

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

David Harvey, **Joris van der Hoeven**



$M(N)$: 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, 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)

$M(N)$: 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)

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, π. $O(M(N) \log N)$

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

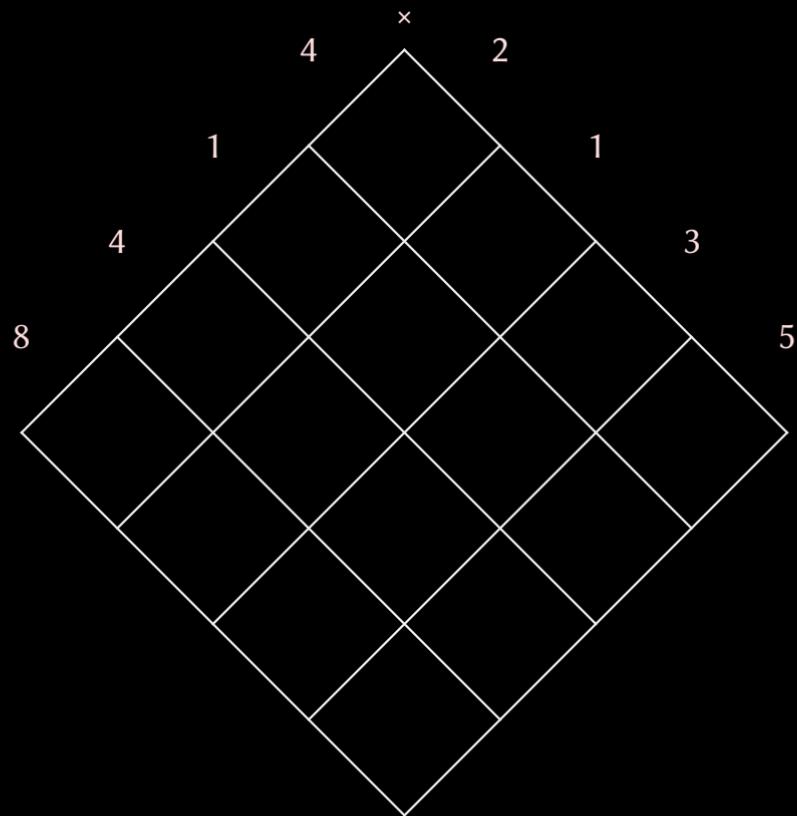
Computing e, π. $O(M(N) \log N)$

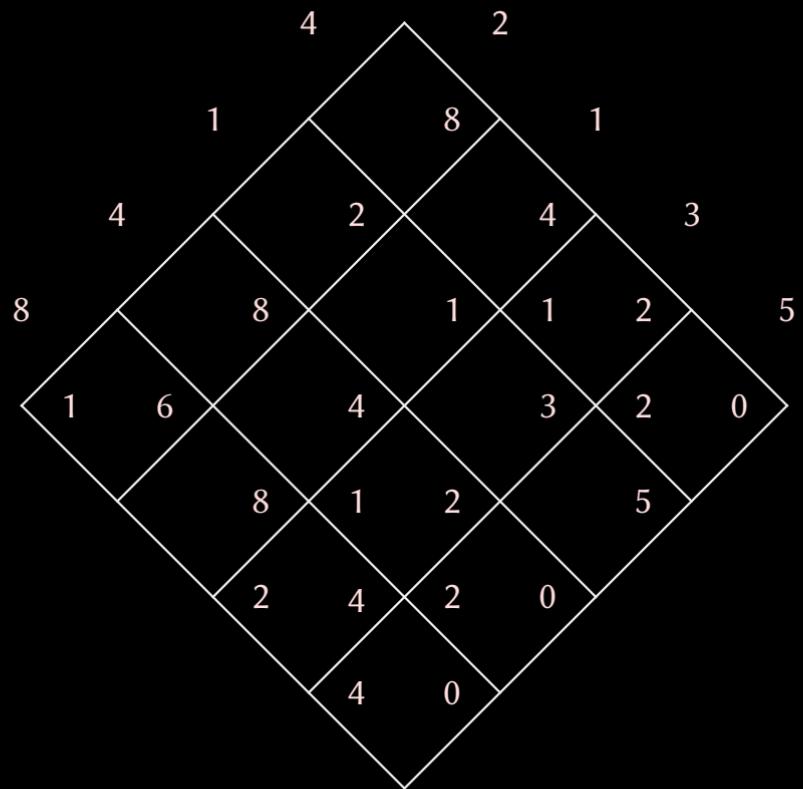
Base conversion. $O\left(M(N) \frac{\log N}{\log \log N}\right)$ (FFT-model)

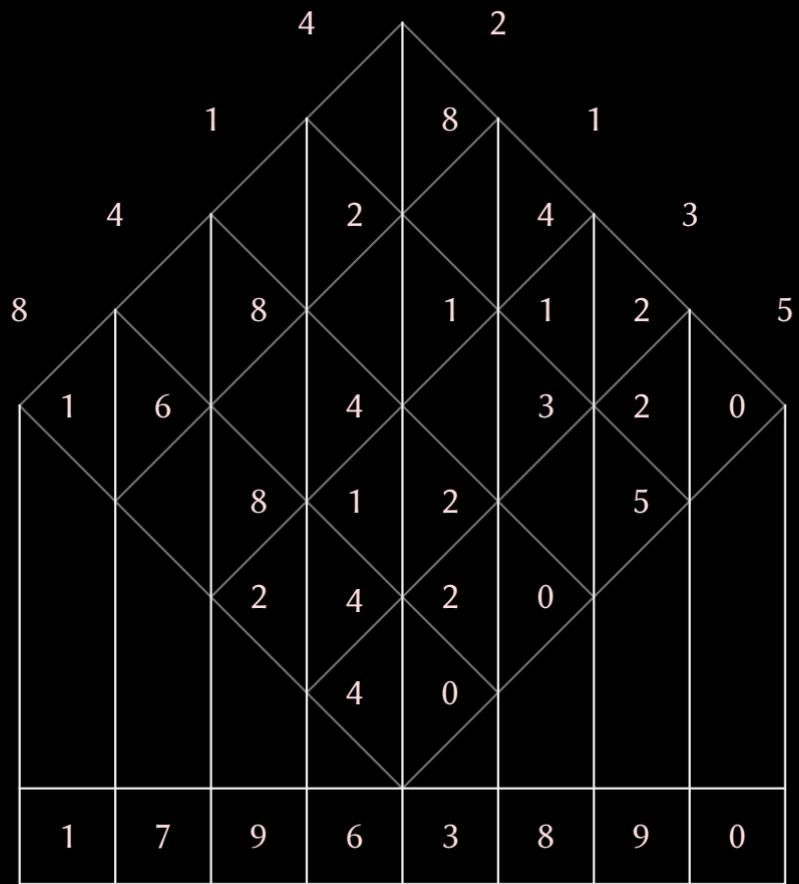
FFT. $O(M(np))$, length n , bit-precision $p \geq \log n$

$M(N)$ = speed of basic arithmetic

- Also**
- Better theoretical techniques $\xrightarrow{\text{often}}$ faster practical implementations
 - Asymptotic complexity abstracts from concrete machines
 - Mechanizing multiplication is a historically fascinating problem







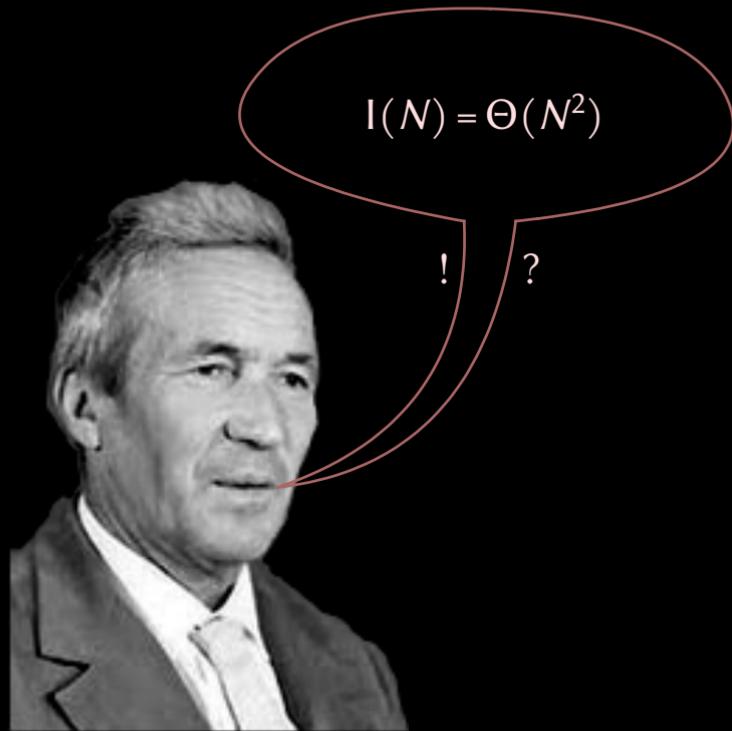
Can we do better?

4/22



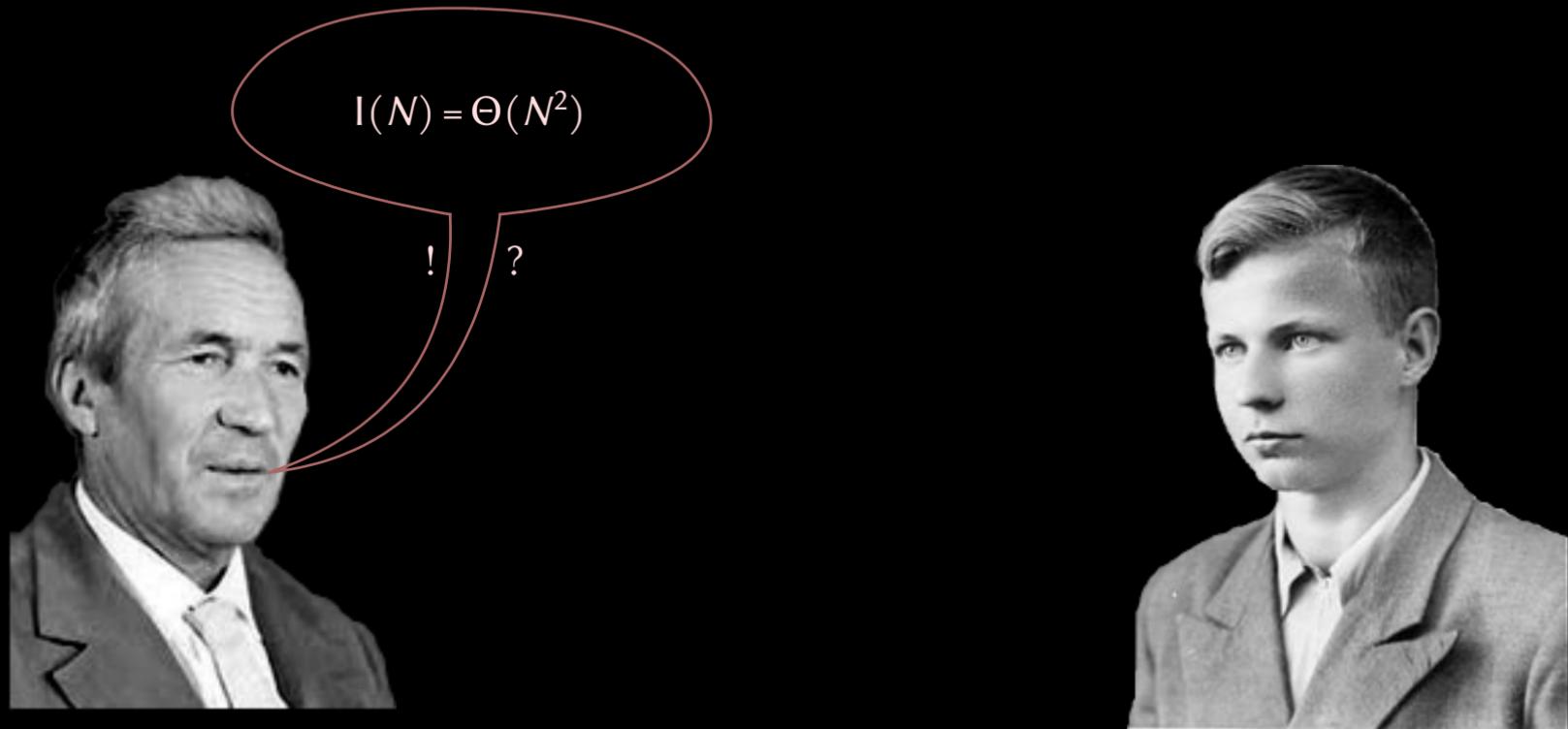
Can we do better?

4/22



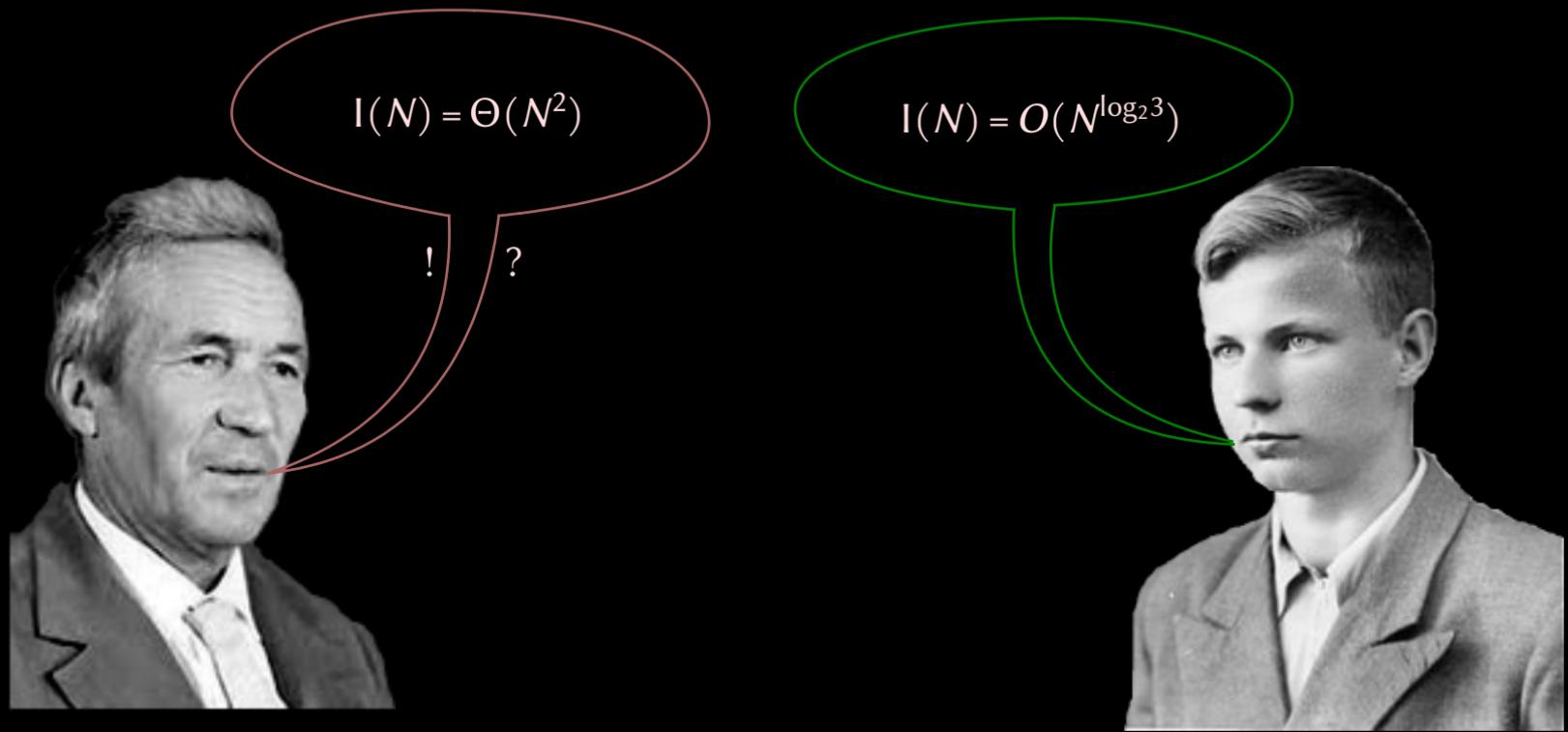
Can we do better?

4/22



Can we do better?

4/22



1962

Short history

| | | |
|------|--------------------|--|
| 1962 | Karatsuba | $O(N^{\log 3/\log 2})$ |
| 1963 | Toom | $O(N 2^{\sqrt{5 \log N / \log 2}})$ |
| 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-Lecercf | $O(N \log N 8^{\log^* N})$ |
| 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

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

Karatsuba multiplication

$$\begin{array}{r} 1302 \quad 2020 \\ \times \quad 3141 \quad 5926 \end{array}$$

Karatsuba multiplication

6/22

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \quad \quad \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

Karatsuba multiplication

6/22

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \quad \quad \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

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

Karatsuba multiplication

6/22

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \quad \quad \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

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

Karatsuba multiplication

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \quad \quad \quad \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

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

$$a \cdot d + b \cdot c = (a + b) \cdot (c + d) - \textcolor{red}{a} \cdot \textcolor{red}{c} - \textcolor{red}{b} \cdot \textcolor{red}{d}$$

Karatsuba multiplication

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

$$(ax + b) \cdot (cx + d) = \textcolor{cyan}{a} \cdot \textcolor{cyan}{c} x^2 + (a \cdot d + b \cdot c)x + \textcolor{red}{b} \cdot \textcolor{red}{d}$$

$$a \cdot d + b \cdot c = (a + b) \cdot (c + d) - \textcolor{cyan}{a} \cdot \textcolor{cyan}{c} - \textcolor{red}{b} \cdot \textcolor{red}{d}$$

Complexity

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

Karatsuba multiplication

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

$$(ax + b) \cdot (cx + d) = \textcolor{teal}{a} \cdot \textcolor{teal}{c} x^2 + (a \cdot d + b \cdot c)x + \textcolor{red}{b} \cdot \textcolor{red}{d}$$

$$a \cdot d + b \cdot c = (a + b) \cdot (c + d) - \textcolor{teal}{a} \cdot \textcolor{teal}{c} - \textcolor{red}{b} \cdot \textcolor{red}{d}$$

Complexity

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

Karatsuba multiplication

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

$$(ax + b) \cdot (cx + d) = \textcolor{teal}{a} \cdot \textcolor{teal}{c} x^2 + (a \cdot d + b \cdot c)x + \textcolor{red}{b} \cdot \textcolor{red}{d}$$

$$a \cdot d + b \cdot c = (a + b) \cdot (c + d) - \textcolor{teal}{a} \cdot \textcolor{teal}{c} - \textcolor{red}{b} \cdot \textcolor{red}{d}$$

Complexity

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

Karatsuba multiplication

$$\begin{array}{r} \underbrace{1302}_a \quad \underbrace{2020}_b \\ \times \quad \end{array} \quad \begin{array}{r} \underbrace{3141}_c \quad \underbrace{5926}_d \end{array}$$

$$(ax + b) \cdot (cx + d) = \textcolor{teal}{a} \cdot \textcolor{teal}{c} x^2 + (a \cdot d + b \cdot c)x + \textcolor{red}{b} \cdot \textcolor{red}{d}$$

$$a \cdot d + b \cdot c = (a + b) \cdot (c + d) - \textcolor{teal}{a} \cdot \textcolor{teal}{c} - \textcolor{red}{b} \cdot \textcolor{red}{d}$$

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

$$4627579679788114 \times 4519170871966234$$

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

Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$

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

Kronecker substitution

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

$$4627000005796000007978000008114 \times 4519000001708000007196000006234$$

Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$

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

Kronecker substitution

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

$$4627000005796000007978000008114 \times 4519000001708000007196000006234$$

$$\textcolor{red}{1004003} \times \textcolor{red}{2001005} = \textcolor{red}{2009015023015}$$

Cyclic polynomials

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

n : cycle length

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

Cyclic polynomials

8/22

\mathbb{K} : a field (or a 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

8/22

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

n : cycle length

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

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

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

Cyclic polynomials

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

n : cycle length

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

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

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

Summary so far

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

The Discrete Fourier Transform

9/22

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

n : cycle or transform length

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

\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

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

\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

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

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

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

n : cycle or transform length

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

Chinese remainder theorem

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

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

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

n : cycle or transform length

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

Chinese remainder theorem

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

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

Discrete Fourier transform

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

\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

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

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

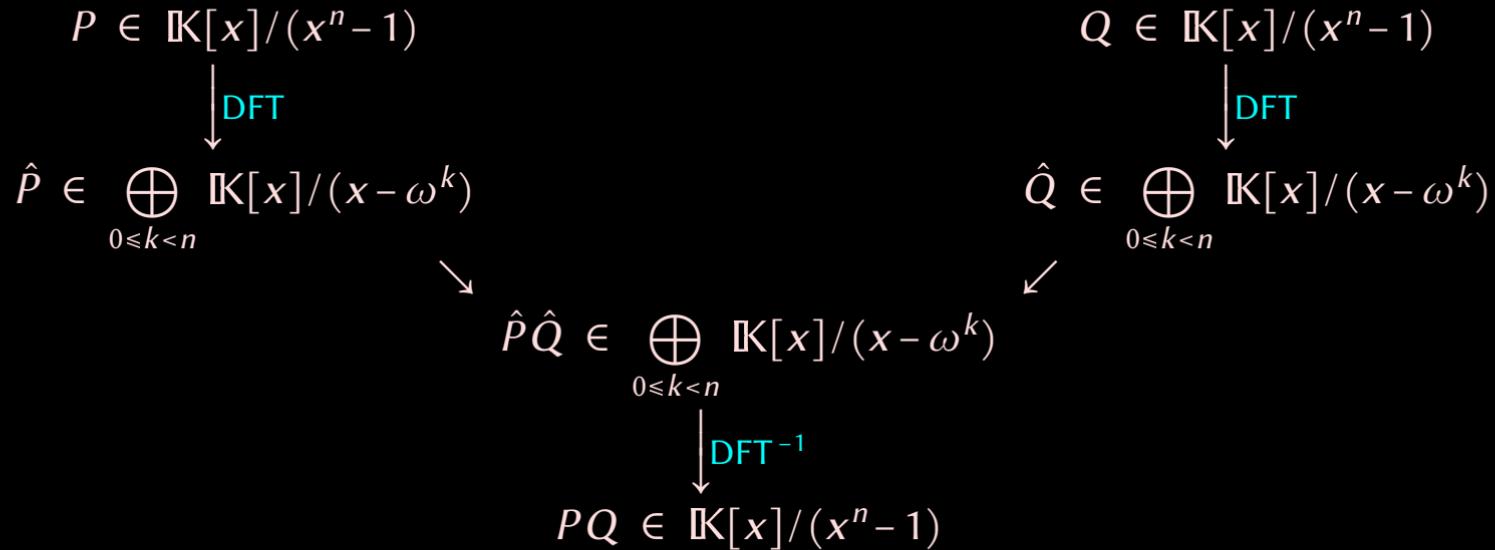
Discrete Fourier transform

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

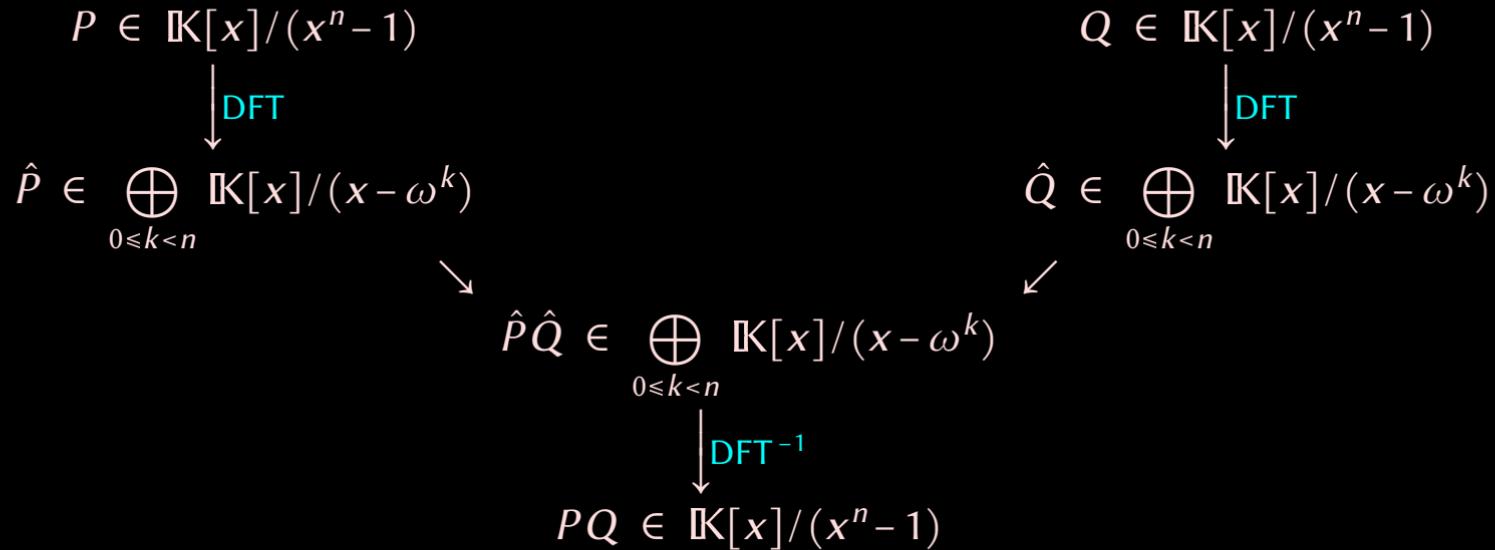
$$\text{DFT}_\omega^{-1} \quad \frac{1}{n} \text{DFT}_{\omega^{-1}}$$

FFT multiplication

10/22



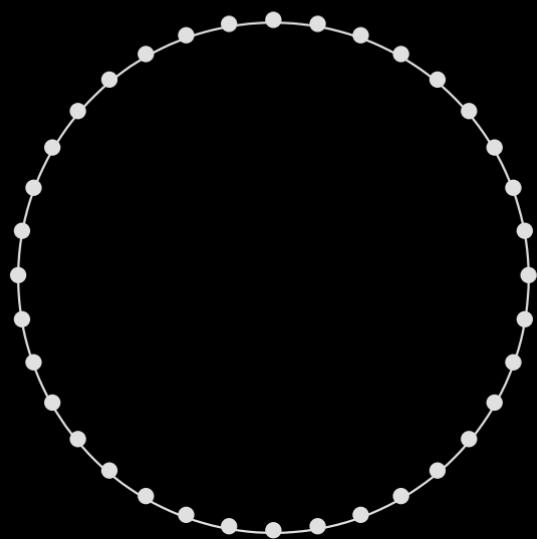
FFT multiplication



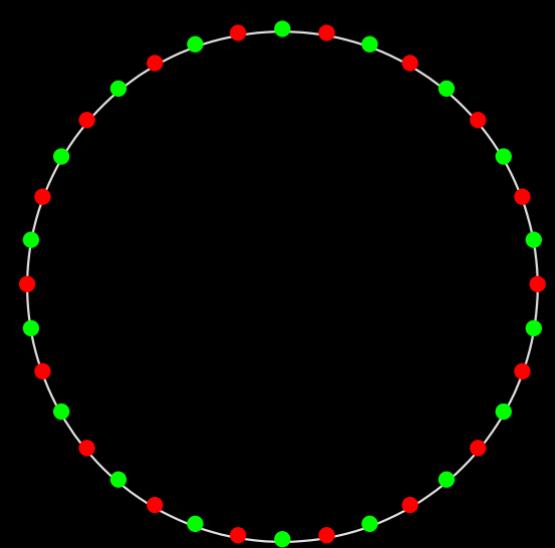
Summary so far

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

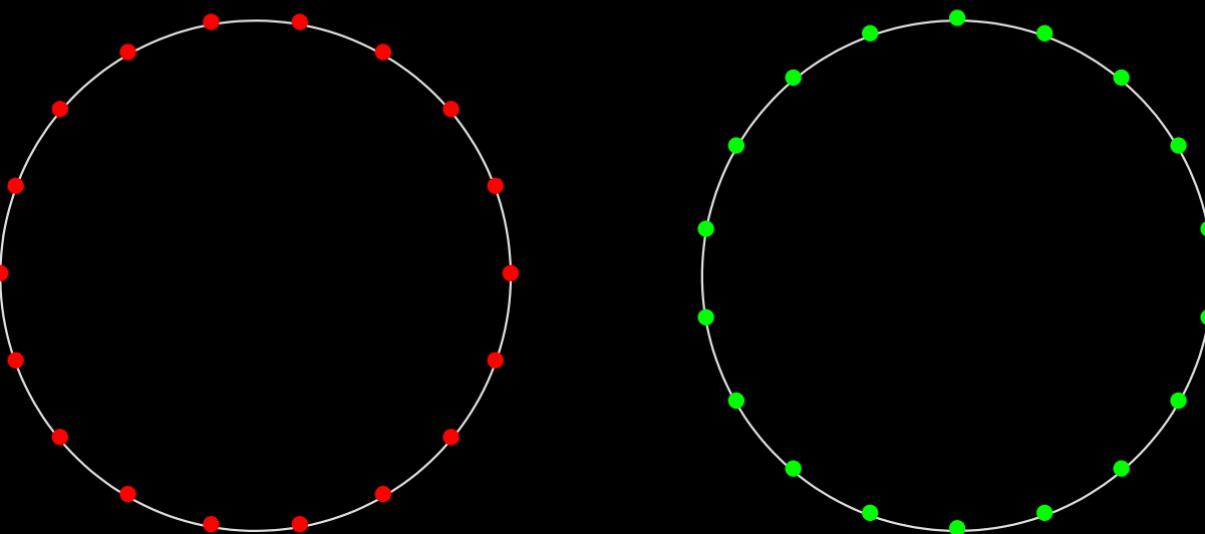
Making the FFT fast



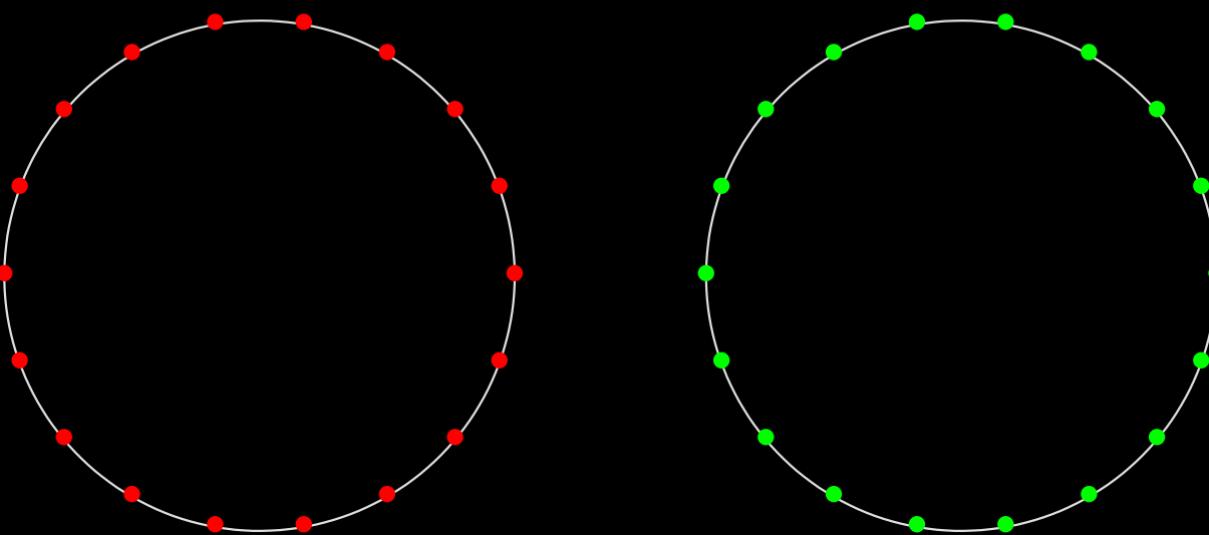
Making the FFT fast



Making the FFT fast

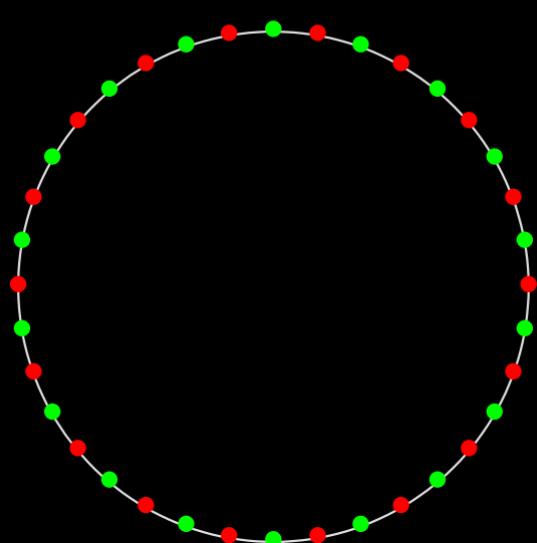


Making the FFT fast



Making the FFT fast

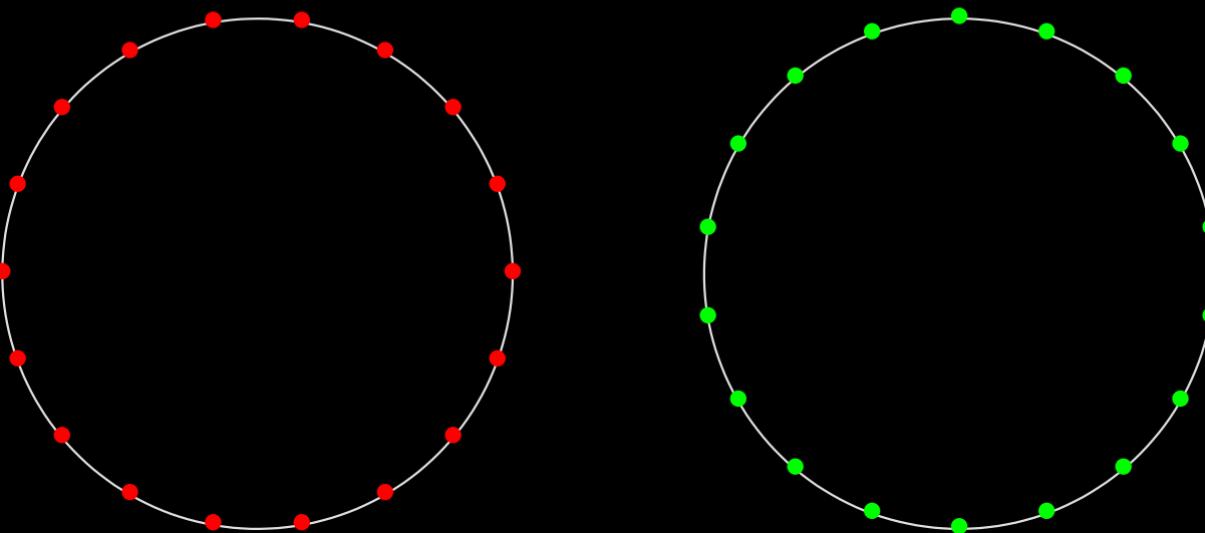
11/22



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

Making the FFT fast

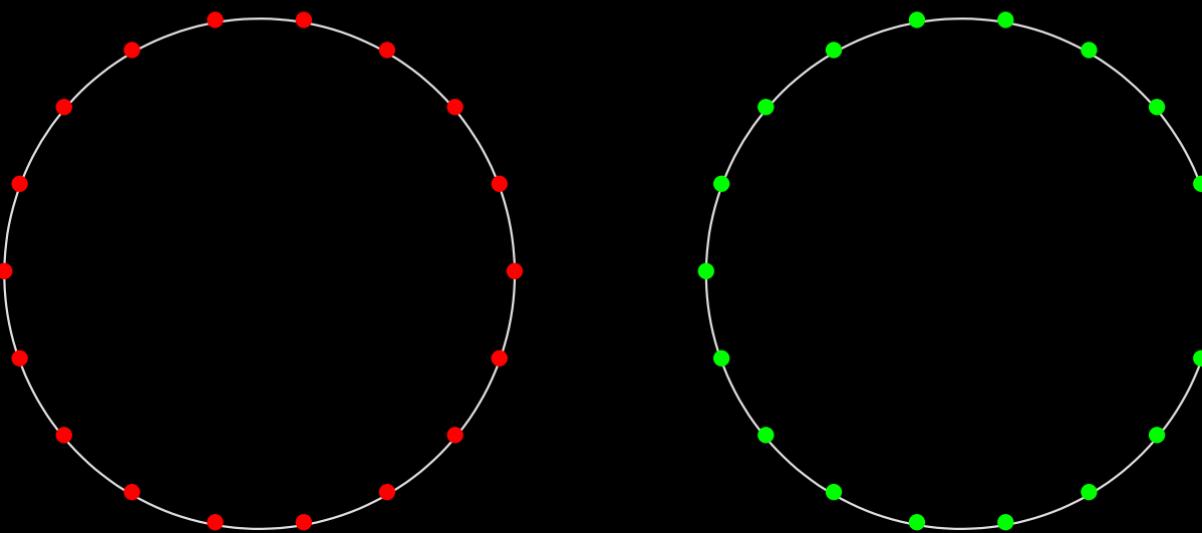
11/22



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

Making the FFT fast

11/22



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

Complexity analysis

12/22

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

Complexity analysis

12/22

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



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

\cong

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

Complexity analysis

12/22

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

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

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

Complexity analysis

12/22

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

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

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

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

How to choose 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 $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω 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 $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists...

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

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 $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, 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

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 $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, 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. $M(N) = O(NM(\log N))$ $M(N) = O(N \log N \log \log N \dots)$

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 $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, 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. $M(N) = O(NM(\log N))$ | $M(N) = O(N \log N \log \log N \dots)$ |
| II. $M(N) = O(NM(\log N))$ | $M(N) = O(N \log N \log \log N \dots)$ |

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 $p = s2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, 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. $M(N) = O(NM(\log N))$ $M(N) = O(N \log N \log \log N \dots)$
- 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

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

A careful construction yields

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

A careful construction yields

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

A careful construction yields

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

What if...

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

What if...

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

Note about Schönhage–Strassen multiplication

14/22

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

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

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

Nussbaumer Polynomial Transforms

15/22

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

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

Schönhage–Strassen

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

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

Schönhage–Strassen

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

Nussbaumer

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

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

Schönhage–Strassen

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

Nussbaumer

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

What if...

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

Lifting the Chinese remainder theorem

16/22

s_1, \dots, s_d pairwise coprime

Lifting the Chinese remainder theorem

16/22

s_1, \dots, s_d pairwise coprime

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

Lifting the Chinese remainder theorem

16/22

s_1, \dots, s_d pairwise coprime

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

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

Lifting the Chinese remainder theorem

16/22

s_1, \dots, s_d pairwise coprime

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

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

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

s_1, \dots, s_d pairwise coprime

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

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

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

Conclusion

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

Achieved: s_1, \dots, s_d pairwise coprime

Required: $s_1 = \cdots = s_d = n$

Lifting the Chinese remainder theorem

16/22

s_1, \dots, s_d pairwise coprime

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

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

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

Conclusion

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

Achieved: s_1, \dots, s_d pairwise coprime

Required: $s_1 = \cdots = s_d = n$

What if... possible to slightly change s_1, \dots, s_d ?

Rader reduction

17/22

DFT of length $p=5$

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

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

Rader reduction

17/22

DFT of length $p=5$

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

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

Rader reduction

17/22

DFT of length $p=5$

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

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^3, \quad 4 = 2^2 \pmod{5}$$

Rader reduction

DFT of length $p=5$

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

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^3, \quad 4 = 2^2 \pmod{5}$$

Rader reduction

17/22

DFT of length $p=5$

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

\uparrow \uparrow $a_4 \leftarrow$ $a_3 \leftarrow$

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^3, \quad 4 = 2^2 \pmod{5}$$

Rader reduction

17/22

DFT of length $p=5$

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

Rader reduction

17/22

DFT of length $p=5$

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

\Updownarrow

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

modulo $x^4 - 1$

Rader reduction

DFT of length $p=5$

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

\Updownarrow

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

modulo $x^4 - 1$

$$F(p) \leq M_{\mathbb{K}, \text{fixed}}^{\circ}(p-1) + 2p \cdot \text{add}_{\mathbb{K}}$$

$M_{\mathbb{K}}^{\circ}(n)$: cost of one multiplication in $\mathbb{K}[x]/(x^n - 1)$

$M_{\mathbb{K}, \text{fixed}}^{\circ}(n)$: when one argument is fixed

Rader reduction

DFT of length $p=5$

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

⇓

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

modulo $x^4 - 1$

$$\begin{aligned} F_{\mathbb{K}}(p) &\leq M_{\mathbb{K}, \text{fixed}}^{\circ}(p-1) + 2p \cdot \text{add}_{\mathbb{K}} \\ &\leq 2F_{\mathbb{K}}(p-1) + 2p \cdot \text{add}_{\mathbb{K}} \end{aligned}$$

$M_{\mathbb{K}}^{\circ}(n)$: cost of one multiplication in $\mathbb{K}[x]/(x^n - 1)$

$M_{\mathbb{K}, \text{fixed}}^{\circ}(n)$: when one argument is fixed

Univariate reduction

$$\text{FFT in } \mathbb{K}[x]/(x^p - 1) \longrightarrow \text{multiplication in } \mathbb{K} \oplus \mathbb{K}[x]/(x^{p-1} - 1)$$

Multivariate reduction

$$\text{FFT in } \bigotimes_{1 \leq i \leq d} \mathbb{K}[x_i]/(x_i^{p_i} - 1) \longrightarrow \text{multiplication in } \bigotimes_{1 \leq i \leq d} (\mathbb{K} \oplus \mathbb{K}[x_i]/(x_i^{p_i-1} - 1))$$

Essentially

$$\mathbb{K}[x]/(x^{p_1 \cdots p_d} - 1) \longrightarrow \mathbb{K}[u_1, \dots, u_d]/(u_1^{p_1-1} - 1, \dots, u_d^{p_d-1} - 1)$$

How to choose our primes

19/22

$$p_i = q_i 2^l + 1, \quad q_i \ll 2^l, \quad q_i \text{ odd prime}, \quad i = 1, \dots, d$$

How to choose our primes

19/22

$$p_i = q_i 2^l + 1, \quad q_i \ll 2^l, \quad q_i \text{ odd prime}, \quad i = 1, \dots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

How to choose our primes

19/22

$$p_i = q_i 2^l + 1, \quad q_i \ll 2^l, \quad q_i \text{ odd prime}, \quad i = 1, \dots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

How to choose our primes

19/22

$$p_i = q_i 2^l + 1, \quad q_i \ll 2^l, \quad q_i \text{ odd prime}, \quad i = 1, \dots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

| | |
|------------|---|
| $l = 8$ | $q = 3, 13, 31, 37, 157, 163, 181, 193, \dots$ |
| $l = 16$ | $q = 37, 103, 307, 313, 397, 421, 487, 541, \dots$ |
| $l = 32$ | $q = 43, 73, 157, 181, 211, 433, 571, 601, \dots$ |
| $l = 64$ | $q = 163, 337, 487, 907, 1051, 1297, 1453, 1567, \dots$ |
| $l = 128$ | $q = 1171, 2551, 3607, 3907, 4021, 4483, 4567, 4603, \dots$ |
| $l = 256$ | $q = 607, 1567, 1783, 2683, 2797, 4993, 6577, 6871, \dots$ |
| $l = 512$ | $q = 223, 2083, 2803, 3853, 4783, 9403, 9781, 10303, \dots$ |
| $l = 1024$ | $q = 1987, 4447, 15031, 22807, 26713, 46153, 46507, 47653, \dots$ |

How to choose our primes

19/22

$$p_i = q_i 2^l + 1, \quad q_i \ll 2^l, \quad q_i \text{ odd prime}, \quad i = 1, \dots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

$$\begin{aligned} & \mathbb{K}[x_1, \dots, x_d]/(x_1^{p_1-1} - 1, \dots, x_d^{p_d-1} - 1) \\ & \cong \mathbb{K}[u_1, \dots, u_d, v_1, \dots, v_d]/(u_1^{q_1} - 1, \dots, u_d^{q_d} - 1, v_1^{2^l} - 1, \dots, v_d^{2^l} - 1) \\ & \cong \mathbb{K}[y, v_2, \dots, v_d]/(y^{q_1 \cdots q_d 2^l} - 1, v_2^{2^l} - 1, \dots, v_d^{2^l} - 1) \end{aligned}$$

How to choose our primes

$$p_i = q_i 2^l + 1, \quad q_i \ll 2^l, \quad q_i \text{ odd prime}, \quad i = 1, \dots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

$$\begin{aligned} & \mathbb{K}[x_1, \dots, x_d]/(x_1^{p_1-1} - 1, \dots, x_d^{p_d-1} - 1) \\ & \cong \mathbb{K}[u_1, \dots, u_d, v_1, \dots, v_d]/(u_1^{q_1} - 1, \dots, u_d^{q_d} - 1, v_1^{2^l} - 1, \dots, v_d^{2^l} - 1) \\ & \cong \mathbb{K}[y, v_2, \dots, v_d]/(y^{q_1 \cdots q_d 2^l} - 1, v_2^{2^l} - 1, \dots, v_d^{2^l} - 1) \end{aligned}$$

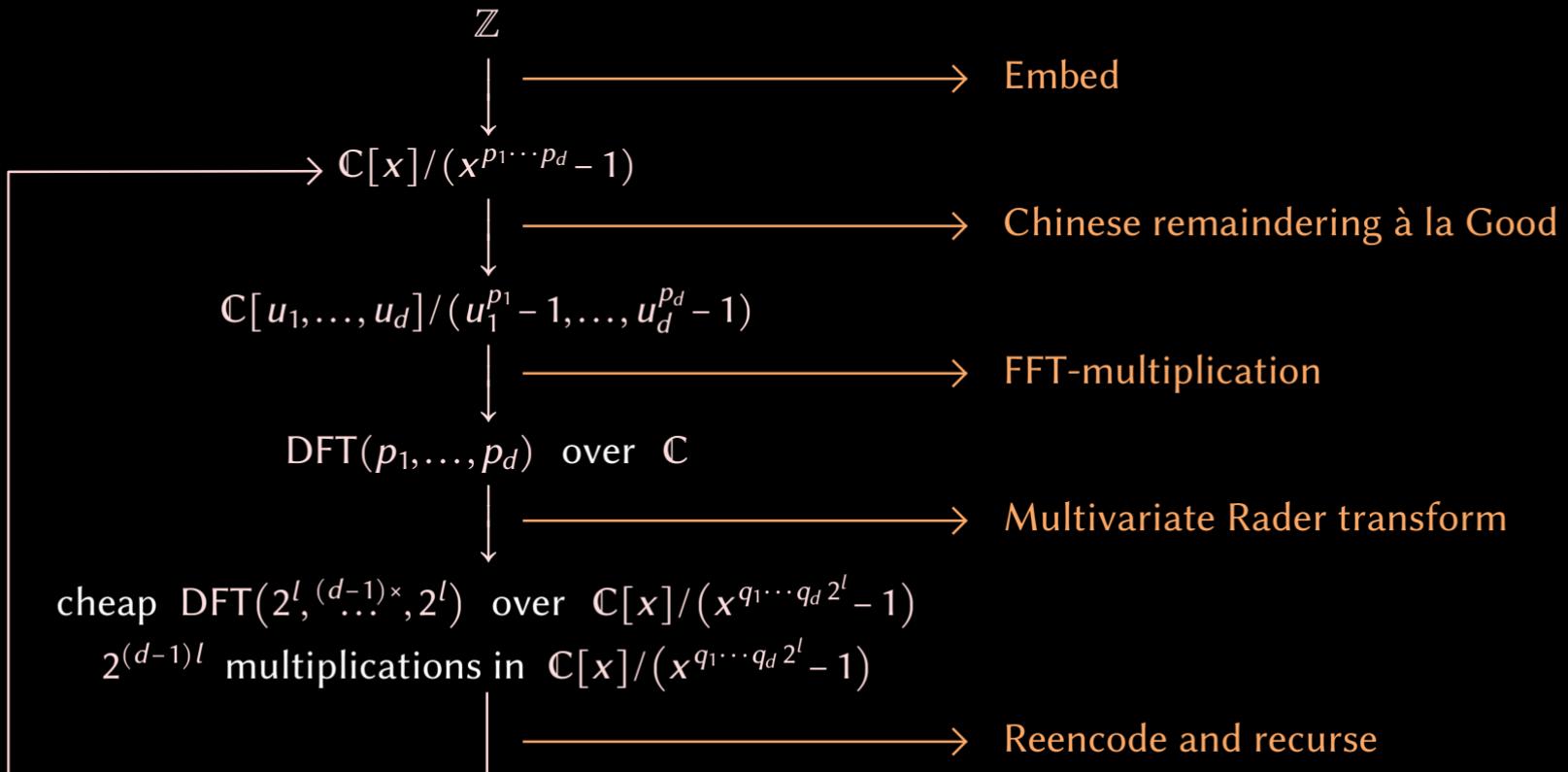
Conclusion

$$\mathbb{K}[x]/(x^{p_1 \cdots p_d} - 1) \longrightarrow \mathbb{K}[y, v_2, \dots, v_d]/(y^{q_1 \cdots q_d 2^l} - 1, v_2^{2^l} - 1, \dots, v_d^{2^l} - 1)$$

$$\begin{aligned} M_{\mathbb{K}}^{\circ}(p_1 \cdots p_d) &\leq 2^{(d-1)l} M_{\mathbb{K}}^{\circ}(\underbrace{q_1 \cdots q_d 2^l}_{2^{(1+\epsilon)l}}) + O(d 2^l \log 2^l \text{add}_{\mathbb{K}}) \\ &\geq 2^{(d+\epsilon)l} \end{aligned}$$

Summary

20/22



Linnik constants

$$P(a, k) := \min \{ck + a : c \in \mathbb{N}, ck + a \text{ is prime}\}$$

$$P(k) := \max \{P(a, k) : 0 < a < k, a \wedge k = 1\}$$

L is a Linnik constant $\Leftrightarrow P(k) = O(k^L)$

Linnik constants

$$P(a, k) := \min \{ck + a : c \in \mathbb{N}, ck + a \text{ is prime}\}$$

$$P(k) := \max \{P(a, k) : 0 < a < k, a \wedge k = 1\}$$

L is a Linnik constant $\Leftrightarrow P(k) = O(k^L)$

Theorem

If there exists a Linnik constant $L < 1 + \frac{1}{303}$, then

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

Linnik constants

$$P(a, k) := \min \{ck + a : c \in \mathbb{N}, ck + a \text{ is prime}\}$$

$$P(k) := \max \{P(a, k) : 0 < a < k, a \wedge k = 1\}$$

L is a Linnik constant $\Leftrightarrow P(k) = O(k^L)$

Theorem

If there exists a Linnik constant $L < 1 + \frac{1}{303}$, then

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

Theorem

If there exists a Linnik constant $L < 1 + 2^{-1162}$, then

$$M_{\mathbb{F}_q}(n) = O(n \log q \log(n \log q)),$$

uniformly in q .

Thank you !



<http://www.texmacs.org>