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

Joris van der Hoeven

CNRS, visiting professor at PIMS and SFU

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

PIMS, SFU, Burnaby **January 28, 2020**

Motivation

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

Motivation

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

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

Motivation

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

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

Division. $O(M(N))$

Motivation

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

Why study the asymptotic behaviour of M(N) ?

Division. $O(M(N))$

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

Motivation

$M(N)$: 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, π. $O(M(N) \log N)$

$M(N)$: 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, π. $O(M(N)\log N)$

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

Motivation

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

Why study the asymptotic behaviour of M(N) ?

Division. $O(\mathsf{M}(N))$

Gcd. $O(\mathsf{M}(N)\log N)$

Computing e, π. $O(\mathsf{M}(N)\log N)$

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

FFT. $O(\mathsf{M}(n\,p))$, length n, bit-precision $p \geqslant \log n$

Motivation

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

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

Division. $O(\mathsf{M}(N))$

Gcd. $O(\mathsf{M}(N) \log N)$

Computing e, π. $O(\mathsf{M}(N) \log N)$

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

FFT. $O(\mathsf{M}(n\,p))$, length n, bit-precision $p \geqslant \log n$

$\mathsf{M}(N)$ = speed of basic arithmetic

Motivation

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

Why study the asymptotic behaviour of $\mathsf{M}(N)$?

Division. $O(\mathsf{M}(N))$

Gcd. $O(\mathsf{M}(N)\log N)$

Computing e, π. $O(\mathsf{M}(N)\log N)$

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

FFT. $O(\mathsf{M}(n\,p))$, length n, bit-precision $p \geqslant \log n$

$$\mathsf{M}(N) = \text{speed of basic arithmetic}$$

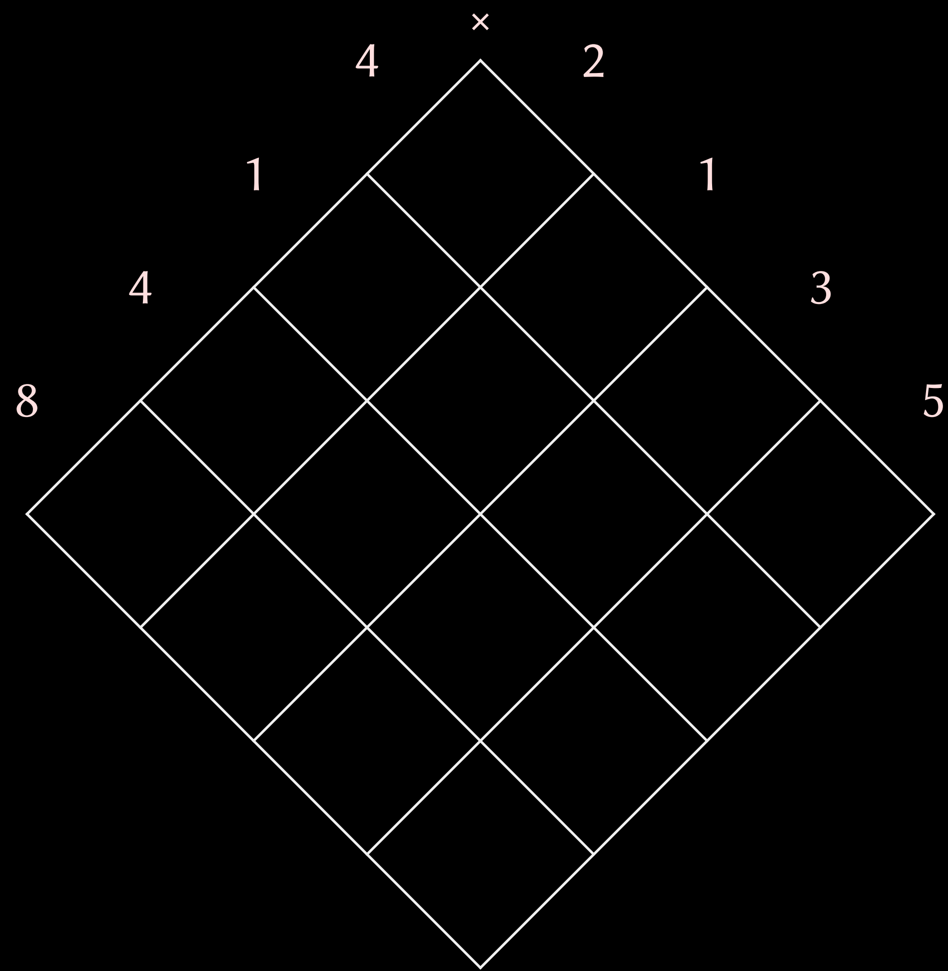
Also

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

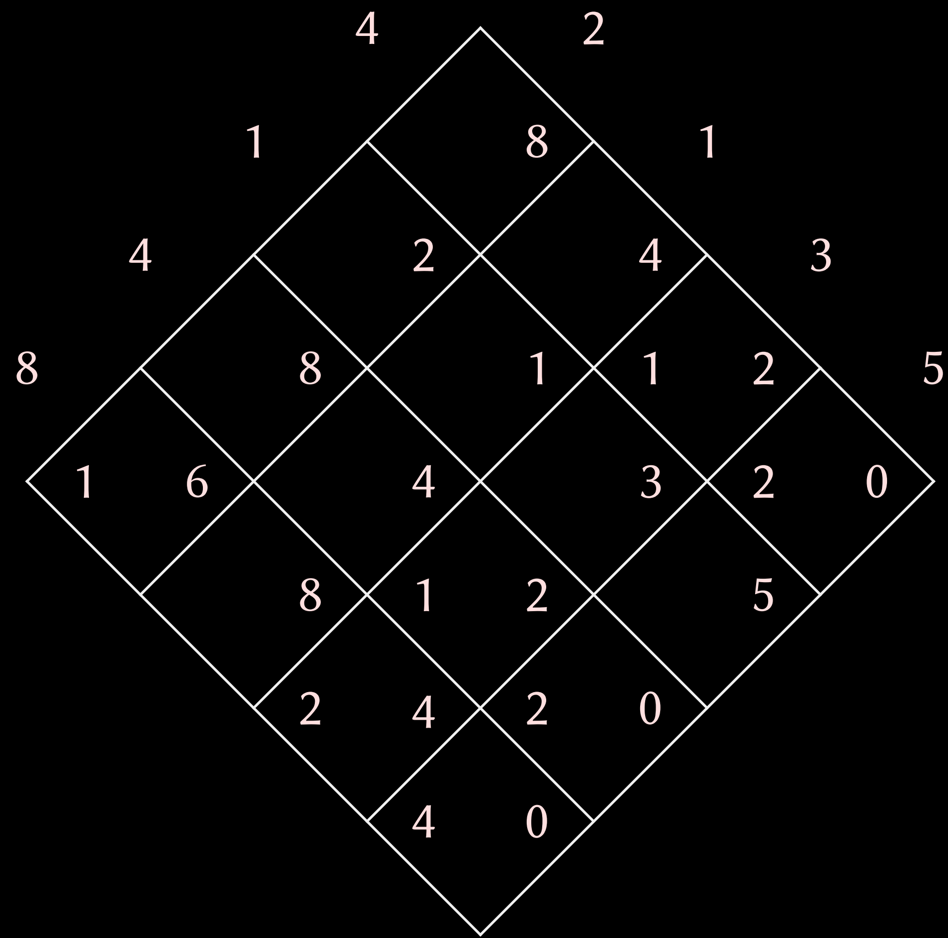
Naive multiplication

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

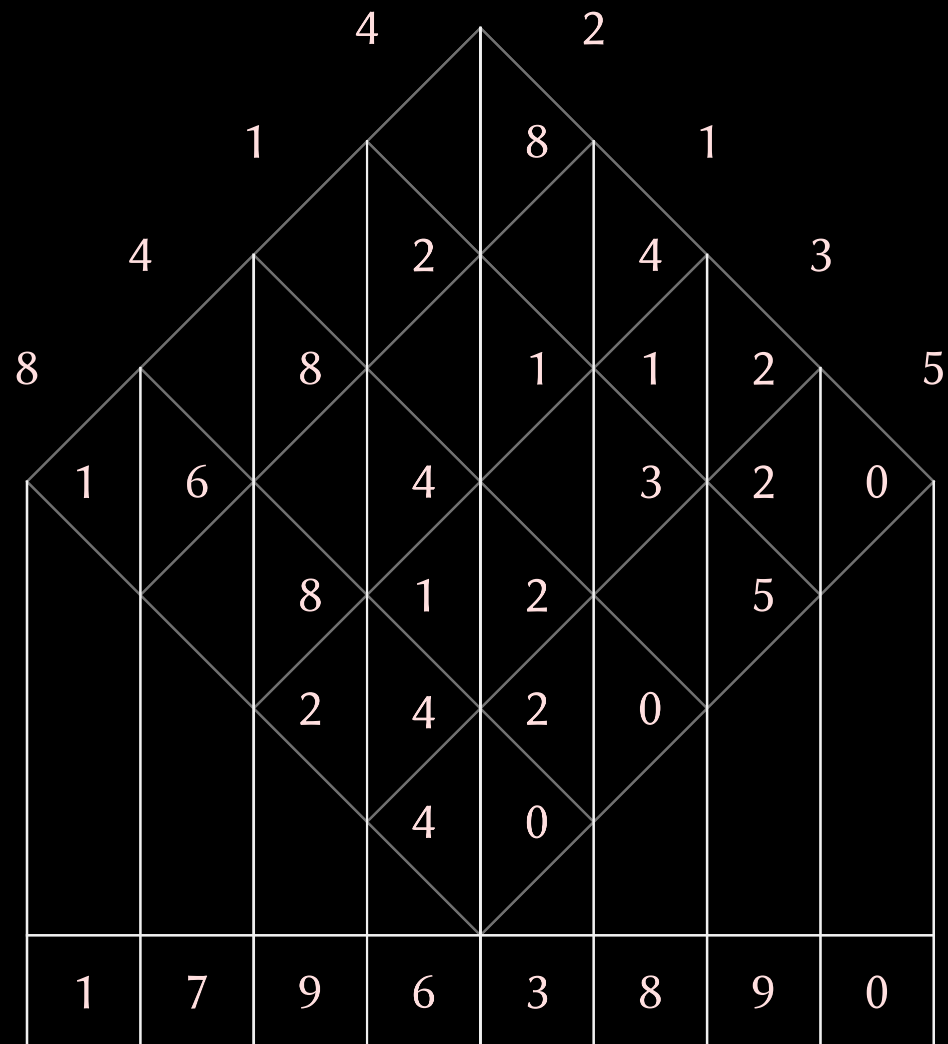
Naive multiplication



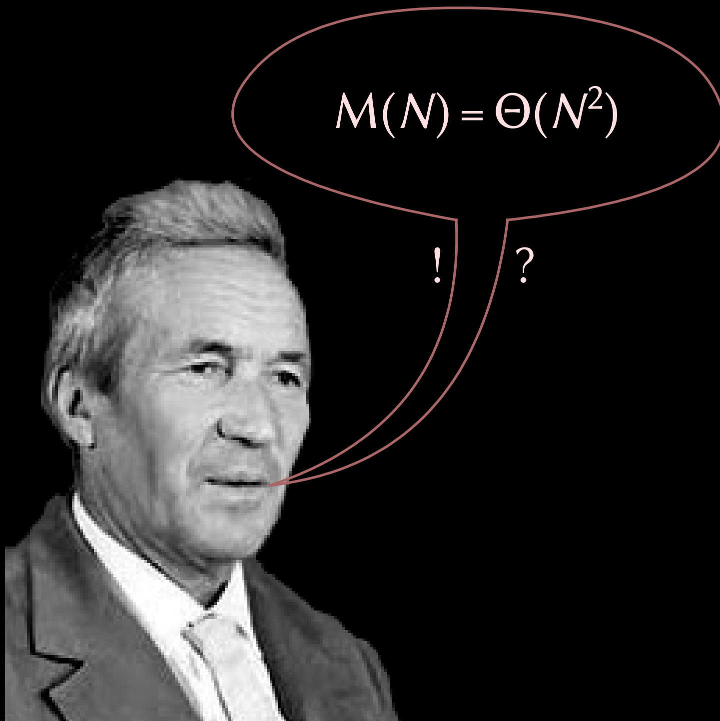
Naive multiplication



Naive multiplication



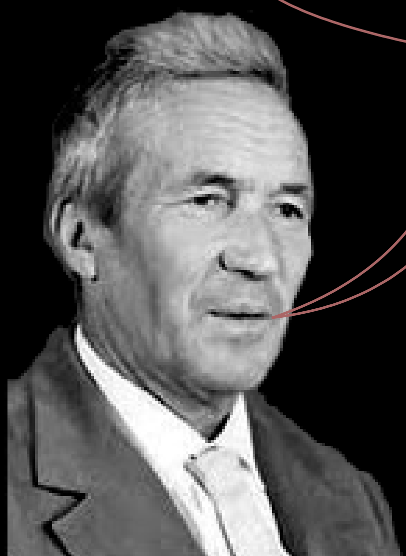
Can we do better?



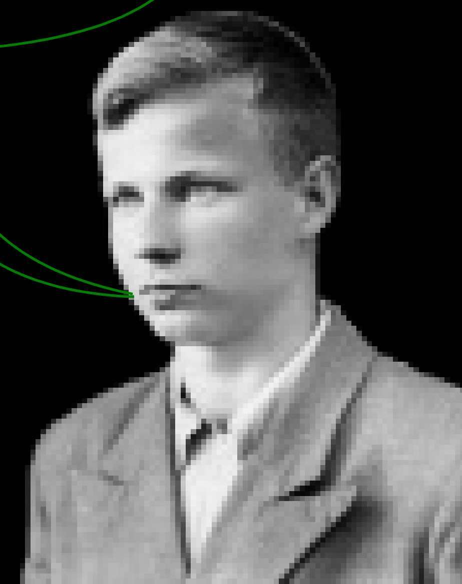
Can we do better?

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

! ?



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



1962

Short history

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	$O(N \log N)$

Kronecker segmentation

$$4627579679788114 \quad \times \quad 4519170871966234$$
$$\wr$$
$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

Integers versus polynomials

Kronecker segmentation

$$4627579679788114 \quad \times \quad 4519170871966234$$
$$\rightsquigarrow$$
$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

Kronecker substitution

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$
$$\rightsquigarrow$$
$$4627000005796000007978000008114 \quad \times \quad 4519000001708000007196000006234$$

Integers versus polynomials

Kronecker segmentation

$$4627579679788114 \quad \times \quad 4519170871966234$$
$$\wr$$
$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

Kronecker substitution

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$
$$\wr$$
$$4627000005796000007978000008114 \quad \times \quad 4519000001708000007196000006234$$

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

Cyclic polynomials

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

n: cycle length

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

Cyclic polynomials

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

n: cycle length

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

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

Cyclic polynomials

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

n: cycle length

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

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

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

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

n: cycle length

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

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

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

Summary so far

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

The Discrete Fourier Transform

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

n : cycle or transform length

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

The Discrete Fourier Transform

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

n : cycle or transform length

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

Chinese remainder theorem

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

The Discrete Fourier Transform

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

n : cycle or transform length

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

Chinese remainder theorem

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

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

The Discrete Fourier Transform

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

n : cycle or transform length

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

Chinese remainder theorem

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

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

The Discrete Fourier Transform

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

n : cycle or transform length

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

Chinese remainder theorem

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

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

Discrete Fourier transform

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

The Discrete Fourier Transform

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

n: cycle or transform length

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

Chinese remainder theorem

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

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

Discrete Fourier transform

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

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

FFT multiplication

$$P \in \mathbb{K}[x]/(x^n - 1) \qquad\qquad Q \in \mathbb{K}[x]/(x^n - 1)$$

$$\downarrow \text{DFT} \qquad\qquad \downarrow \text{DFT}$$

$$\hat{P} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \qquad\qquad \hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\searrow \qquad\qquad \swarrow$$

$$\hat{P}\hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\downarrow \text{DFT}^{-1}$$

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

FFT multiplication

$$P \in \mathbb{K}[x]/(x^n - 1) \qquad\qquad Q \in \mathbb{K}[x]/(x^n - 1)$$

$$\downarrow \text{DFT} \qquad\qquad \downarrow \text{DFT}$$

$$\hat{P} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \qquad\qquad \hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\searrow \qquad\qquad \swarrow$$

$$\hat{P}\hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

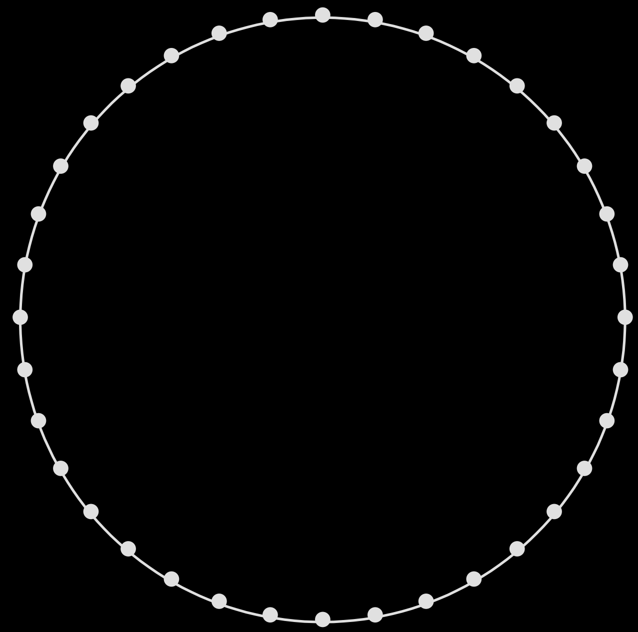
$$\downarrow \text{DFT}^{-1}$$

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

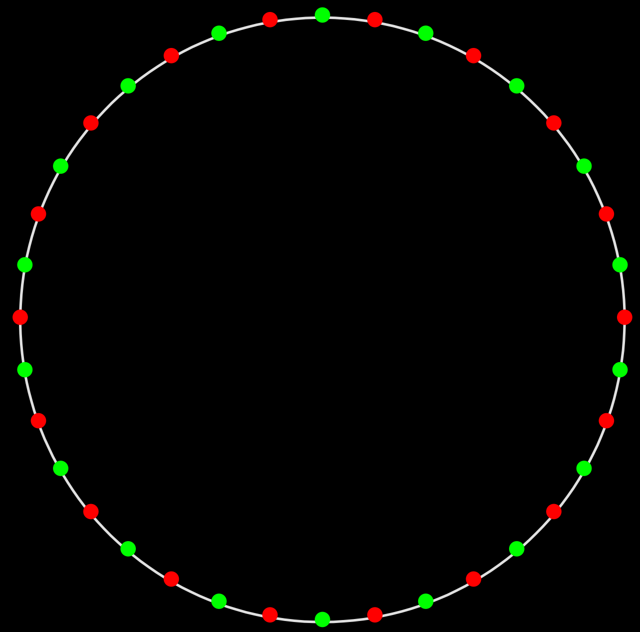
Summary so far

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

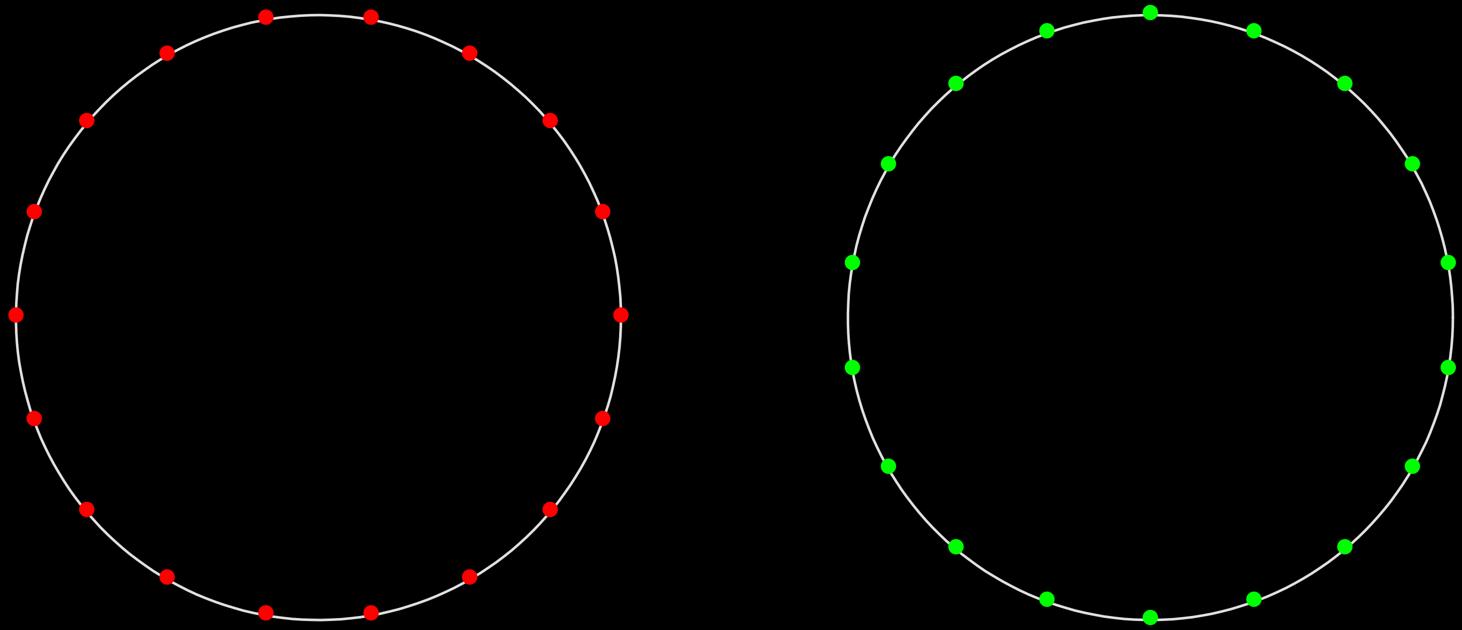
Making the FFT fast

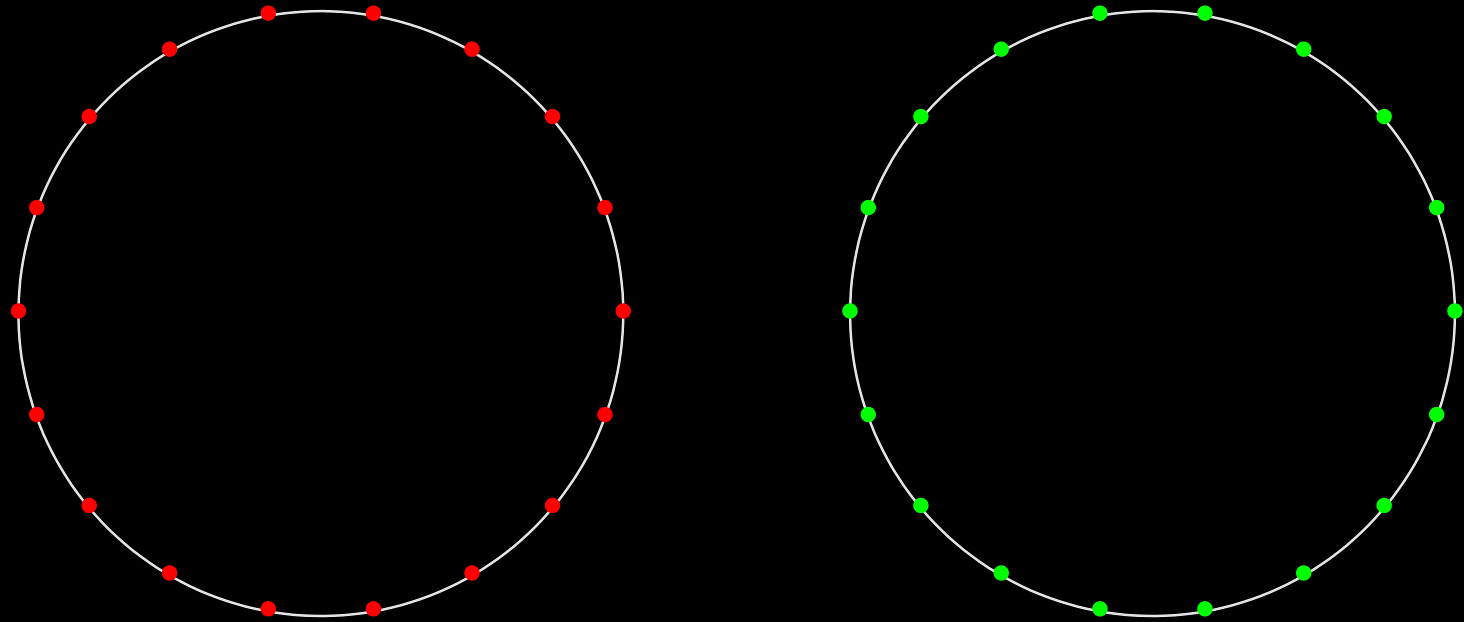


Making the FFT fast

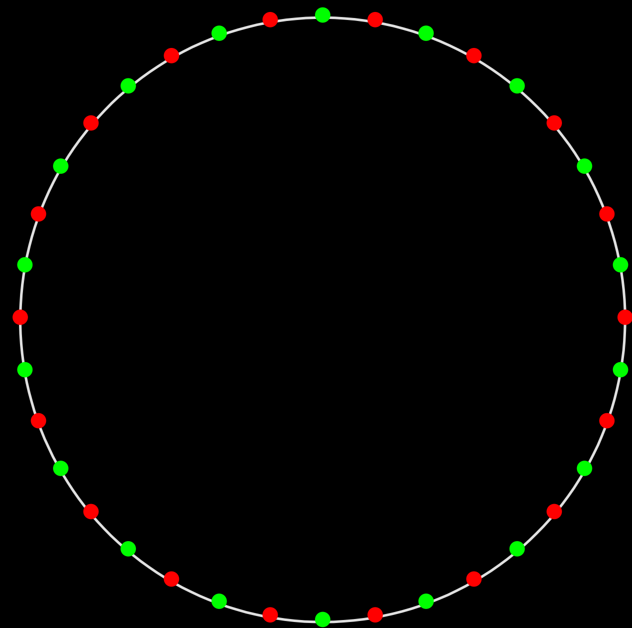


Making the FFT fast



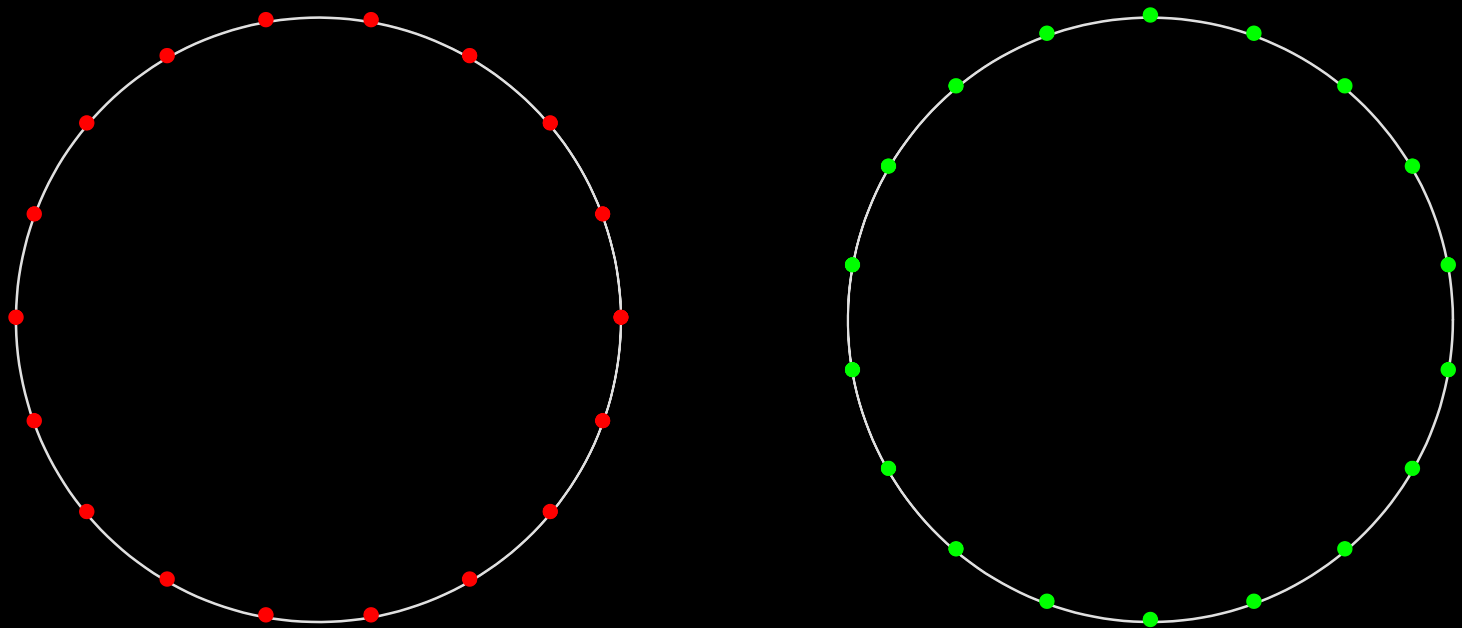


Making the FFT fast



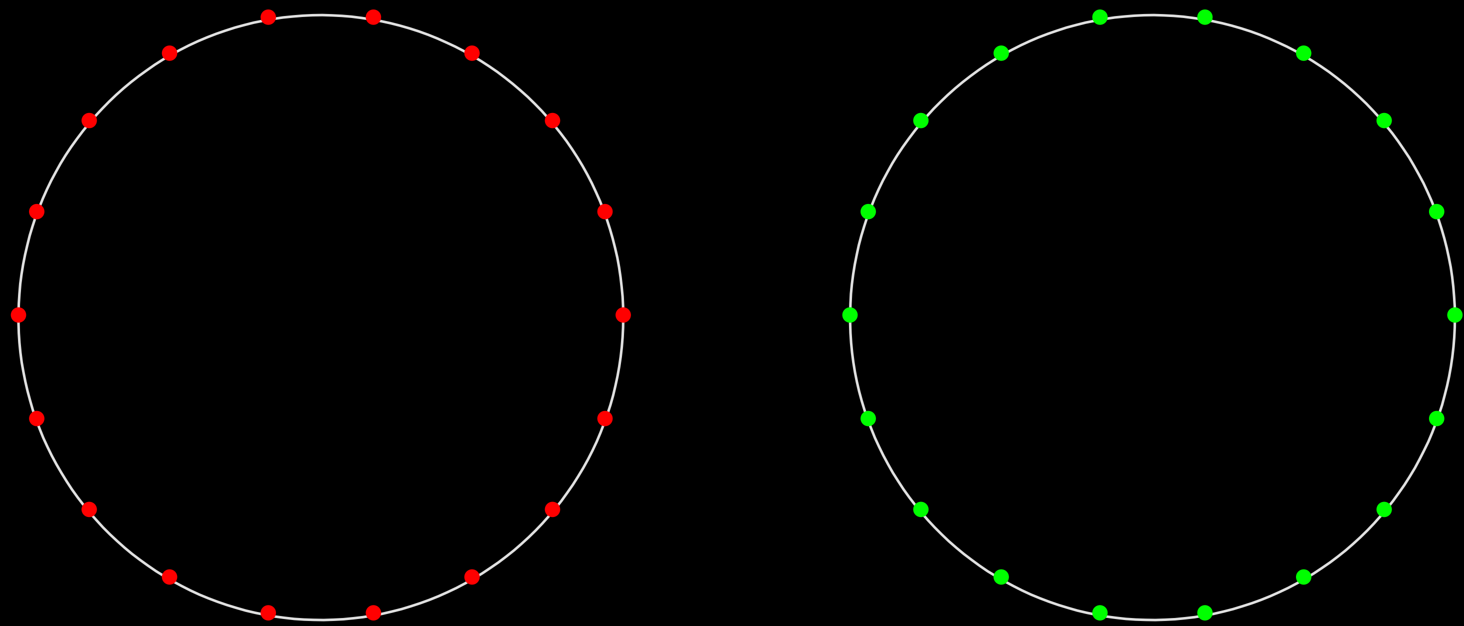
$$\mathbb{K}[x]/(x^{2n} - 1)$$

Making the FFT fast



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

Making the FFT fast



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

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

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

$$\omega^n = -1$$

Complexity analysis

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

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

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

$$\cong$$

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

Complexity analysis

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

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

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

Complexity analysis

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

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

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

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

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

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

How to choose $\mathbb{K}$?

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

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

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

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

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

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

Back to N-bit integer multiplication

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 $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω 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

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

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

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω 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. $\mathsf{M}(N) = O(N\,\mathsf{M}(\log N))$ $\qquad\qquad$ $\mathsf{M}(N) = O(N \log N \log\log N \cdots)$

How to choose $\mathbb{K}$?

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

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω 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. $\mathsf{M}(N) = O(N\,\mathsf{M}(\log N))$ $\qquad$ $\mathsf{M}(N) = O(N \log N \log \log N \cdots)$

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

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

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

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω 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. $\mathsf{M}(N) = O(N\,\mathsf{M}(\log N))$ $\qquad$ $\mathsf{M}(N) = O(N \log N \log \log N \cdots)$

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

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

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

Note about Schönhage–Strassen multiplication

A careful construction yields

$$\mathrm{M}^{\ominus}(n) \leqslant C\,n \log n + 2\,n^{1/2}\,\mathrm{M}^{\ominus}(n^{1/2})$$

A careful construction yields

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

Note about Schönhage–Strassen multiplication

A careful construction yields

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

A careful construction yields

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

Note about Schönhage–Strassen multiplication

What if…

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

What if…

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

Note about Schönhage–Strassen multiplication

What if…

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

Note about Schönhage–Strassen multiplication

What if…

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

Note about Schönhage–Strassen multiplication

What if...

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

Next aim

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

What if…

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

Next aim

$$
M(n) \leqslant C n \log n + (d - \epsilon)\, n^{1 - 1/d} M(n^{1/d}) \quad \text{or}
$$

$$
M\left(\frac{n^d}{d - \epsilon}\right) \leqslant C n^d \log n + n^{d-1} M(n)
$$

Nussbaumer Polynomial Transforms

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

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

Schönhage–Strassen

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

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

Nussbaumer Polynomial Transforms

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

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

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

$$\mathrm{mul}_{\mathbb{L}[u_1, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1)} \leqslant n^{d-1}\,\mathrm{mul}_{\mathbb{L}} + O(n^d \log n)$$

Nussbaumer Polynomial Transforms

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

Schönhage–Strassen

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

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

Nussbaumer

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

$$\mathrm{mul}_{\mathbb{L}[u_1, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1)} \quad \leqslant \quad n^{d-1} \mathrm{mul}_{\mathbb{L}} + O(n^d \log n)$$

Next goal

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

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

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

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

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

$$x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}}$$

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

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

$$x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}}$$

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

$$s_1, \ldots, s_d \quad \text{pairwise coprime}$$

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

Setup

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

Lifting the Chinese remainder theorem

$$s_1, \ldots, s_d \quad \text{pairwise coprime}$$

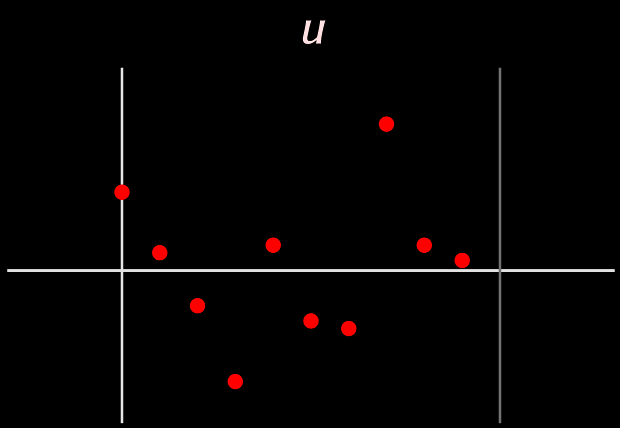
$$\begin{aligned}
\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) &\cong \mathbb{Z}/s_1\mathbb{Z} + \cdots + \mathbb{Z}/s_d\mathbb{Z} \\
x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} &\cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}} \\
\mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1)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

Setup

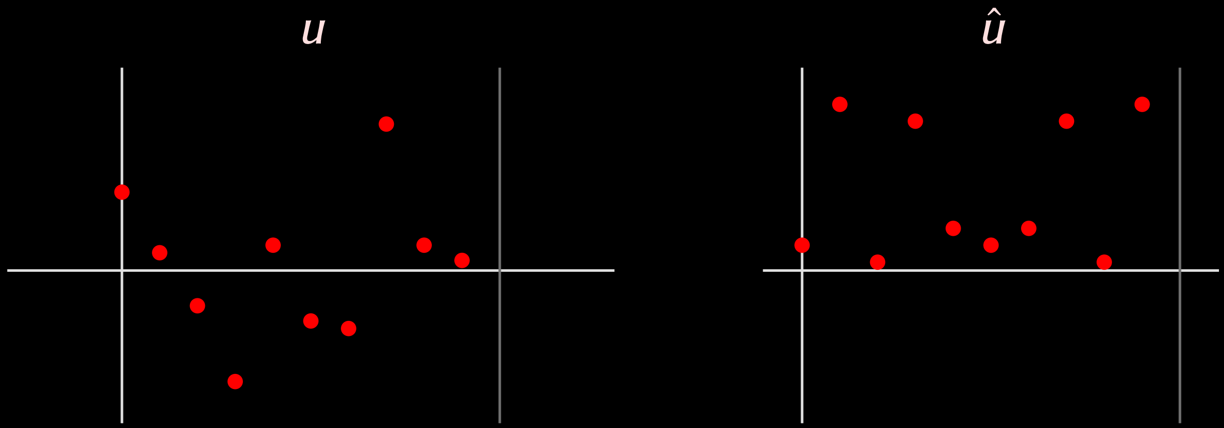
- d fixed once and for all (sufficiently large)
- $s_1 = 2^l$
- $s_k = (1 - o(1))\, 2^l$ or $s_k = (1 - o(1))\, 2^{l-1}$, $\quad k = 2, \ldots, d$

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

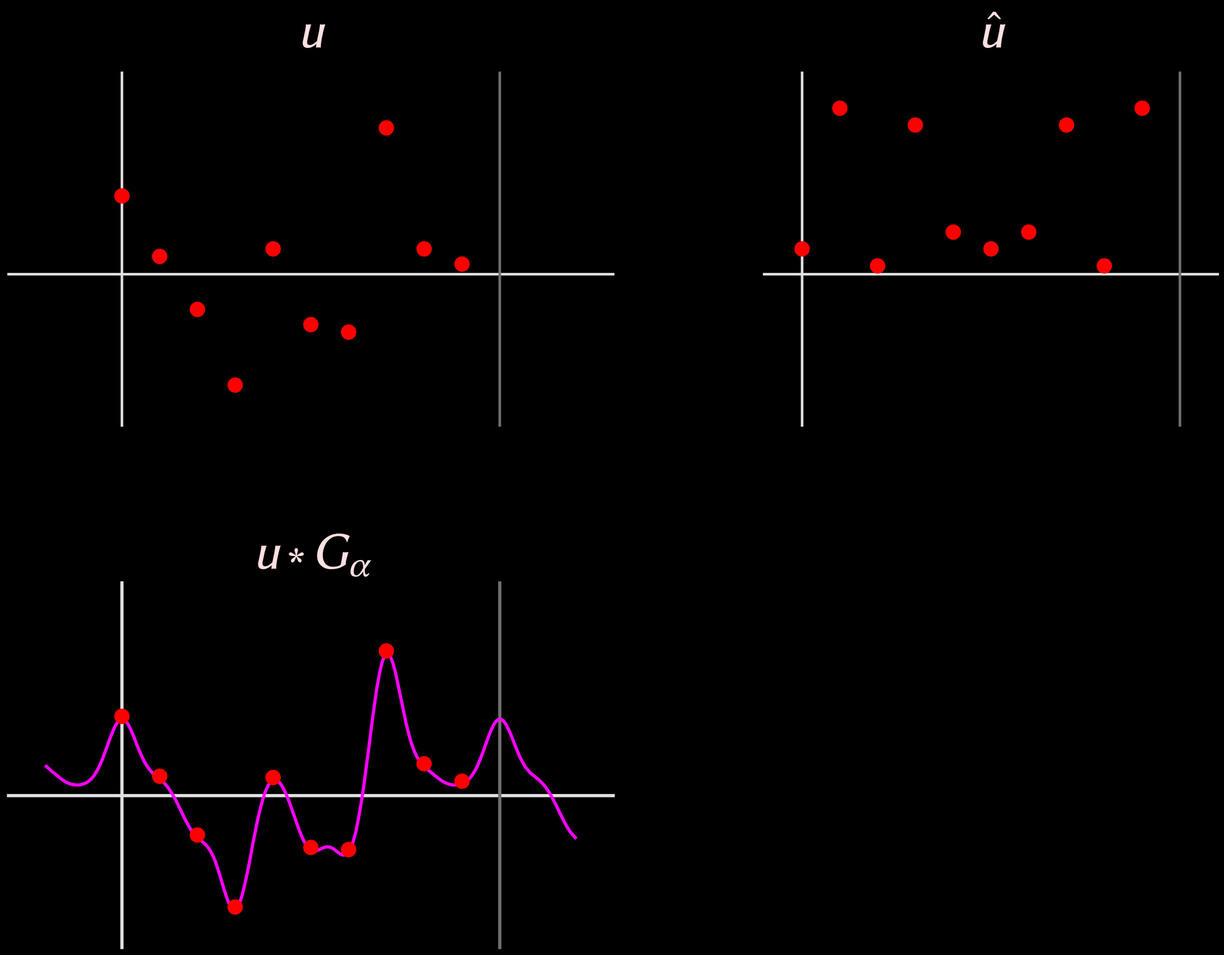
Gaussian resampling



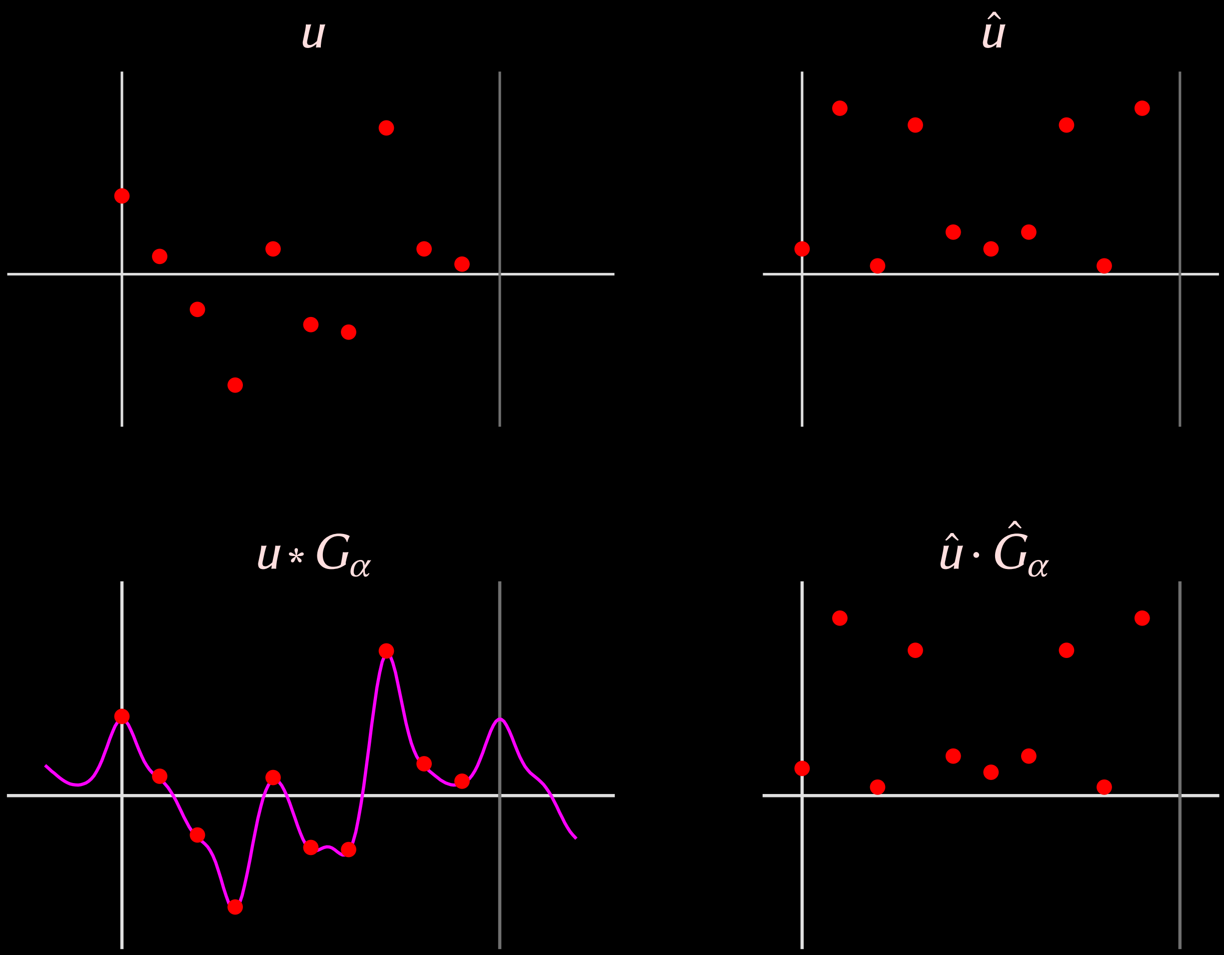
Gaussian resampling



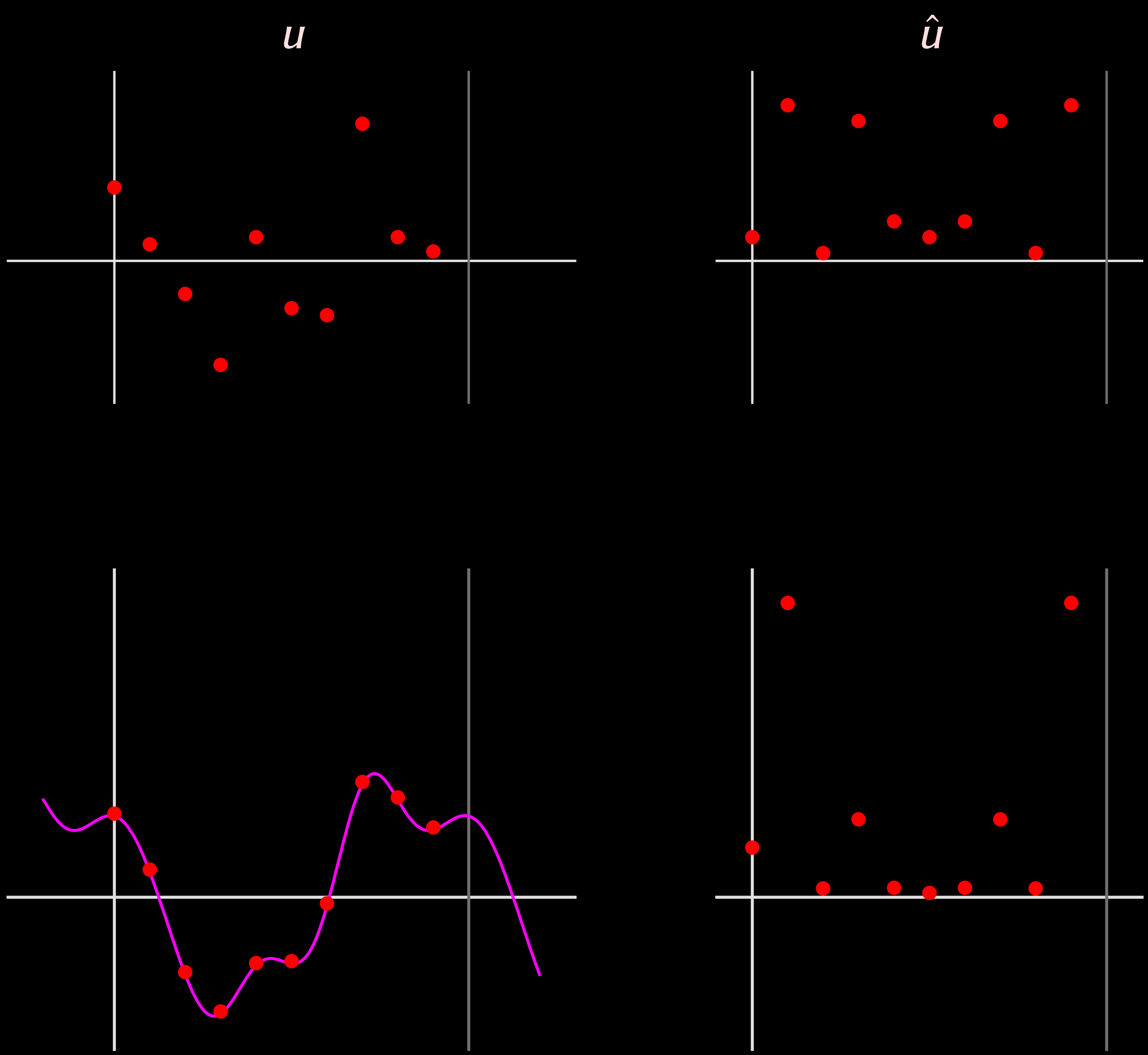
Gaussian resampling



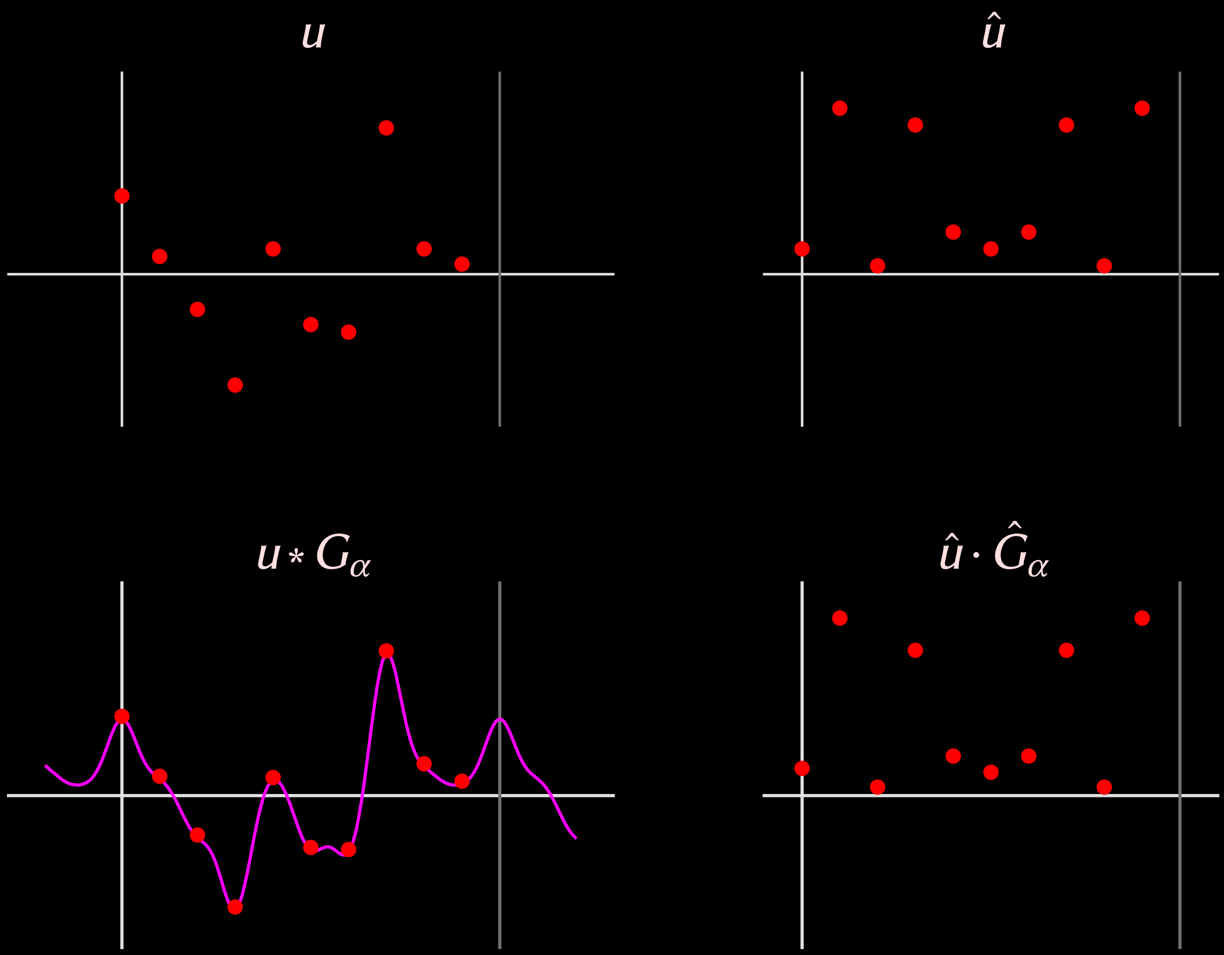
Gaussian resampling



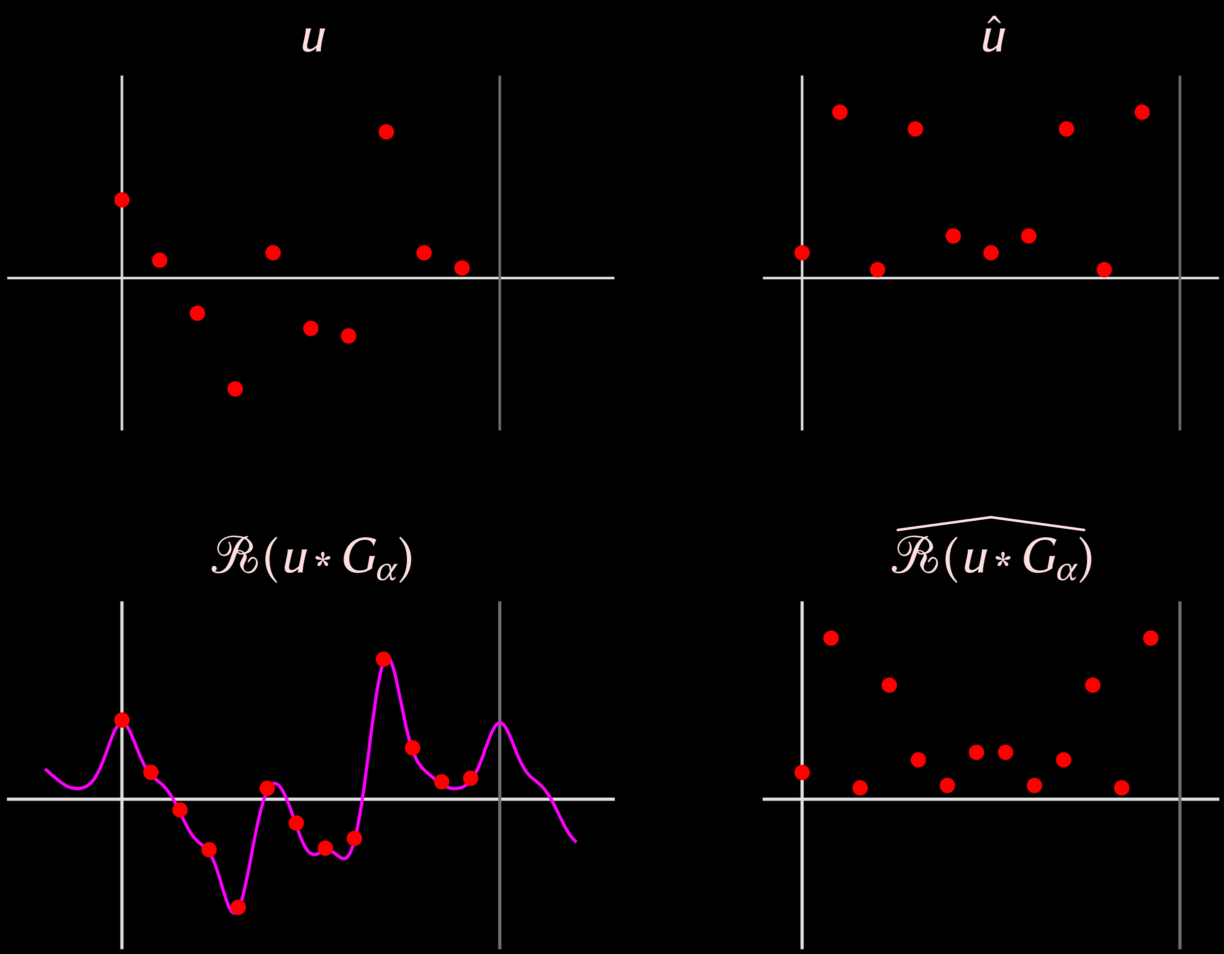
Gaussian resampling



Gaussian resampling



Gaussian resampling



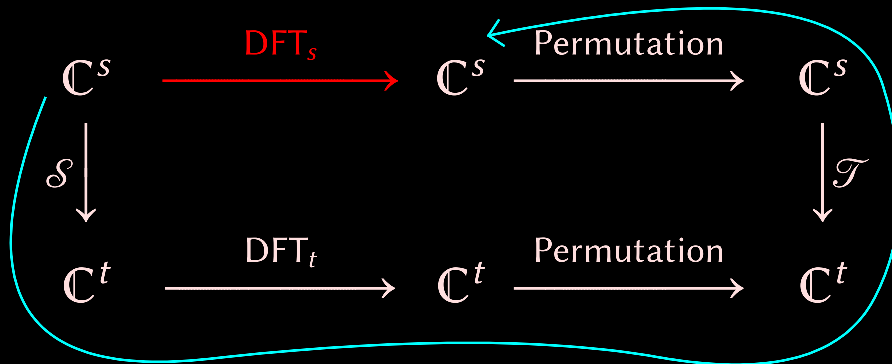
Gaussian resampling

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

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

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

Gaussian resampling



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

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

The resampling matrices

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

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

The resampling matrices

Matrix for $\mathscr{T}$ 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

The resampling matrices

Matrix for $\mathscr{T}$ 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

$\frac{t}{s} \geqslant 1 + \frac{1}{\alpha^2} \implies$ accurate DFT_s through $\mathbb{C}^s \xrightarrow{\mathscr{S}} \mathbb{C}^t \xrightarrow{\mathrm{DFT}_t} \mathbb{C}^t \xrightarrow{\Pi} \mathbb{C}^t \xrightarrow{\mathscr{T}^{-1}} \mathbb{C}^s \xrightarrow{\Pi} \mathbb{C}^s$

Conclusion

$$\mathbb{Z}$$

$\downarrow$ → Embed

$$\mathbb{C}[x]/(x^{r_1 \cdots r_d} - 1)$$

$\downarrow$ → Chinese remaindering

$$\mathbb{C}[u_1, \ldots, u_d]/(u_1^{r_1} - 1, \ldots, u_d^{r_d} - 1)$$

$\downarrow$ → FFT-multiplication

$$\mathrm{DFT}(r_2, \ldots, r_d) \quad \text{over} \quad \mathbb{C}[u_1]/(u_1^{r_1} - 1)$$

$\downarrow$ → Gaussian resampling

$$\mathrm{DFT}(r_1, \ldots, r_1) \quad \text{over} \quad \mathbb{C}[u_1]/(u_1^{r_1} - 1)$$

$\downarrow$ → Bluestein reduction

$$\mathbb{C}[u_1, \ldots, u_d]/(u_1^{r_1} - 1, \ldots, u_d^{r_1} - 1)$$

→ Nussbaumer FFTs

Thank you !

http://www.TeXmacs.org