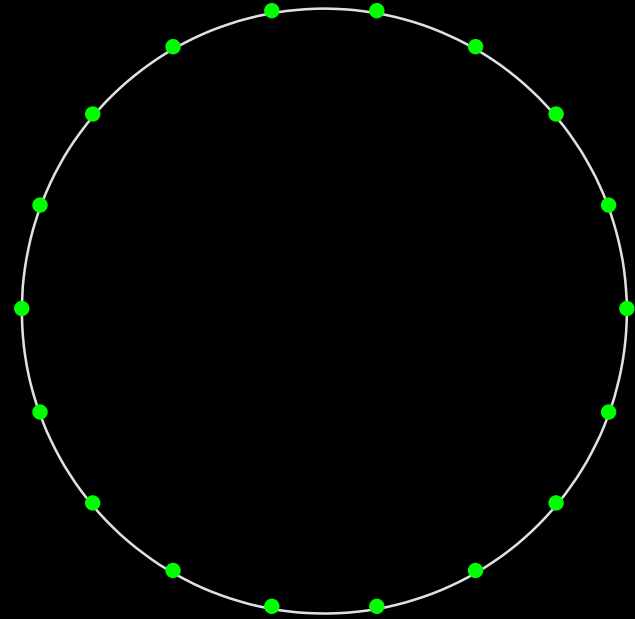
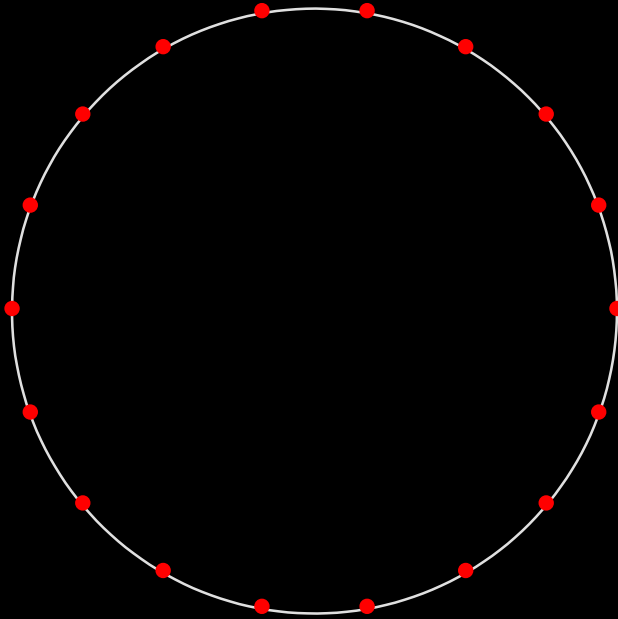




$$\mathbb{K}[x]/(x^{2n} - 1)$$




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



$$\begin{aligned}
 \mathbb{K}[x]/(x^{2n}-1) &\cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1) \\
 &\cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(\tilde{x}^n-1) \\
 &\quad \tilde{x} = \omega x \\
 &\quad \omega^n = -1
 \end{aligned}$$

$$F_{\mathbb{K}}(2n) \leq 2F_{\mathbb{K}}(n) + n \text{add}_{\mathbb{K}} + n \text{sub}_{\mathbb{K}} + n \text{mul}_{\omega^{\mathbb{N}}}$$

$$F_{\mathbb{K}}(2n) \leq 2F_{\mathbb{K}}(n) + \underbrace{n \text{ add}_{\mathbb{K}} + n \text{ sub}_{\mathbb{K}} + n \text{ mul}_{\omega^{\mathbb{N}}}}_{\text{cost of } \mathbb{K}[x]/(x^{2n}-1)}$$


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

$$\cong$$

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

$$F_{\mathbb{K}}(2n) \leq 2F_{\mathbb{K}}(n) + \underbrace{n \text{ add}_{\mathbb{K}} + n \text{ sub}_{\mathbb{K}}}_{\text{addition and subtraction}} + \underbrace{n \text{ mul}_{\omega^N}}_{\text{multiplication}}$$

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

$$\cong$$

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

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

$$\cong$$

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

$$F_{\mathbb{K}}(2n) \leq 2F_{\mathbb{K}}(n) + \underbrace{n \text{ add}_{\mathbb{K}} + n \text{ sub}_{\mathbb{K}}}_{\text{addition and subtraction}} + \underbrace{n \text{ mul}_{\omega^{\mathbb{N}}}}_{\text{multiplication}}$$

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

 $\cong$ 

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

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

 $\cong$ 

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

$$n = 2^{\lg n} \implies F_{\mathbb{K}}(n) \leq n \lg n \left( \text{add}_{\mathbb{K}} + \frac{1}{2} \text{mul}_{\omega^{\mathbb{N}}} \right)$$

**How to choose  $\mathbb{K}$ ?**



## How to choose $\mathbb{K}$ ?

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

## How to choose $\mathbb{K}$ ?

- I.  $\mathbb{K} = \mathbb{C}_b$  with  $b \asymp \log N$ ,  $n \asymp \frac{N}{\log N}$ ,  $\omega = e^{\frac{2\pi i}{n}}$
- II.  $\mathbb{K} = \mathbb{F}_p$  with  $p = s2^l + 1$ ,  $\lg p \asymp \log N$ ,  $n = 2^l \asymp \frac{N}{\log N}$ ,  $\omega$  exists...

## How to choose $\mathbb{K}$ ?

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

II.  $\mathbb{K} = \mathbb{F}_p$  with  $p = s2^l + 1$ ,  $\lg p \asymp \log N$ ,  $n = 2^l \asymp \frac{N}{\log N}$ ,  $\omega$  exists...

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

## How to choose $\mathbb{K}$ ?

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

II.  $\mathbb{K} = \mathbb{F}_p$  with  $p = s2^l + 1$ ,  $\lg p \asymp \log N$ ,  $n = 2^l \asymp \frac{N}{\log N}$ ,  $\omega$  exists...

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

## Complexity analysis

## How to choose $\mathbb{K}$ ?

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

II.  $\mathbb{K} = \mathbb{F}_p$  with  $p = s2^l + 1$ ,  $\lg p \asymp \log N$ ,  $n = 2^l \asymp \frac{N}{\log N}$ ,  $\omega$  exists...

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

## Complexity analysis

I.  $M(N) = O(NM(\log N))$

$M(N) = O(N \log N \log \log N \cdots)$

## How to choose $\mathbb{K}$ ?

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

II.  $\mathbb{K} = \mathbb{F}_p$  with  $p = s2^l + 1$ ,  $\lg p \asymp \log N$ ,  $n = 2^l \asymp \frac{N}{\log N}$ ,  $\omega$  exists...

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

## Complexity analysis

I.  $M(N) = O(NM(\log N))$

$$M(N) = O(N \log N \log \log N \cdots)$$

II.  $M(N) = O(NM(\log N))$

$$M(N) = O(N \log N \log \log N \cdots)$$

## How to choose $\mathbb{K}$ ?

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

II.  $\mathbb{K} = \mathbb{F}_p$  with  $p = s2^l + 1$ ,  $\lg p \asymp \log N$ ,  $n = 2^l \asymp \frac{N}{\log N}$ ,  $\omega$  exists...

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

## Complexity analysis

I.  $M(N) = O(NM(\log N))$

$M(N) = O(N \log N \log \log N \dots)$

II.  $M(N) = O(NM(\log N))$

$M(N) = O(N \log N \log \log N \dots)$

III.  $M^\ominus(N) \leq 2\sqrt{N}M^\ominus(\sqrt{N}) + O(N \log N)$

$M(N) = O(N \log N \log \log N)$

$M^\ominus(N)$ : cost of multiplication in  $\mathbb{Z}/(2^N + 1)\mathbb{Z}$

**A careful construction yields**

$$M^{\Theta}(n) \leq Cn \log n + 2n^{1/2} M^{\Theta}(n^{1/2})$$



## A careful construction yields

$$\begin{aligned} M^\ominus(n) &\leq Cn \log n + 2n^{1/2} M^\ominus(n^{1/2}) \\ &\leq Cn \log n + Cn \log n + 4n^{3/4} M^\ominus(n^{1/4}) \end{aligned}$$

## A careful construction yields

$$\begin{aligned}M^\ominus(n) &\leq Cn \log n + 2n^{1/2} M^\ominus(n^{1/2}) \\ &\leq Cn \log n + Cn \log n + 4n^{3/4} M^\ominus(n^{1/4}) \\ &\leq Cn \log n + Cn \log n + Cn \log n + 8n^{7/8} M^\ominus(n^{1/8})\end{aligned}$$

## A careful construction yields

$$\begin{aligned} M^\Theta(n) &\leq Cn \log n + 2n^{1/2} M^\Theta(n^{1/2}) \\ &\leq Cn \log n + Cn \log n + 4n^{3/4} M^\Theta(n^{1/4}) \\ &\leq Cn \log n + Cn \log n + Cn \log n + 8n^{7/8} M^\Theta(n^{1/8}) \\ &\vdots \\ &\leq Cn \log n + \overset{\log \log n}{\dots} \times + Cn \log n + O(n \log n) \end{aligned}$$

**What if...**

$$M^{\Theta}(n) \leq C n \log n + 1.98 n^{1/2} M^{\Theta}(n^{1/2})$$

**What if...**

$$\begin{aligned} M^\ominus(n) &\leq Cn \log n + 1.98 n^{1/2} M^\ominus(n^{1/2}) \\ &\leq Cn \log n + 0.99 Cn \log n + 1.98^2 n^{3/4} M^\ominus(n^{1/4}) \end{aligned}$$

What if...

$$\begin{aligned} M^{\ominus}(n) &\leq Cn \log n + 1.98 n^{1/2} M^{\ominus}(n^{1/2}) \\ &\leq Cn \log n + 0.99 Cn \log n + 1.98^2 n^{3/4} M^{\ominus}(n^{1/4}) \\ &\leq Cn \log n + 0.99 Cn \log n + 0.99^2 Cn \log n + 1.98^3 n^{7/8} M^{\ominus}(n^{1/8}) \end{aligned}$$

## What if...

$$\begin{aligned}M^\ominus(n) &\leq Cn \log n + 1.98 n^{1/2} M^\ominus(n^{1/2}) \\ &\leq Cn \log n + 0.99 Cn \log n + 1.98^2 n^{3/4} M^\ominus(n^{1/4}) \\ &\leq Cn \log n + 0.99 Cn \log n + 0.99^2 Cn \log n + 1.98^3 n^{7/8} M^\ominus(n^{1/8}) \\ &\vdots \\ &\leq O(n \log n)\end{aligned}$$

## What if...

$$\begin{aligned}M^\ominus(n) &\leq Cn \log n + 1.98 n^{1/2} M^\ominus(n^{1/2}) \\ &\leq Cn \log n + 0.99 Cn \log n + 1.98^2 n^{3/4} M^\ominus(n^{1/4}) \\ &\leq Cn \log n + 0.99 Cn \log n + 0.99^2 Cn \log n + 1.98^3 n^{7/8} M^\ominus(n^{1/8}) \\ &\vdots \\ &\leq O(n \log n)\end{aligned}$$

## Next aim

$$M(n) \leq Cn \log n + (d - \epsilon) n^{1-1/d} M(n^{1/d})$$



## What if...

$$\begin{aligned}
 M^\ominus(n) &\leq Cn \log n + 1.98 n^{1/2} M^\ominus(n^{1/2}) \\
 &\leq Cn \log n + 0.99 Cn \log n + 1.98^2 n^{3/4} M^\ominus(n^{1/4}) \\
 &\leq Cn \log n + 0.99 Cn \log n + 0.99^2 Cn \log n + 1.98^3 n^{7/8} M^\ominus(n^{1/8}) \\
 &\vdots \\
 &\leq O(n \log n)
 \end{aligned}$$

## Next aim

$$\begin{aligned}
 M(n) &\leq Cn \log n + (d - \epsilon) n^{1-1/d} M(n^{1/d}) \quad \text{or} \\
 M\left(\frac{n^d}{d - \epsilon}\right) &\leq Cn^d \log n + n^{d-1} M(n)
 \end{aligned}$$

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

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

## Schönhage-Strassen

$$\begin{aligned} \mathbb{L}[x]/(x^n - 1) &\xrightarrow{\text{DFT}} \mathbb{L}^n \\ \text{mul}_{\mathbb{L}[x]/(x^n - 1)} &\leq n \text{mul}_{\mathbb{L}} + O(n^2 \log n) \end{aligned}$$

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

## Schönhage-Strassen

$$\begin{aligned} \mathbb{L}[x]/(x^n - 1) &\xrightarrow{\text{DFT}} \mathbb{L}^n \\ \text{mul}_{\mathbb{L}[x]/(x^n - 1)} &\leq n \text{mul}_{\mathbb{L}} + O(n^2 \log n) \end{aligned}$$

## Nussbaumer

$$\begin{aligned} \mathbb{L}[u_2, \dots, u_d]/(u_2^n - 1, \dots, u_d^n - 1) &\xrightarrow{\text{DFT}} \mathbb{L}^{n^{d-1}} \\ \text{mul}_{\mathbb{L}[u_1, \dots, u_d]/(u_2^n - 1, \dots, u_d^n - 1)} &\leq n^{d-1} \text{mul}_{\mathbb{L}} + O(n^d \log n) \end{aligned}$$

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

## Schönhage-Strassen

$$\begin{aligned} \mathbb{L}[x]/(x^n - 1) &\stackrel{\text{DFT}}{\iff} \mathbb{L}^n \\ \text{mul}_{\mathbb{L}[x]/(x^n - 1)} &\leq n \text{mul}_{\mathbb{L}} + O(n^2 \log n) \end{aligned}$$

## Nussbaumer

$$\begin{aligned} \mathbb{L}[u_2, \dots, u_d]/(u_2^n - 1, \dots, u_d^n - 1) &\stackrel{\text{DFT}}{\iff} \mathbb{L}^{n^{d-1}} \\ \text{mul}_{\mathbb{L}[u_1, \dots, u_d]/(u_2^n - 1, \dots, u_d^n - 1)} &\leq n^{d-1} \text{mul}_{\mathbb{L}} + O(n^d \log n) \end{aligned}$$

## Next goal

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

$s_1, \dots, s_d$  pairwise coprime

$s_1, \dots, s_d$  pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1 \mathbb{Z} + \cdots + \mathbb{Z}/s_d \mathbb{Z}$$

$s_1, \dots, s_d$  pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1 \mathbb{Z} + \cdots + \mathbb{Z}/s_d \mathbb{Z}$$

$$\chi^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong \chi_1^{\mathbb{Z}/s_1 \mathbb{Z}} \times \cdots \times \chi_d^{\mathbb{Z}/s_d \mathbb{Z}}$$



$s_1, \dots, s_d$  pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1 \mathbb{Z} + \cdots + \mathbb{Z}/s_d \mathbb{Z}$$

$$\mathbf{x}^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong \mathbf{u}_1^{\mathbb{Z}/s_1 \mathbb{Z}} \times \cdots \times \mathbf{u}_d^{\mathbb{Z}/s_d \mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[\mathbf{x}]/(\mathbf{x}^{s_1 \cdots s_d} - 1) &\cong \mathbb{K}[u_1]/(u_1^{s_1} - 1) \otimes \cdots \otimes \mathbb{K}[u_d]/(u_d^{s_d} - 1) \\ &\cong \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1) \end{aligned}$$

$s_1, \dots, s_d$  pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1 \mathbb{Z} + \cdots + \mathbb{Z}/s_d \mathbb{Z}$$

$$\mathbb{X}^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong \mathbb{u}_1^{\mathbb{Z}/s_1 \mathbb{Z}} \times \cdots \times \mathbb{u}_d^{\mathbb{Z}/s_d \mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[\mathbb{X}]/(\mathbb{X}^{s_1 \cdots s_d} - 1) &\cong \mathbb{K}[\mathbb{u}_1]/(\mathbb{u}_1^{s_1} - 1) \otimes \cdots \otimes \mathbb{K}[\mathbb{u}_d]/(\mathbb{u}_d^{s_d} - 1) \\ &\cong \mathbb{K}[\mathbb{u}_1, \dots, \mathbb{u}_d]/(\mathbb{u}_1^{s_1} - 1, \dots, \mathbb{u}_d^{s_d} - 1) \end{aligned}$$

## Setup

- $d$  fixed once and for all (sufficiently large)
- $s_1 = 2^l$
- $s_k = (1 - o(1)) 2^l$  or  $s_k = (1 - o(1)) 2^{l-1}$ ,  $k = 2, \dots, d$

$s_1, \dots, s_d$  pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1 \mathbb{Z} + \cdots + \mathbb{Z}/s_d \mathbb{Z}$$

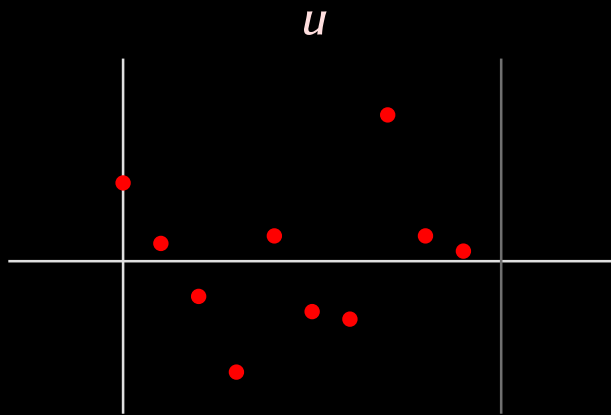
$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1 \mathbb{Z} \times \cdots \times \mathbb{Z}/s_d \mathbb{Z}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) &\cong \mathbb{K}[u_1]/(u_1^{s_1} - 1) \otimes \cdots \otimes \mathbb{K}[u_d]/(u_d^{s_d} - 1) \\ &\cong \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1) \end{aligned}$$

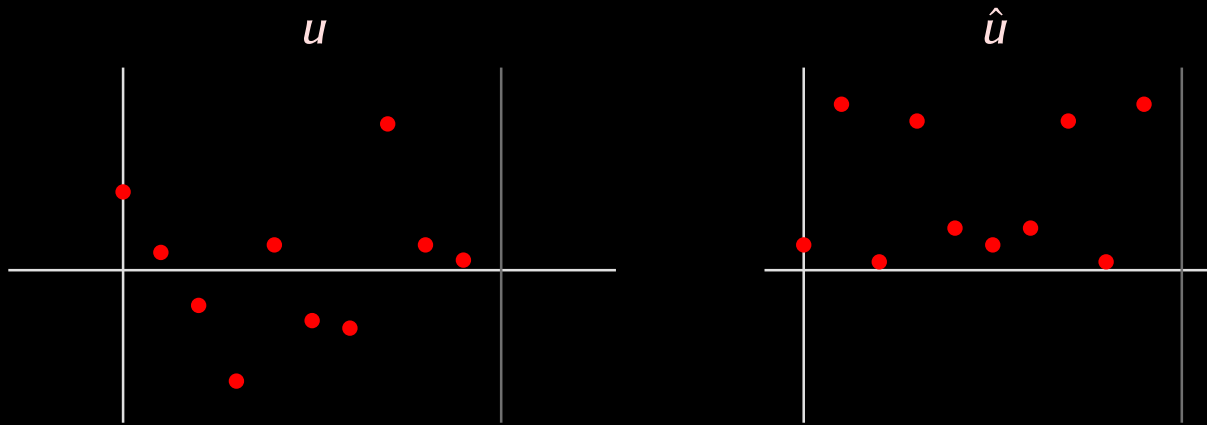
## Setup

- $d$  fixed once and for all (sufficiently large)
- $s_1 = 2^l$
- $s_k = (1 - o(1)) 2^l$  or  $s_k = (1 - o(1)) 2^{l-1}$ ,  $k = 2, \dots, d$

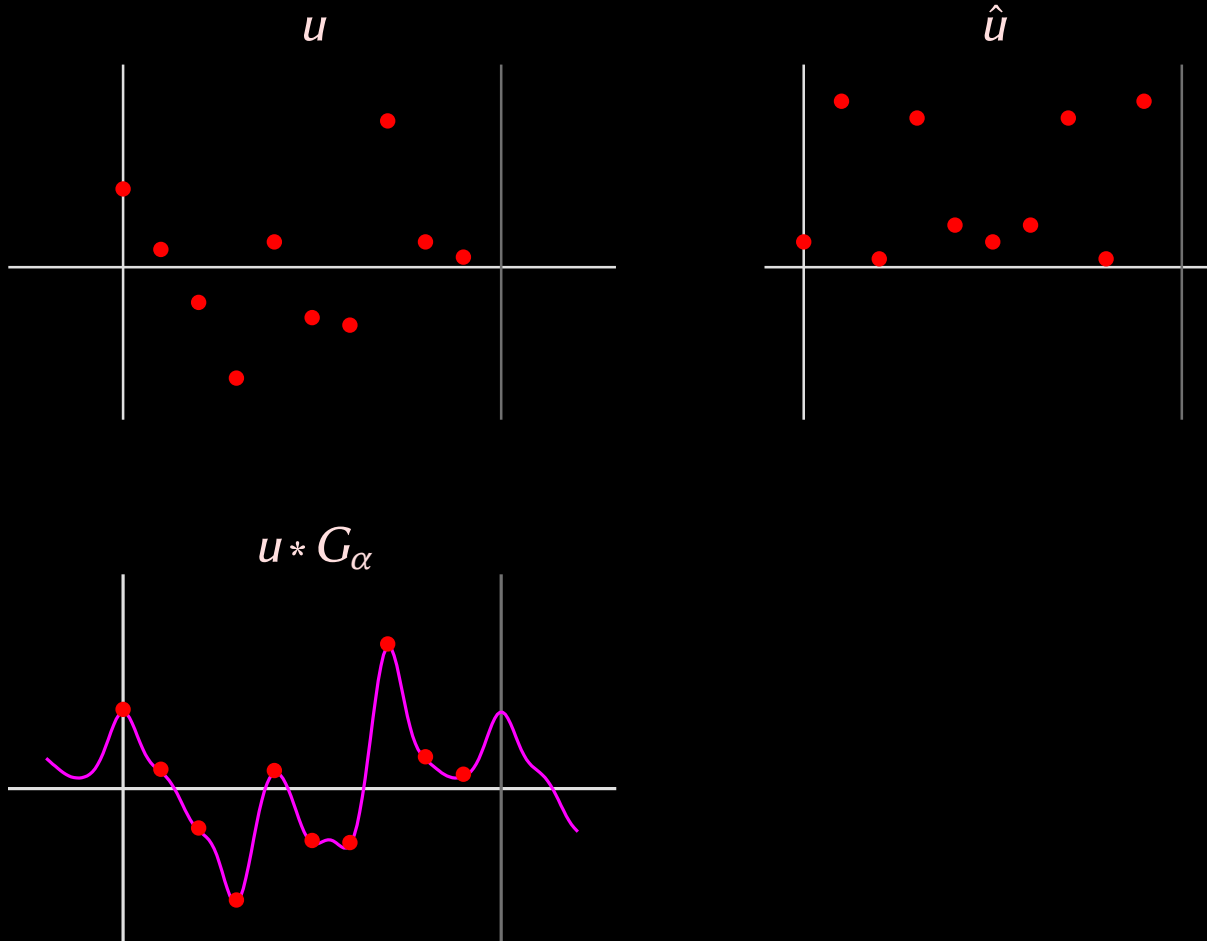
$$\mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1) \xrightarrow{?} \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_1} - 1)$$



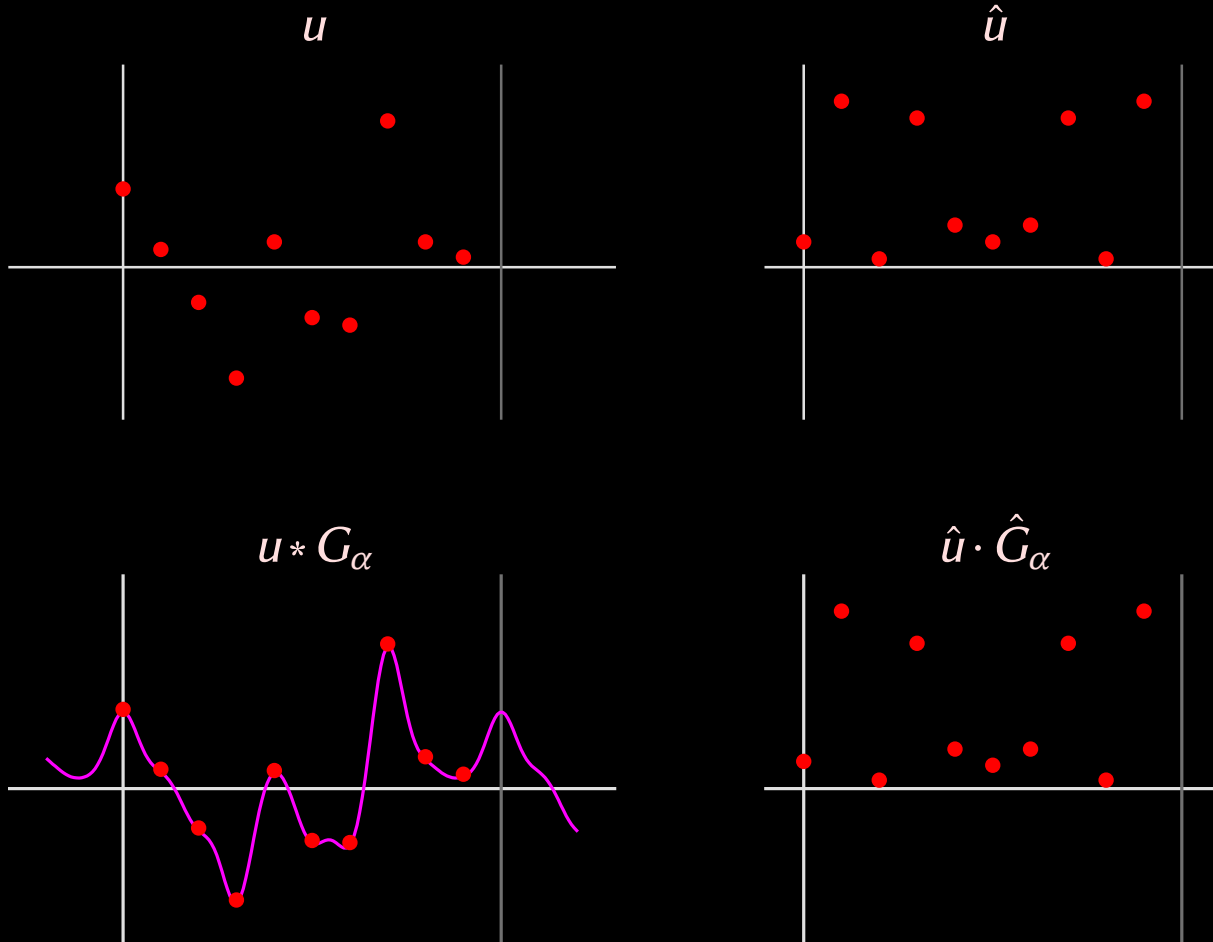
# Gaussian resampling



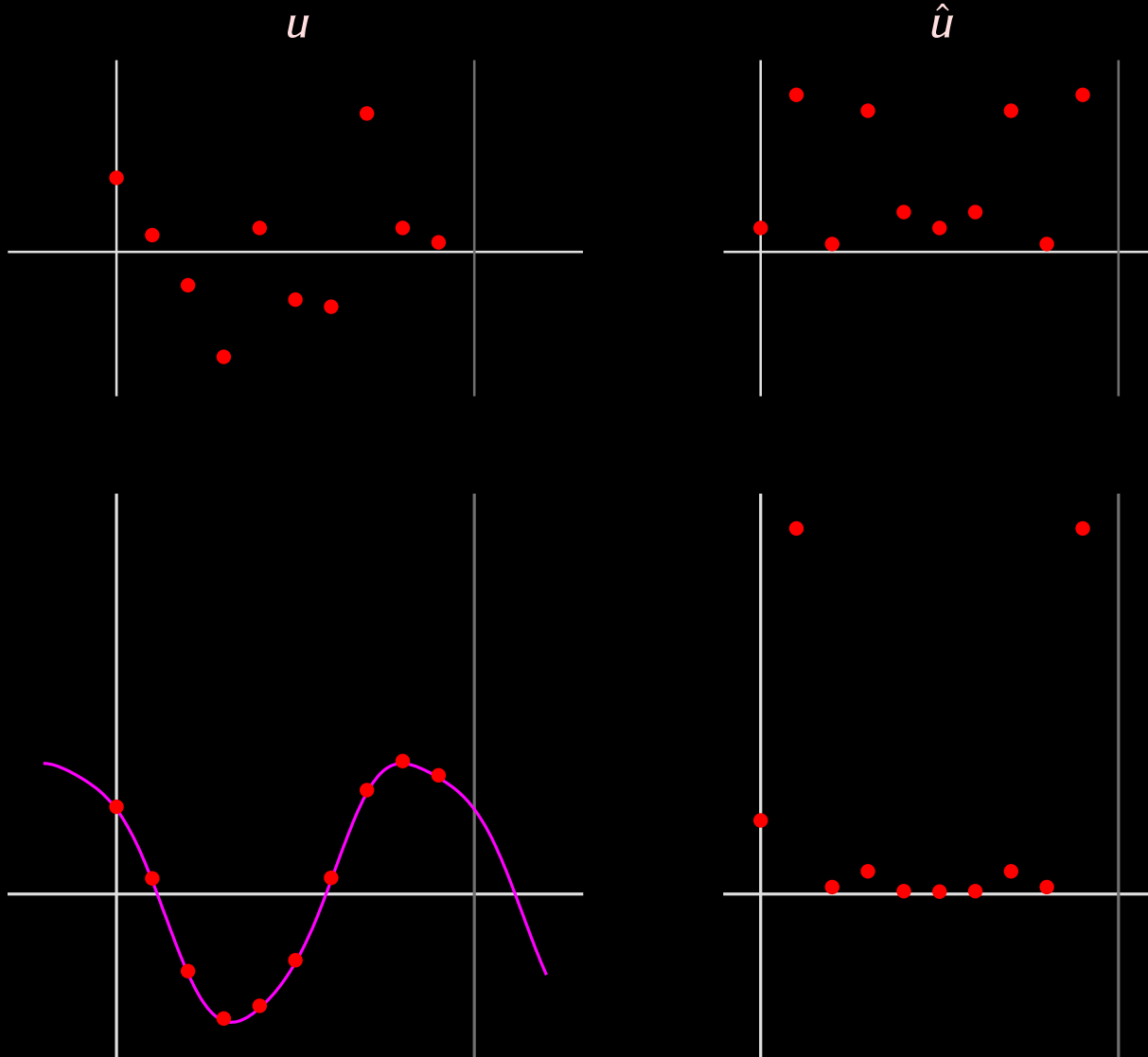
# Gaussian resampling



# Gaussian resampling

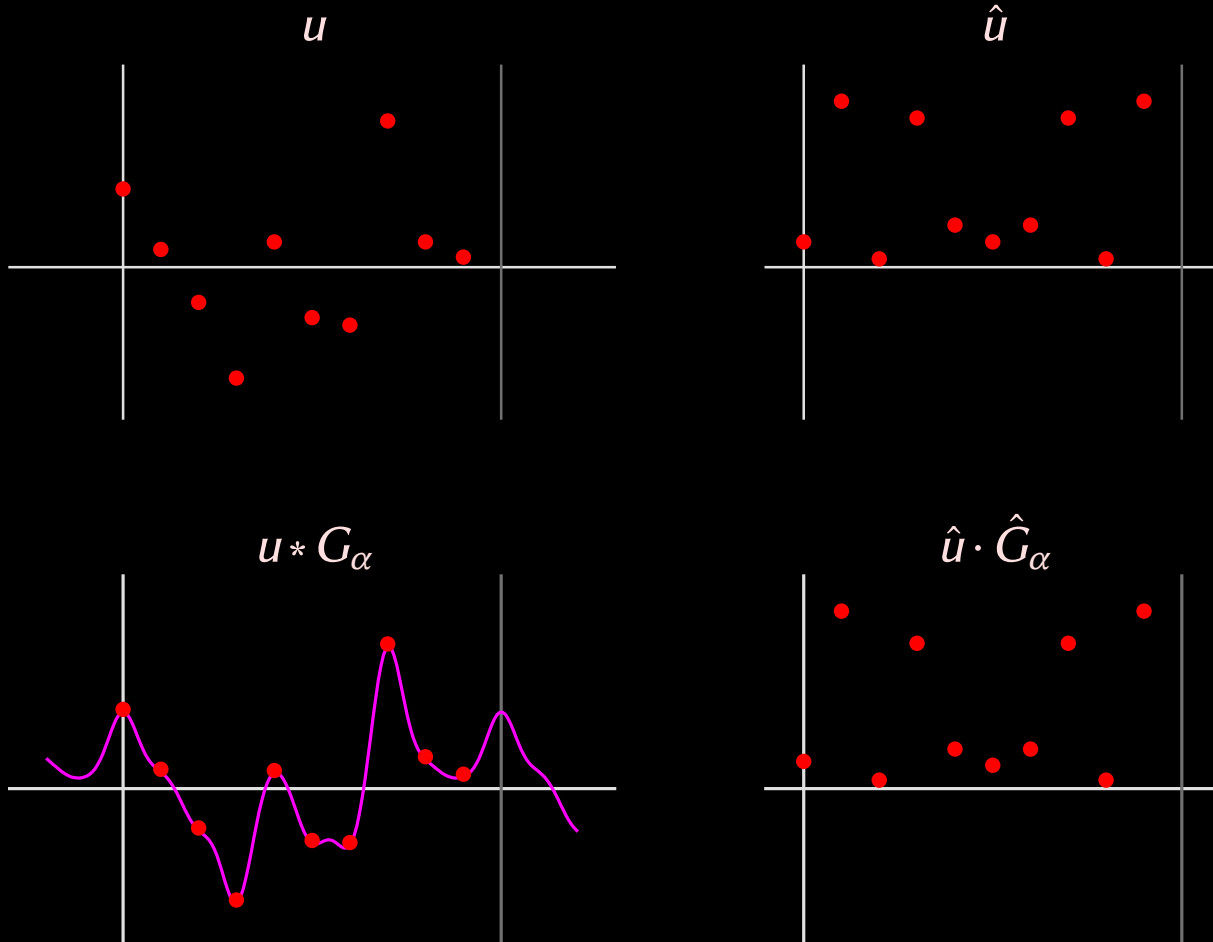


# Gaussian resampling

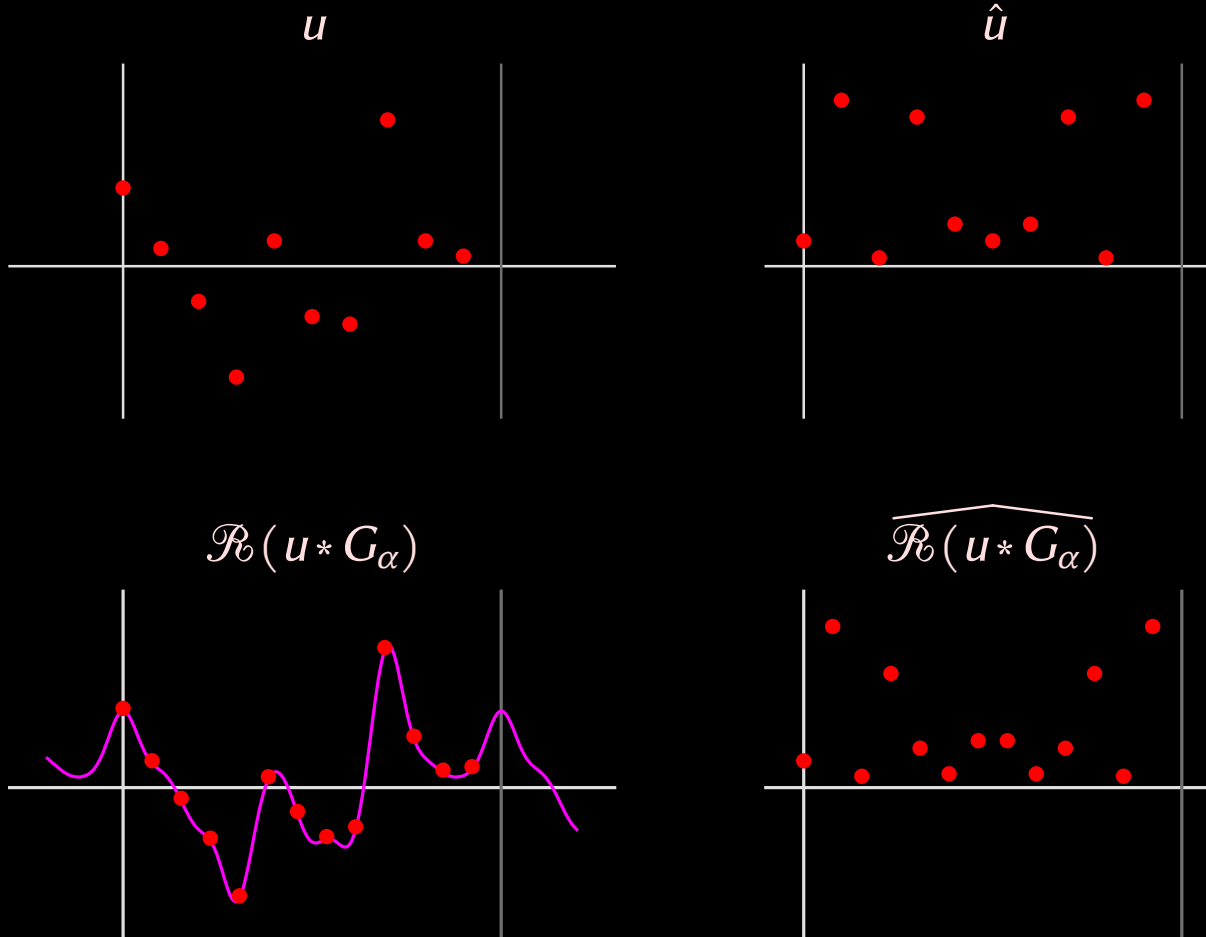




# Gaussian resampling



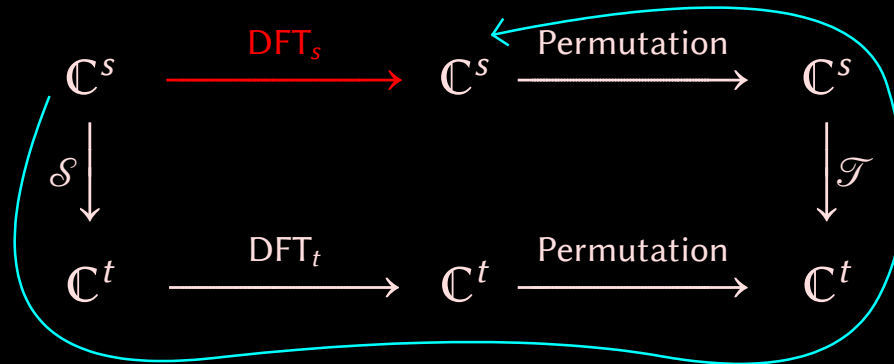
# Gaussian resampling



$$\begin{array}{ccccc}
 \mathbb{C}^s & \xrightarrow{\text{DFT}_s} & \mathbb{C}^s & \xrightarrow{\text{Permutation}} & \mathbb{C}^s \\
 \mathcal{S} \downarrow & & & & \downarrow \mathcal{T} \\
 \mathbb{C}^t & \xrightarrow{\text{DFT}_t} & \mathbb{C}^t & \xrightarrow{\text{Permutation}} & \mathbb{C}^t
 \end{array}$$

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

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



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

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

Matrix for  $\mathcal{S}$  when  $s = 10$ ,  $t = 13$ , and  $\alpha = 2$

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

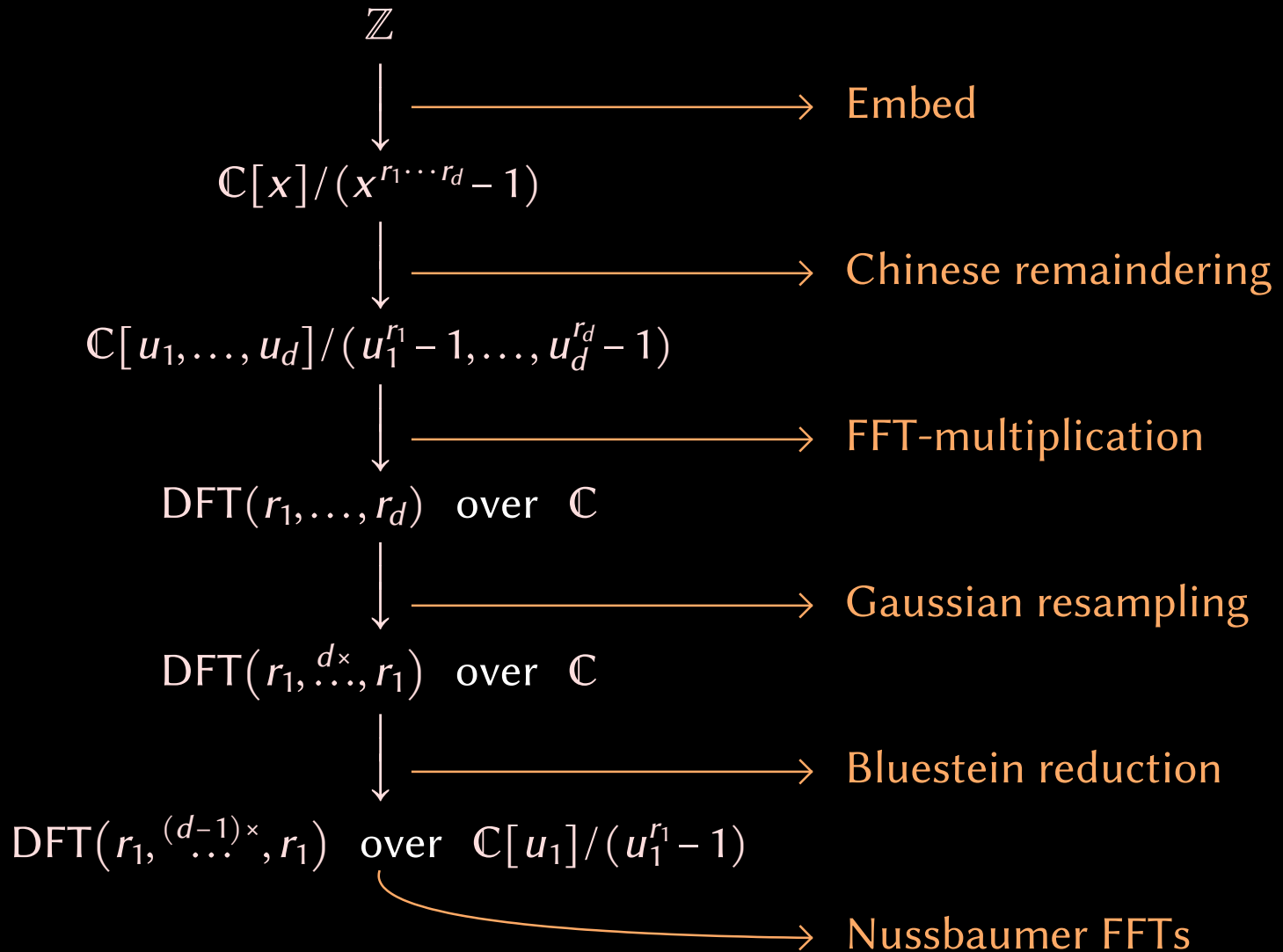
Matrix for  $\mathcal{T}$  when  $s = 10$ ,  $t = 13$ , and  $\alpha = 2$

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

Matrix for  $\mathcal{T}$  when  $s = 10$ ,  $t = 13$ , and  $\alpha = 2$

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

$$\frac{t}{s} \geq 1 + \frac{1}{\alpha^2} \implies \text{accurate DFT}_s \text{ through } \mathbb{C}^s \xrightarrow{\mathcal{S}} \mathbb{C}^t \xrightarrow{\text{DFT}_t} \mathbb{C}^t \xrightarrow{\Pi} \mathbb{C}^t \xrightarrow{\mathcal{T}^{-1}} \mathbb{C}^s \xrightarrow{\Pi} \mathbb{C}^s$$





# Thank you !



<http://www.TEXMACS.org>