Integer multiplication: classical tools

Joris van der Hoeven

CNRS, visiting professor at PIMS and SFU

Joint work with David Harvey (UNSW, Sydney)

SFU, Burnaby **January 21, 2020**

Motivation

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

Motivation

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

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

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. $O(\mathsf{M}(n))$

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. $O(\mathsf{M}(n) \log n)$

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 π. $O(\mathsf{M}(n) \log n)$

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 π. $O(\mathsf{M}(n) \log n)$

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

Motivation

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

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

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

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

Computing 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 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 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 $p \geqslant \log n$

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

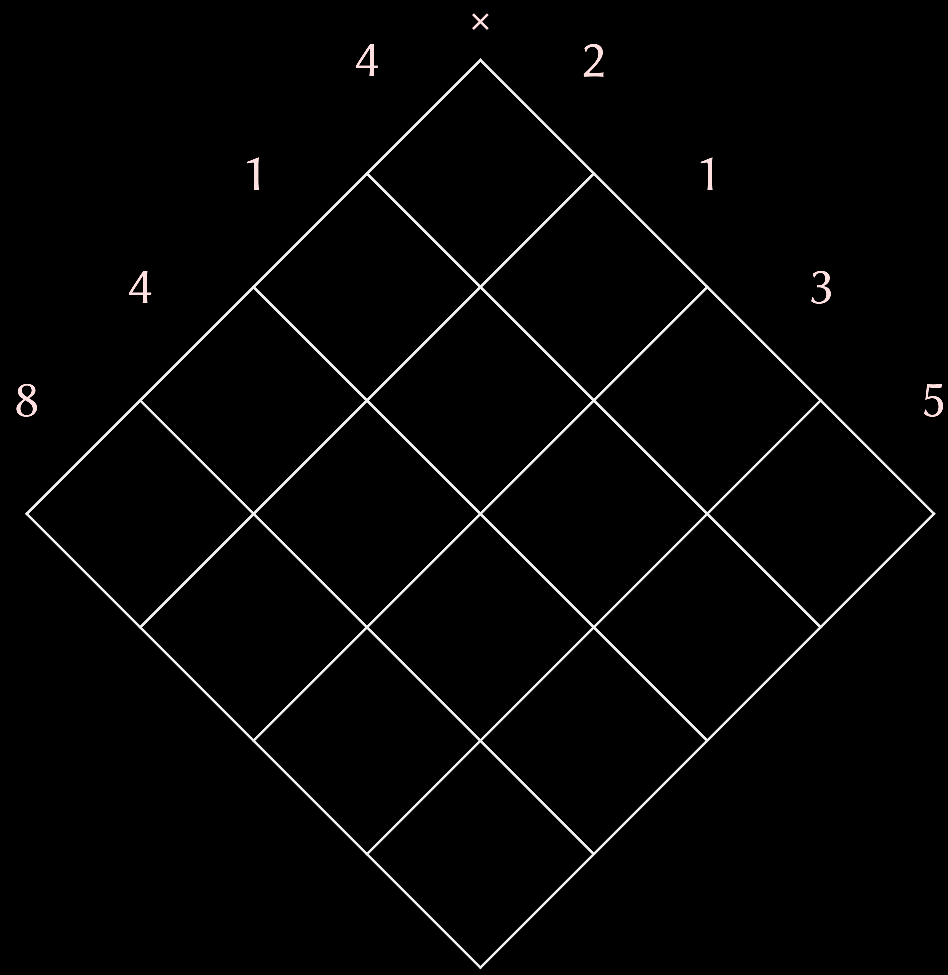
Also

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

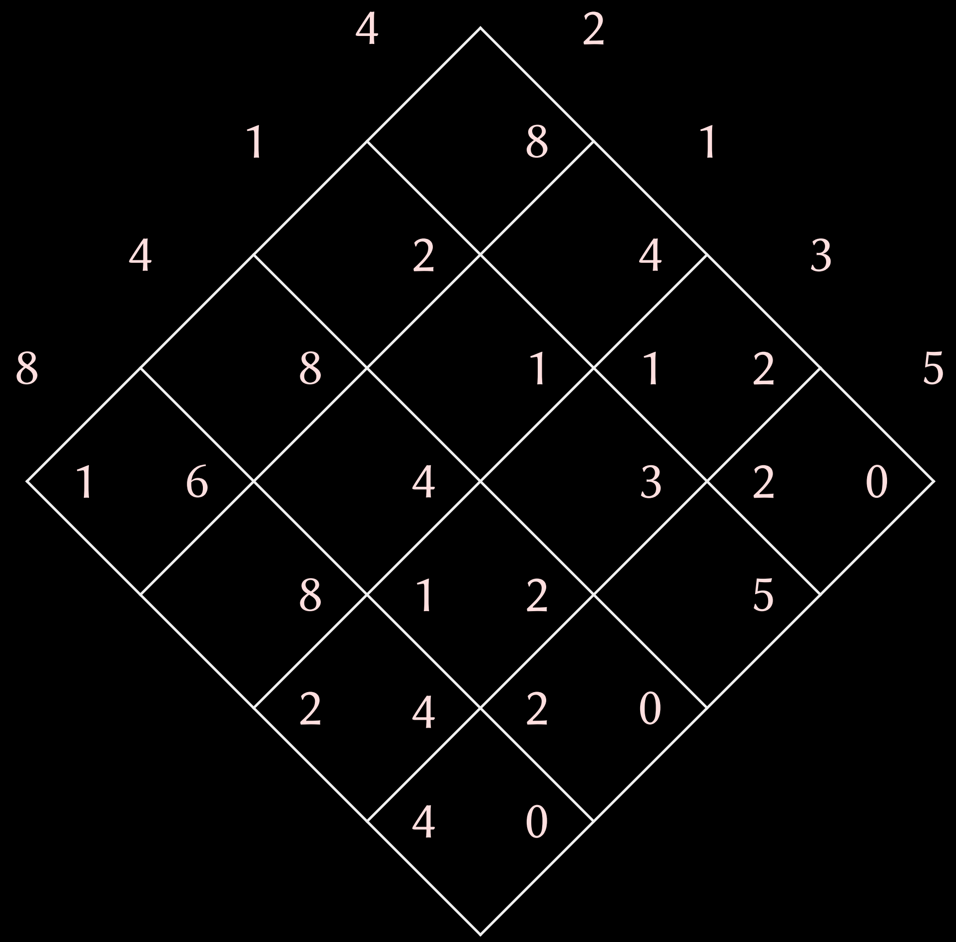
Naive multiplication

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

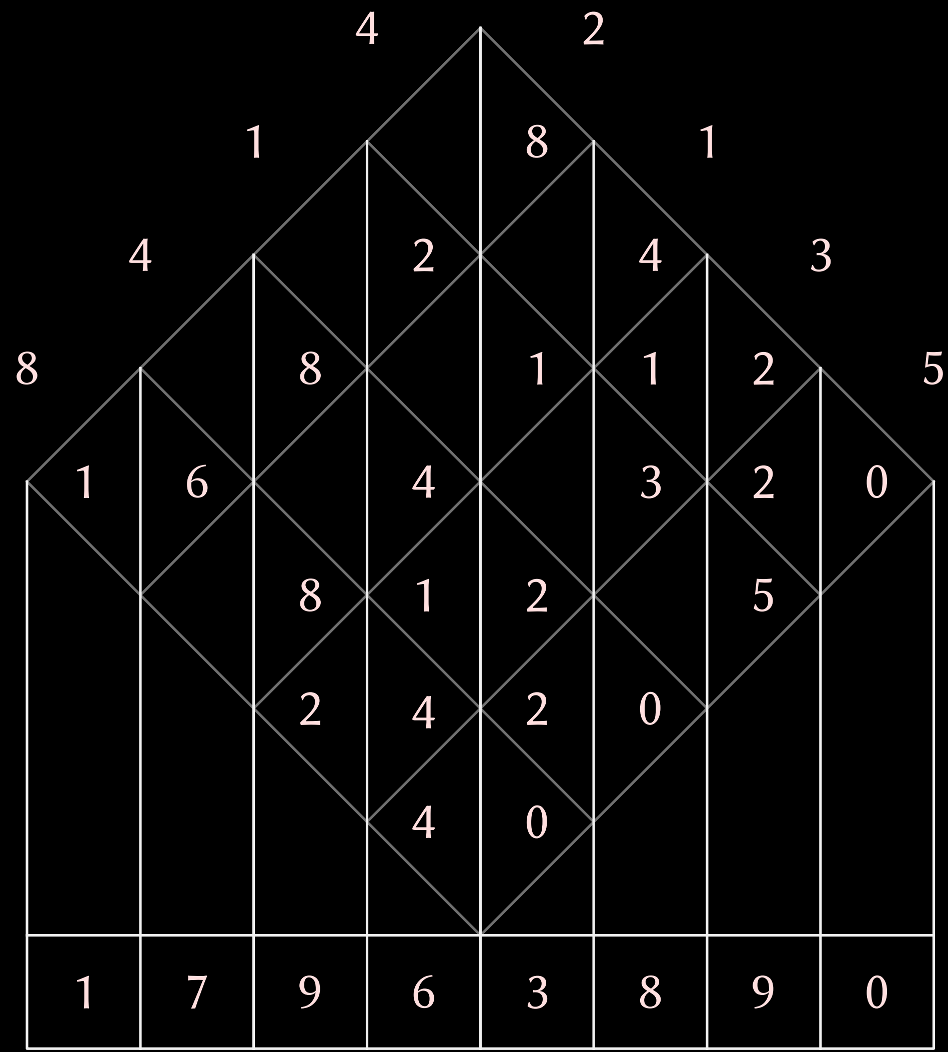
Naive multiplication



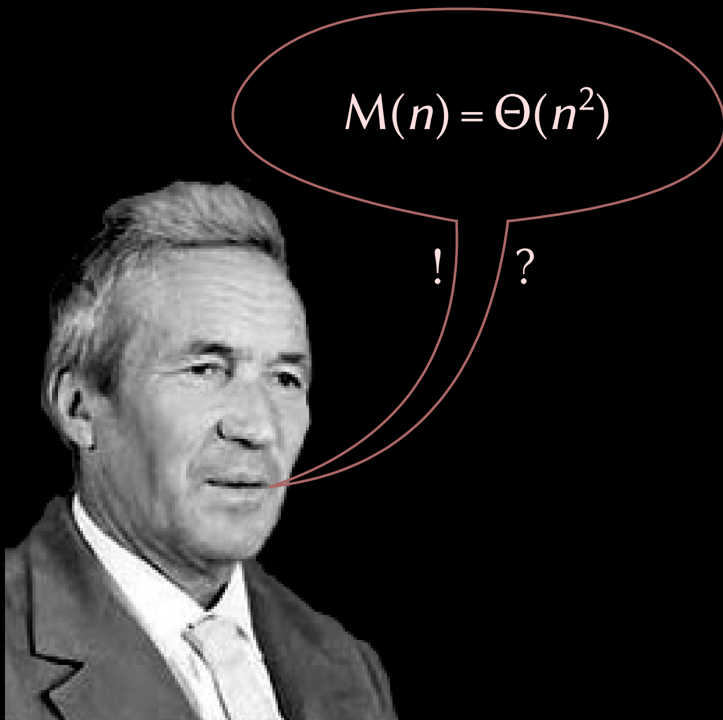
Naive multiplication



Naive multiplication



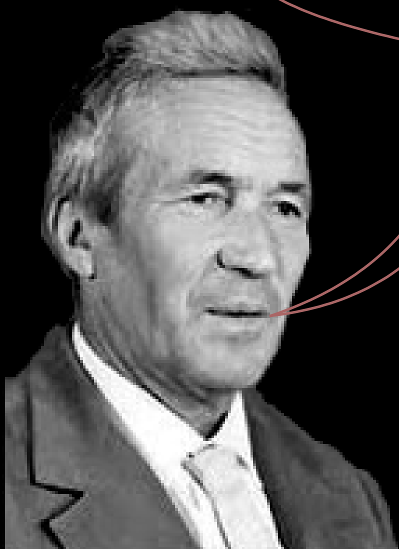
Can we do better?



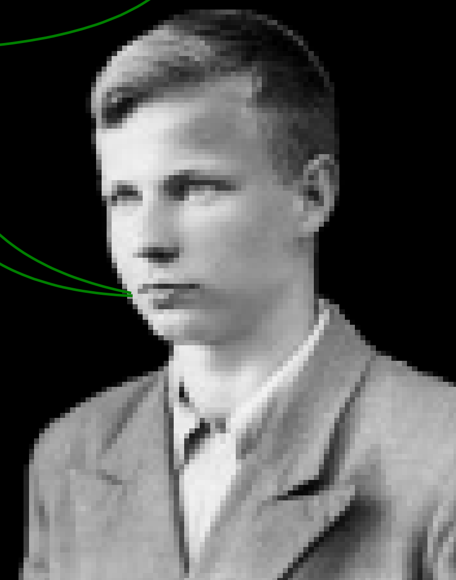
Can we do better?

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

! ?



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



1962

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

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

Kronecker substitution

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$
$$\wr$$
$$4627000057960000797800008114 \quad \times \quad 4519000017080000719600006234$$

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

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

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

Multiplying by evaluation-interpolation

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

$P, Q \in \mathbb{K}[x]$: polynomials of degree $< k$

$R = PQ$ of degree $< 2k - 1$

Multiplying by evaluation-interpolation

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

$P, Q \in \mathbb{K}[x]$: polynomials of degree $< k$

$R = PQ$ of degree $< 2k - 1$

R uniquely determined by its values at pairwise distinct points $\alpha_1, \ldots, \alpha_{2k-1} \in \mathbb{K}$

Multiplying by evaluation-interpolation

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

$P, Q \in \mathbb{K}[x]$: polynomials of degree $< k$

$R = PQ$ of degree $< 2k-1$

R uniquely determined by its values at pairwise distinct points $\alpha_1, \ldots, \alpha_{2k-1} \in \mathbb{K}$

$$P \longrightarrow (P(\alpha_1), \ldots, P(\alpha_{2k-1}))$$

$$Q \longrightarrow (Q(\alpha_1), \ldots, Q(\alpha_{2k-1}))$$

$$\searrow \qquad \swarrow$$

$$(P(\alpha_1)\,Q(\alpha_1), \ldots, P(\alpha_{2k-1})\,Q(\alpha_{2k-1})) = (R(\alpha_1), \ldots, R(\alpha_{2k-1})) \longrightarrow R$$

Karatsuba multiplication

$k = 2$

$\alpha_0 = \infty, \ \alpha_2 = 0, \ \alpha_3 = 1$

Karatsuba multiplication

$k = 2$

$\alpha_0 = \infty,\ \alpha_2 = 0,\ \alpha_3 = 1 \quad \longrightarrow \quad \alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0)$, $\alpha_1 = (0, 1)$, $\alpha_2 = (1, 1)$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

8414 2135

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

$$8414 \rightsquigarrow 84\,x + 14\,y \qquad 2135 \rightsquigarrow 21\,x + 35\,y$$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

$$
\begin{array}{ccc}
8414 & \qquad\qquad & 2135 \\
\rightsquigarrow & & \rightsquigarrow \\
84\,x + 14\,y & & 21\,x + 35\,y \\
\downarrow & & \downarrow \\
(84, 14, 98) & & (21, 35, 56)
\end{array}
$$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

$$\begin{array}{ccccc} 8414 & & & & 2135 \\ \wr\!\downarrow & & & & \wr\!\downarrow \\ 84\,x + 14\,y & & & & 21\,x + 35\,y \\ \downarrow & & & & \downarrow \\ (84, 14, 98) & & & & (21, 35, 56) \\ & \searrow & & \swarrow & \\ & & (1764, 490, 5376) & & \end{array}$$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

$$
\begin{array}{ccc}
8414 & & 2135 \\
\wr\downarrow & & \wr\downarrow \\
84\,x + 14\,y & & 21\,x + 35\,y \\
\downarrow & & \downarrow \\
(84, 14, 98) & & (21, 35, 56) \\
& \searrow \quad \swarrow & \\
& (1764, 490, 5376) & \\
& \downarrow & \\
& (1764\,x^2 + 3234\,x\,y + 490\,y^2) &
\end{array}
$$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

$$8414 \rightsquigarrow 84\,x + 14\,y \longrightarrow (84, 14, 98)$$

$$2135 \rightsquigarrow 21\,x + 35\,y \longrightarrow (21, 35, 56)$$

$$(1764, 490, 5376) \longrightarrow (1764\,x^2 + 3234\,x\,y + 490\,y^2)$$

3234 → $5376 - 1764 - 490$

Karatsuba multiplication

$k = 2$

$\alpha_0 = (1, 0),\ \alpha_1 = (0, 1),\ \alpha_2 = (1, 1)$

$$
\begin{array}{ccccc}
8414 & & & & 2135 \\
\wr\downarrow & & & & \wr\downarrow \\
84\,x + 14\,y & & & & 21\,x + 35\,y \\
\downarrow & & & & \downarrow \\
(84, 14, 98) & & & & (21, 35, 56) \\
& \searrow & & \swarrow & \\
& & (1764, 490, 5376) & & \\
& & \downarrow & & \\
& & (1764\,x^2 + 3234\,x\,y + 490\,y^2) & & \\
& & \wr\downarrow & & \\
& & 17963890 & &
\end{array}
$$

Karatsuba multiplication: $k = 2$ 1962

$$M(2\,n) = 3\,M(n) + O(n)$$

$$M(n) = O(n^{\log_2 3}) \approx O(n^{1.5849625})$$

Complexity analysis

Karatsuba multiplication: $k = 2$ 1962

$$M(2n) = 3M(n) + O(n)$$

$$M(n) = O(n^{\log_2 3}) \approx O(n^{1.5849625})$$

Toom-Cook multiplication: $k > 2$ 1963

$$M(kn) = (2k+1)M(n) + O(n)$$

$$M(n) = O(n^{\log_k (2k+1)}) = O(n^{1+O(1/\log k)})$$

Complexity analysis

Karatsuba multiplication: $k = 2$ 1962

$$M(2n) = 3M(n) + O(n)$$

$$M(n) = O(n^{\log_2 3}) \approx O(n^{1.5849625})$$

Toom-Cook multiplication: $k > 2$ 1963

$$M(kn) = (2k+1)M(n) + O(n)$$

$$M(n) = O(n^{\log_k (2k+1)}) = O(n^{1+O(1/\log k)})$$

Let k grow with n

Complexity analysis

Karatsuba multiplication: $k = 2$ 1962

$$M(2n) = 3M(n) + O(n)$$

$$M(n) = O(n^{\log_2 3}) \approx O(n^{1.5849625})$$

Toom-Cook multiplication: $k > 2$ 1963

$$M(kn) = (2k+1)M(n) + O(n)$$

$$M(n) = O(n^{\log_k(2k+1)}) = O(n^{1+O(1/\log k)})$$

Let k grow with n

$$M(n) = O\left(n\, 2^{5\sqrt{\log n/\log 2}}\right)$$ 1963, Toom

Complexity analysis

Karatsuba multiplication: $k = 2$ 1962

$$M(2n) = 3M(n) + O(n)$$

$$M(n) = O(n^{\log_2 3}) \approx O(n^{1.5849625})$$

Toom-Cook multiplication: $k > 2$ 1963

$$M(kn) = (2k+1)M(n) + O(n)$$

$$M(n) = O(n^{\log_k (2k+1)}) = O(n^{1+O(1/\log k)})$$

Let k grow with n

$$M(n) = O\left(n\, 2^{5\sqrt{\log n/\log 2}}\right)$$ 1963, Toom

$$M(n) = O\left(n\, 2^{\sqrt{2\log n/\log 2}} (\log n)^{3/2}\right)$$ 1966, Schönhage

Complexity analysis

Karatsuba multiplication: $k=2$ 1962

$$M(2n) = 3M(n) + O(n)$$

$$M(n) = O(n^{\log_2 3}) \approx O(n^{1.5849625})$$

Toom-Cook multiplication: $k>2$ 1963

$$M(kn) = (2k+1)M(n) + O(n)$$

$$M(n) = O(n^{\log_k(2k+1)}) = O(n^{1+O(1/\log k)})$$

Let k grow with n

$$M(n) = O\left(n 2^{5\sqrt{\log n/\log 2}}\right)$$ 1963, Toom

$$M(n) = O\left(n 2^{\sqrt{2\log n/\log 2}} (\log n)^{3/2}\right)$$ 1966, Schönhage

$$M(n) = O\left(n 2^{\sqrt{2\log n/\log 2}} \log n\right)$$ 1969, Knuth

Can we do better?

Problem

When k gets large, evaluation-interpolation gets expensive

Next goal

Faster evaluation-interpolation for well-chosen points

The Fast Fourier Transform

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

n : transform length

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

The Fast Fourier Transform

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

n : transform length

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

Discrete Fourier transform

$$(\hat{c}_0, \ldots, \hat{c}_{n-1}) = \mathrm{DFT}_{\omega;n}(c_0, \ldots, c_{n-1})$$

$$C = c_0 + \cdots + c_{n-1} x^{n-1}$$

$$\hat{c}_k = C(\omega^k)$$

The Fast Fourier Transform

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

n : transform length

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

Discrete Fourier transform

$$(\hat{c}_0, \ldots, \hat{c}_{n-1}) \;=\; \mathrm{DFT}_{\omega;n}(c_0, \ldots, c_{n-1})$$

$$C \;=\; c_0 + \cdots + c_{n-1} x^{n-1} \;\in\; \mathbb{K}[x]/(x^n - 1)$$

$$\hat{c}_k \;=\; C(\omega^k)$$

The Fast Fourier Transform

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

n : transform length

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

Discrete Fourier transform

$$(\hat{c}_0, \ldots, \hat{c}_{n-1}) = \mathrm{DFT}_{\omega;n}(c_0, \ldots, c_{n-1})$$

$$C = c_0 + \cdots + c_{n-1} x^{n-1} \in \mathbb{K}[x]/(x^n - 1)$$

$$\hat{c}_k = C(\omega^k)$$

Chinese remainder perspective

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

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

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

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

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

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

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

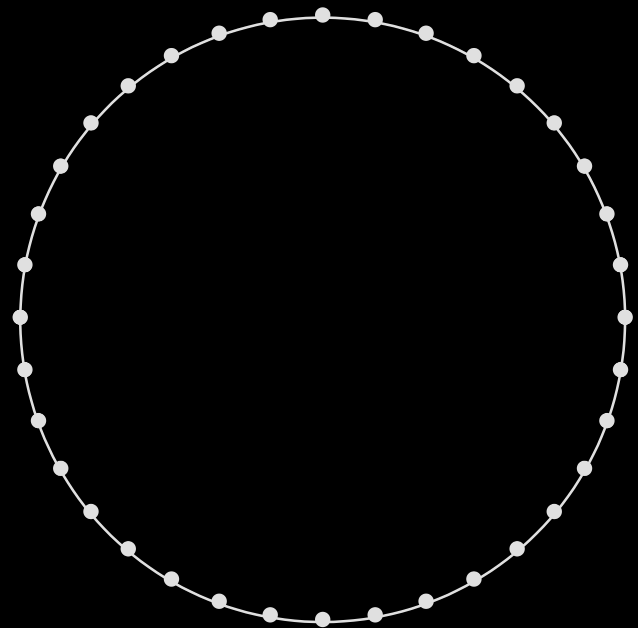
$$\big\downarrow \text{DFT}^{-1}$$

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

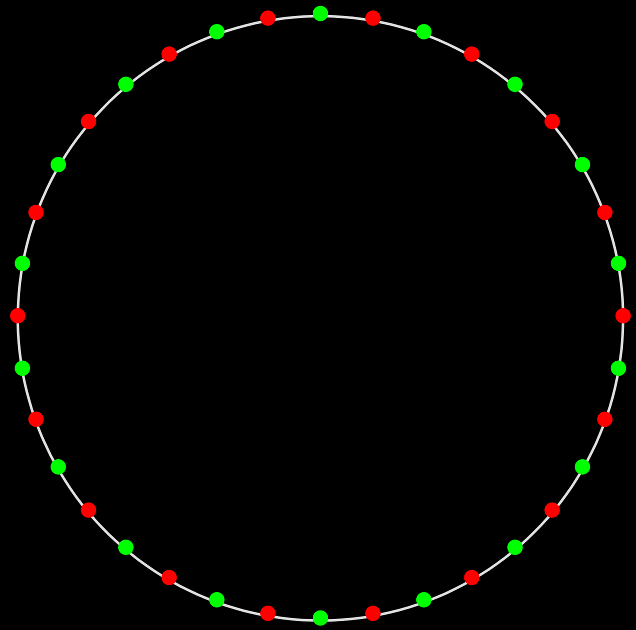
Inverse transforms

$$\begin{aligned}
(\hat{c}_0, \ldots, \hat{c}_{n-1}) &= \text{DFT}_{\omega;n}(c_0, \ldots, c_{n-1}) \\
(c_0, \ldots, c_{n-1}) &= \frac{1}{n}\text{DFT}_{\omega^{-1};n}(\hat{c}_0, \ldots, \hat{c}_{n-1})
\end{aligned}$$

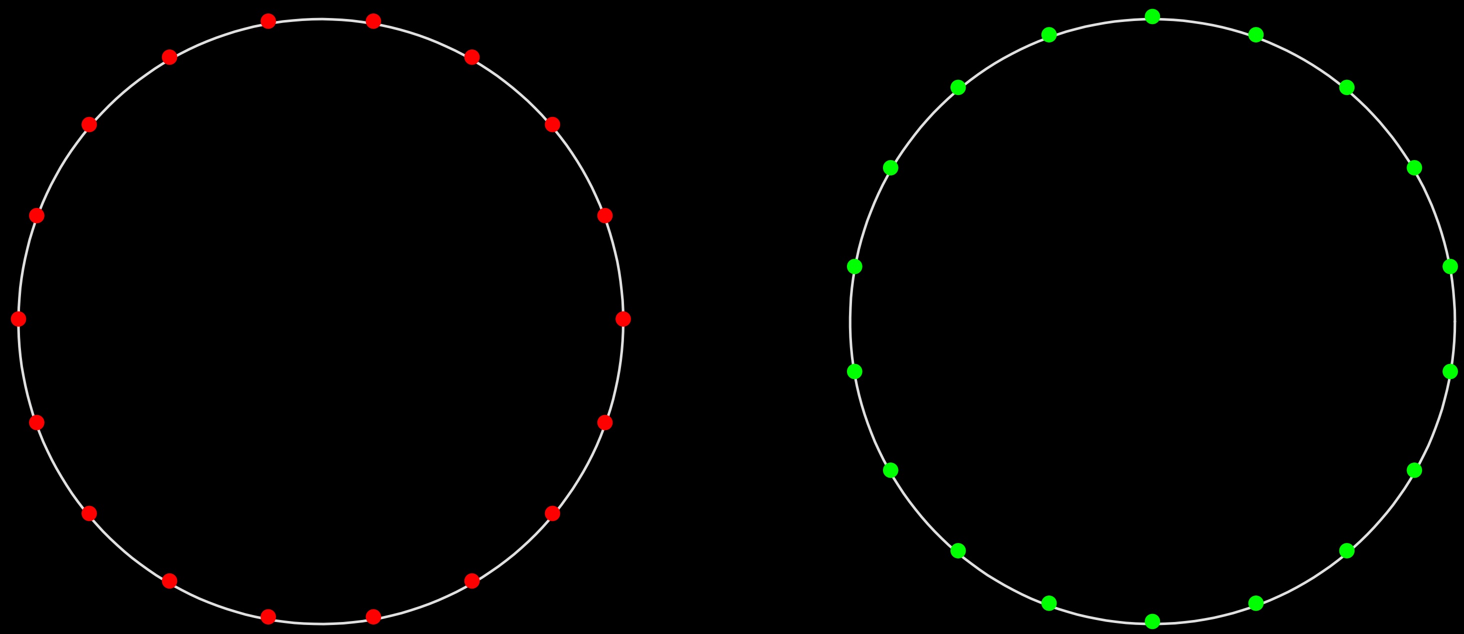
Making the FFT fast



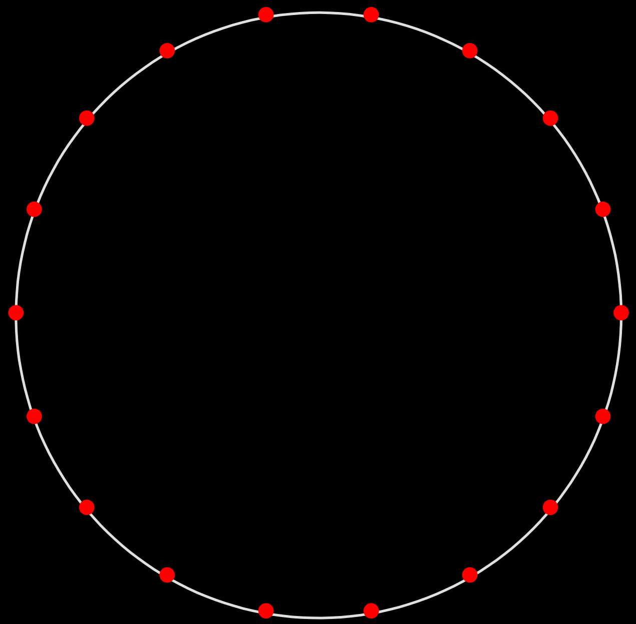
Making the FFT fast

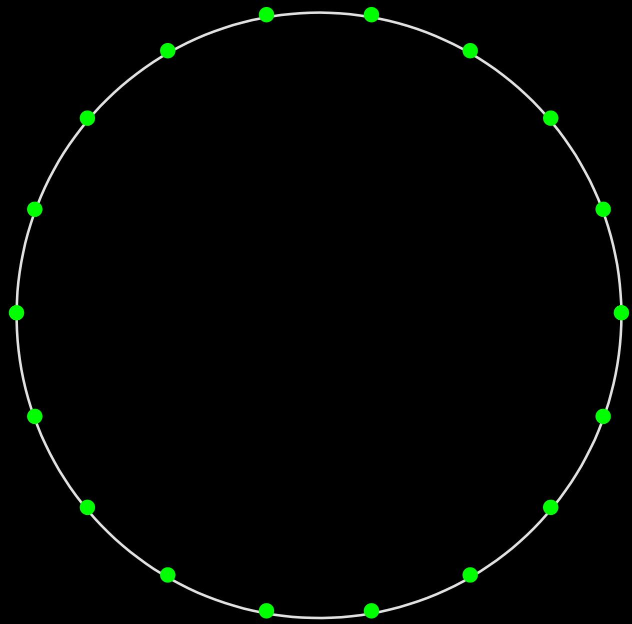


Making the FFT fast

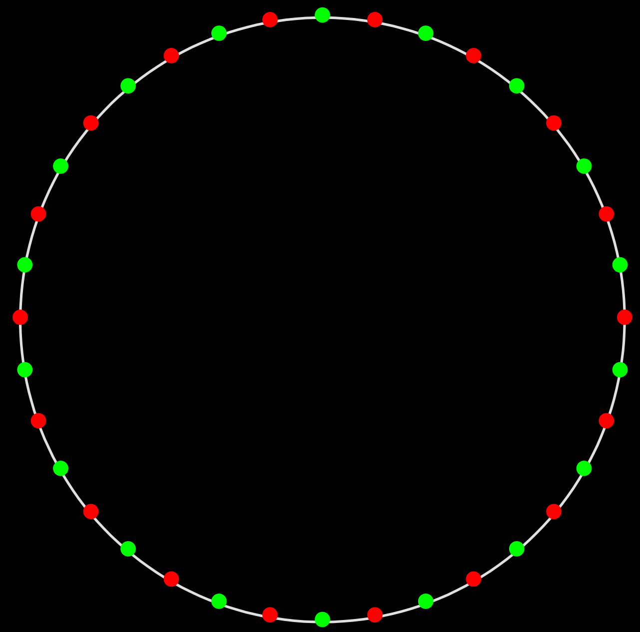


Making the FFT fast



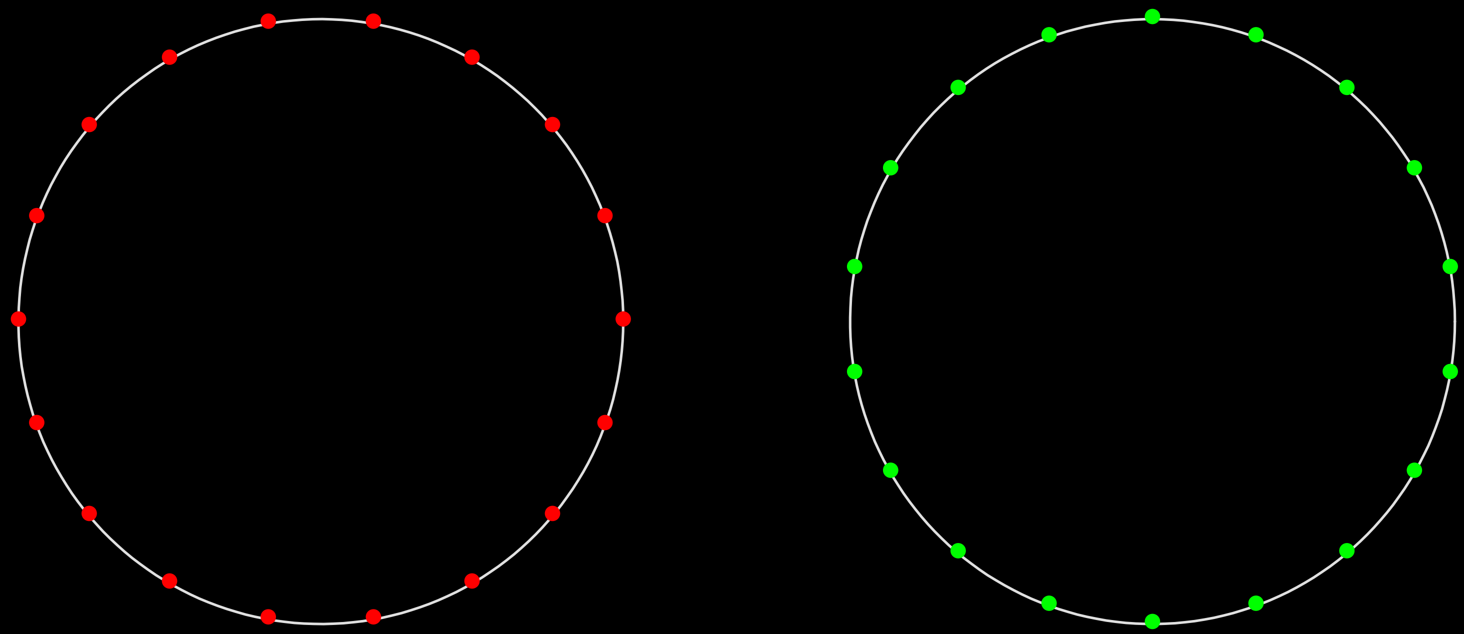


Making the FFT fast



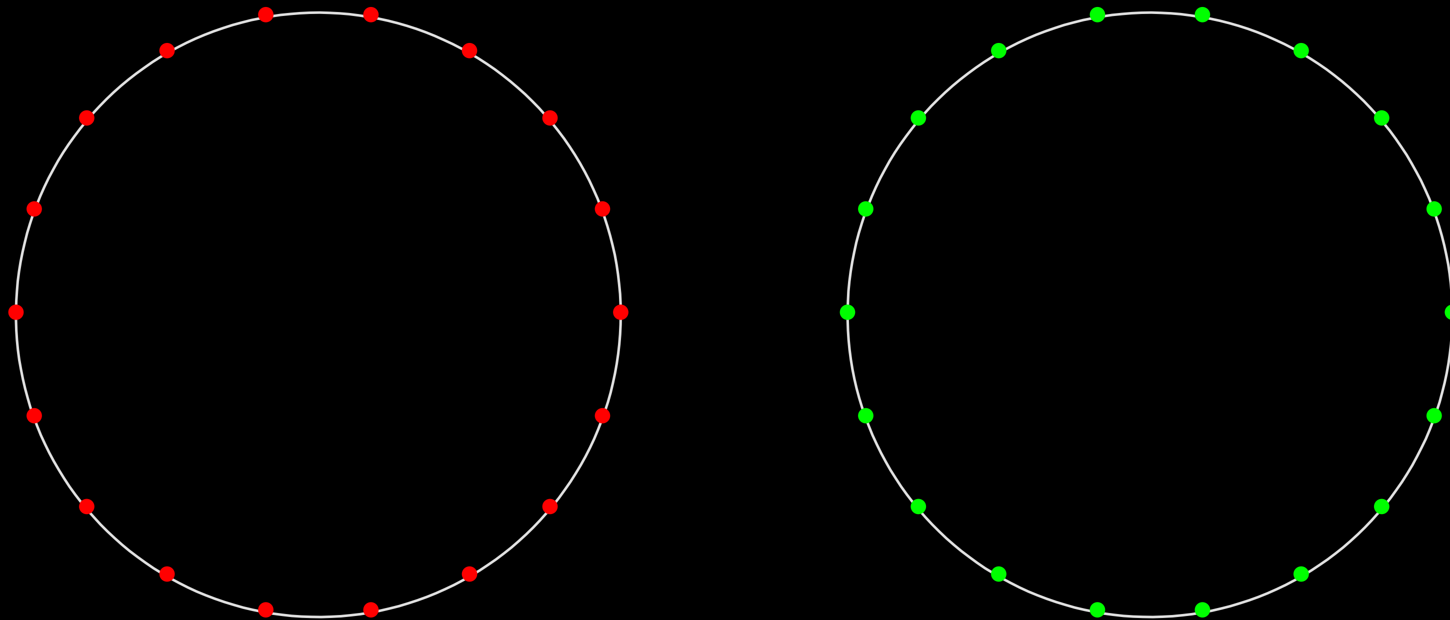
$\mathbb{K}[x]/(x^{2n} - 1)$

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

Assume that $n = 2^l$ is a power of two

Complexity analysis

Assume that $n = 2^l$ is a power of two

$$\mathsf{F}_{\mathbb{K}}(2n) \quad = \quad 2\,\mathsf{F}_{\mathbb{K}}(n) + O(n)$$

Complexity analysis

Assume that $n = 2^l$ is a power of two

$$\mathrm{F}_{\mathbb{K}}(2\,n) = 2\,\mathrm{F}_{\mathbb{K}}(n) + O(n)$$

$$\begin{aligned}
\mathrm{F}_{\mathbb{K}}(2^l) &\leqslant 2\,\mathrm{F}_{\mathbb{K}}(2^{l-1}) + C\,2^l \\
&\leqslant 2^2\,\mathrm{F}_{\mathbb{K}}(2^{l-2}) + 2\,C\,2^l \\
&\leqslant 2^3\,\mathrm{F}_{\mathbb{K}}(2^{l-3}) + 3\,C\,2^l \\
&\vdots \\
&\leqslant 2^l\,\mathrm{F}_{\mathbb{K}}(1) + l\,C\,2^l
\end{aligned}$$

Complexity analysis

Assume that $n = 2^l$ is a power of two

$$\mathsf{F}_{\mathbb{K}}(2n) = 2\,\mathsf{F}_{\mathbb{K}}(n) + O(n)$$

$$\begin{aligned}
\mathsf{F}_{\mathbb{K}}(2^l) &\leqslant 2\,\mathsf{F}_{\mathbb{K}}(2^{l-1}) + C\,2^l \\
&\leqslant 2^2\,\mathsf{F}_{\mathbb{K}}(2^{l-2}) + 2\,C\,2^l \\
&\leqslant 2^3\,\mathsf{F}_{\mathbb{K}}(2^{l-3}) + 3\,C\,2^l \\
&\vdots \\
&\leqslant 2^l\,\mathsf{F}_{\mathbb{K}}(1) + l\,C\,2^l
\end{aligned}$$

$$\mathsf{F}_{\mathbb{K}}(n) = O(n \log n)$$

Complexity analysis

Assume that $n = 2^l$ is a power of two

$$\mathsf{F}_{\mathbb{K}}(2n) = 2\,\mathsf{F}_{\mathbb{K}}(n) + O(n)$$

$$\begin{aligned}
\mathsf{F}_{\mathbb{K}}(2^l) &\leqslant 2\,\mathsf{F}_{\mathbb{K}}(2^{l-1}) + C\,2^l \\
&\leqslant 2^2\,\mathsf{F}_{\mathbb{K}}(2^{l-2}) + 2\,C\,2^l \\
&\leqslant 2^3\,\mathsf{F}_{\mathbb{K}}(2^{l-3}) + 3\,C\,2^l \\
&\vdots \\
&\leqslant 2^l\,\mathsf{F}_{\mathbb{K}}(1) + l\,C\,2^l
\end{aligned}$$

$$\mathsf{F}_{\mathbb{K}}(n) = O(n \log n)$$

But what is $\mathbb{K}$ for our application to integer multiplication?

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{2872216826762157625376253762153762156735216735126727321653 42}^{N}$$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{28722\ 16826\ 76215\ 76253\ 76253\ 76215\ 37621\ 56735\ 21673\ 51267\ 27321\ 65342}^{N}$$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{\underbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}_{n}}^{N}$$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}$$
$$\underbrace{\hphantom{28722\ 16826\ 76215\ 76253\ 76253\ 76215\ 37621\ 56735\ 21673\ 51267\ 27321\ 65342}}_{n}$$

Bit-size of the coefficients of the product: $2\,b + \lceil \log_2 n \rceil$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{\underbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}_{n}}^{N}$$

Bit-size of the coefficients of the product: $2\,b + [\log_2 n]$

Loss of bit-precision due to rounding errors: $O(\log n)$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\underbrace{\overbrace{\underbrace{28722}_{b}\;\underbrace{16826}_{b}\;\underbrace{76215}_{b}\;\underbrace{76253}_{b}\;\underbrace{76253}_{b}\;\underbrace{76215}_{b}\;\underbrace{37621}_{b}\;\underbrace{56735}_{b}\;\underbrace{21673}_{b}\;\underbrace{51267}_{b}\;\underbrace{27321}_{b}\;\underbrace{65342}_{b}}^{N}}_{n}$$

Bit-size of the coefficients of the product: $2b + \lceil \log_2 n \rceil$

Loss of bit-precision due to rounding errors: $O(\log n)$

Best choice: $\quad b \asymp \log N, \quad n = N/b \asymp N/\log N$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}$$
$$\underbrace{\hphantom{28722\ 16826\ 76215\ 76253\ 76253\ 76215\ 37621\ 56735\ 21673\ 51267\ 27321\ 65342}}_{n}$$

Bit-size of the coefficients of the product: $2b + \lceil \log_2 n \rceil$

Loss of bit-precision due to rounding errors: $O(\log n)$

Best choice: $\quad b \asymp \log N, \quad n = N/b \asymp N/\log N$

Working precision: $\quad B = 2b + O(\log n) = O(\log N)$

Complex number FFTs

$\mathbb{K} = \mathbb{C}$, while working with a finite bit-precision

$$\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}$$
$$\underbrace{\hphantom{28722\ 16826\ 76215\ 76253\ 76253\ 76215\ 37621\ 56735\ 21673\ 51267\ 27321\ 65342}}_{n}$$

Bit-size of the coefficients of the product: $2\,b + \lceil \log_2 n \rceil$

Loss of bit-precision due to rounding errors: $O(\log n)$

Best choice: $\quad b \asymp \log N, \quad n = N/b \asymp N/\log N$

Working precision: $\quad B = 2\,b + O(\log n) = O(\log N)$

$$\begin{aligned} \mathsf{M}(N) &= O(\mathsf{M}(\log N)\, n \log n) \\ &= O(N\, \mathsf{M}(\log N)) \\ &= O(N \log N\, \mathsf{M}(\log \log N)) \\ &\ \vdots \\ &= O\big(N \log N \cdots \log \circ \overset{k\times}{\cdots} \circ \log N\big) \end{aligned}$$

$$k = \log^* N = \min\left\{ l : \log \circ \overset{l\times}{\cdots} \circ \log N \leqslant 1 \right\}$$

Number field FFTs

$\mathbb{K} = \mathbb{F}_p, \quad p = s\,2^l + 1, \quad \text{small } s \qquad p = 3 \cdot 2^{30} + 1$ (Pollard, 1971)

Number field FFTs

$\mathbb{K} = \mathbb{F}_p$, $\quad p = s\,2^l + 1$, $\quad$ small s $\qquad p = 3 \cdot 2^{30} + 1$ (Pollard, 1971)

$$\underbrace{\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}}_{n}$$

Number field FFTs

$\mathbb{K} = \mathbb{F}_p, \quad p = s\,2^l + 1, \quad \text{small } s \qquad p = 3 \cdot 2^{30} + 1$ (Pollard, 1971)

$$\overbrace{\underbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}_{n}}^{N}$$

Bit-size of the coefficients of the product: $2\,b + \lceil \log_2 n \rceil < \log_2 p$

Number field FFTs

$\mathbb{K} = \mathbb{F}_p, \quad p = s\,2^l + 1, \quad \text{small } s \qquad p = 3 \cdot 2^{30} + 1$ (Pollard, 1971)

$$\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{n}$$

Bit-size of the coefficients of the product: $2\,b + [\log_2 n] < \log_2 p$

No precision loss!

Number field FFTs

$\mathbb{K} = \mathbb{F}_p, \quad p = s\,2^l + 1, \quad \text{small } s \qquad p = 3 \cdot 2^{30} + 1$ (Pollard, 1971)

$$\underbrace{\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}}_{n}$$

Bit-size of the coefficients of the product: $2\,b + [\log_2 n] < \log_2 p$

No precision loss!

Best choice: $\quad b \asymp \log N, \quad n = N / b \asymp N / \log N$

Number field FFTs

$\mathbb{K} = \mathbb{F}_p$, $p = s\,2^l + 1$, small s $\quad p = 3 \cdot 2^{30} + 1$ (Pollard, 1971)

$$\overbrace{\underbrace{28722}_{b}\ \underbrace{16826}_{b}\ \underbrace{76215}_{b}\ \underbrace{76253}_{b}\ \underbrace{76253}_{b}\ \underbrace{76215}_{b}\ \underbrace{37621}_{b}\ \underbrace{56735}_{b}\ \underbrace{21673}_{b}\ \underbrace{51267}_{b}\ \underbrace{27321}_{b}\ \underbrace{65342}_{b}}^{N}$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{n}$$

Bit-size of the coefficients of the product: $2\,b + \lceil \log_2 n \rceil < \log_2 p$

No precision loss!

Best choice: $\quad b \asymp \log N$, $\quad n = N / b \asymp N / \log N$

$$\begin{aligned} \mathsf{M}(N) &= O(\mathsf{M}(\log N)\, n \log n) \\ &= \cdots \\ &= O\big(N \log N \log\log N \cdots \log \circ \overset{k\times}{\cdots} \circ \log N\big), \qquad k = \log^* N \end{aligned}$$

Synthetic FFTs

$\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}, \quad \omega = 2, \quad \omega^{2m} = 1$ (Schönhage-Strassen, 1971)

Synthetic FFTs

$\mathbb{K} = \mathbb{Z}/(2^m+1)\,\mathbb{Z}, \quad \omega = 2, \quad \omega^{2m} = 1$ (Schönhage-Strassen, 1971)

$$\overbrace{\underbrace{\underbrace{2872216826}_{m}\ \underbrace{7621576253}_{m}\ \underbrace{7625376215}_{m}\ \underbrace{3762156735}_{m}\ \underbrace{2167351267}_{m}\ \underbrace{2732165342}_{m}}_{n}}^{N}$$

Synthetic FFTs

$\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}, \quad \omega = 2, \quad \omega^{2m} = 1$ (Schönhage-Strassen, 1971)

$$\underbrace{\overbrace{\underbrace{2872216826}_{m}\ \underbrace{7621576253}_{m}\ \underbrace{7625376215}_{m}\ \underbrace{3762156735}_{m}\ \underbrace{2167351267}_{m}\ \underbrace{2732165342}_{m}}^{N}}_{n}$$

We must have $n \leqslant 2\,m$, since ω is only a $2\,m$-th root of unity

Synthetic FFTs

$\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}, \quad \omega = 2, \quad \omega^{2m} = 1$ (Schönhage-Strassen, 1971)

$$\overbrace{\underbrace{2872216826}_{m}\ \underbrace{7621576253}_{m}\ \underbrace{7625376215}_{m}\ \underbrace{3762156735}_{m}\ \underbrace{2167351267}_{m}\ \underbrace{2732165342}_{m}}^{N}$$

$$\underbrace{\hphantom{2872216826\ 7621576253\ 7625376215\ 3762156735\ 2167351267\ 2732165342}}_{n}$$

We must have $n \leqslant 2m$, since ω is only a $2m$-th root of unity

Best choice: $\quad m \asymp n \asymp \sqrt{N}$

Synthetic FFTs

$\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}, \quad \omega = 2, \quad \omega^{2m} = 1$ (Schönhage-Strassen, 1971)

$$\overbrace{\underbrace{2872216826}_{m}\ \underbrace{7621576253}_{m}\ \underbrace{7625376215}_{m}\ \underbrace{3762156735}_{m}\ \underbrace{2167351267}_{m}\ \underbrace{2732165342}_{m}}^{N}$$
$$\underbrace{\hphantom{2872216826\ 7621576253\ 7625376215\ 3762156735\ 2167351267\ 2732165342}}_{n}$$

We must have $n \leqslant 2m$, since ω is only a $2m$-th root of unity

Best choice: $\quad m \asymp n \asymp \sqrt{N}$

DFTs only require additions and subtractions, no multiplications!

Synthetic FFTs

$\mathbb{K} = \mathbb{Z}/(2^m + 1)\mathbb{Z}, \quad \omega = 2, \quad \omega^{2m} = 1$ (Schönhage-Strassen, 1971)

$$\underbrace{\overbrace{\underbrace{2872216826}_{m}\ \underbrace{7621576253}_{m}\ \underbrace{7625376215}_{m}\ \underbrace{3762156735}_{m}\ \underbrace{2167351267}_{m}\ \underbrace{2732165342}_{m}}^{N}}_{n}$$

We must have $n \leqslant 2m$, since ω is only a $2m$-th root of unity

Best choice: $m \asymp n \asymp \sqrt{N}$

DFTs only require additions and subtractions, no multiplications!

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

$$\begin{aligned} \mathsf{M}^{\ominus}(N) &\leqslant 2n\,\mathsf{M}^{\ominus}(m) + O(N \log N) \\ &= \cdots && \text{(log log } N \text{ recursive steps)} \\ &= O(N \log N \log \log N) \end{aligned}$$

Can we do better?

Main problems

- Over $\mathbb{C}$, the multiplications with powers of ω end up being too expensive
- Schönhage-Strassen does not fully exploit the synthetic roots

Can we do better?

Main problems

- Over $\mathbb{C}$, the multiplications with powers of ω end up being too expensive
- Schönhage-Strassen does not fully exploit the synthetic roots

Recent progress

- Fürer 2007 $M(n) = O(n \log n\, 2^{O(\log^* n)})$
- Harvey-vdH-Lecerf 2014 $M(n) = O(n \log n\, 8^{\log^* n})$
- Harvey 2017 $M(n) = O(n \log n\, 6^{\log^* n})$
- Harvey-vdH 2017 $M(n) = O(n \log n\, (4\sqrt{2})^{\log^* n})$
- Harvey-vdH 2018 $M(n) = O(n \log n\, 4^{\log^* n})$

Multivariate FFTs

1427247692705959881058285969449495136382746624

Multivariate FFTs

1427247692705959881058285969449495136382746624

$$\rightsquigarrow$$

$$1427247692\, v^3 + 705959881058\, v^2 + 285969449495\, v + 136382746624$$

Multivariate FFTs

$$1427247692705959881058285969449495136382746624$$

$$\wr$$

$$1427247692\, v^3 + 705959881058\, v^2 + 285969449495\, v + 136382746624$$

$$\wr$$

$$\begin{aligned}
&(\, u^3 + 427\, u^2 + 247\, u + 692)\, v^3 + \\
&(705\, u^3 + 959\, u^2 + 881\, u + 58)\, v^2 + \\
&(285\, u^3 + 969\, u^2 + 449\, u + 495)\, v + \\
&(136\, u^3 + 382\, u^2 + 746\, u + 624)
\end{aligned}$$

Multivariate FFTs

$$1427247692705959881058285969449495136382746624$$

$$\wr$$

$$1427247692\,v^3 + 705959881058\,v^2 + 285969449495\,v + 136382746624$$

$$\wr$$

$$\begin{aligned}
&(\quad\;\; u^3 + 427\,u^2 + 247\,u + 692)\,v^3 + \\
&(705\,u^3 + 959\,u^2 + 881\,u + \;\;58)\,v^2 + \\
&(285\,u^3 + 969\,u^2 + 449\,u + 495)\,v + \\
&(136\,u^3 + 382\,u^2 + 746\,u + 624)
\end{aligned}$$

$$\mathbb{K}[u,v]/(u^m - 1, v^n - 1) \;\cong\; \bigoplus_{\substack{0 \leqslant i < m \\ 0 \leqslant j < n}} \mathbb{K}[u,v]/(u - \omega_m^i, v - \omega_n^j)$$

Multivariate FFTs

$$1427247692705959881058285969449495136382746624$$

$$\wr\downarrow$$

$$1427247692\, v^3 + 705959881058\, v^2 + 285969449495\, v + 136382746624$$

$$\wr\downarrow$$

$$\begin{aligned}
&(\quad u^3 + 427\, u^2 + 247\, u + 692)\, v^3 + \\
&(705\, u^3 + 959\, u^2 + 881\, u + \ \ 58)\, v^2 + \\
&(285\, u^3 + 969\, u^2 + 449\, u + 495)\, v + \\
&(136\, u^3 + 382\, u^2 + 746\, u + 624)
\end{aligned}$$

$$\mathbb{K}[u,v]/(u^m - 1, v^n - 1) \;\cong\; \bigoplus_{\substack{0 \leqslant i < m \\ 0 \leqslant j < n}} \mathbb{K}[u,v]/(u - \omega_m^i, v - \omega_n^j)$$

$$\mathsf{F}(m,n) \;\leqslant\; n\,\mathsf{F}(m) + m\,\mathsf{F}(n) + [\text{data rearrangements}]$$

Multivariate FFTs

$$1427247692705959881058285969449495136382746624$$

$$\wr$$

$$1427247692\,v^3 + 705959881058\,v^2 + 285969449495\,v + 136382746624$$

$$\wr$$

$$\begin{aligned}
&(u^3 + 427\,u^2 + 247\,u + 692)\,v^3 + \\
&(705\,u^3 + 959\,u^2 + 881\,u + 58)\,v^2 + \\
&(285\,u^3 + 969\,u^2 + 449\,u + 495)\,v + \\
&(136\,u^3 + 382\,u^2 + 746\,u + 624)
\end{aligned}$$

$$\mathbb{K}[u,v]/(u^m - 1, v^n - 1) \;\cong\; \bigoplus_{\substack{0 \leqslant i < m \\ 0 \leqslant j < n}} \mathbb{K}[u,v]/(u - \omega_m^i, v - \omega_n^j)$$

$$\mathrm{F}(m,n) \;\leqslant\; n\,\mathrm{F}(m) + m\,\mathrm{F}(n) + [\text{data rearrangements}]$$

Problem: multiplication doubles degree in each variable

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/n\mathbb{Z}$$

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/n\mathbb{Z}$$

$$x^{\mathbb{Z}/mn\mathbb{Z}} \cong u^{\mathbb{Z}/m\mathbb{Z}} \times v^{\mathbb{Z}/n\mathbb{Z}}$$

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/n\mathbb{Z}$$

$$x^{\mathbb{Z}/mn\mathbb{Z}} \cong u^{\mathbb{Z}/m\mathbb{Z}} \times v^{\mathbb{Z}/n\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{mn} - 1) &\cong \mathbb{K}[u]/(u^m - 1) \otimes \mathbb{K}[v]/(v^n - 1) \\ &\cong \mathbb{K}[u, v]/(u^m - 1, v^n - 1) \end{aligned}$$

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/n\mathbb{Z}$$

$$x^{\mathbb{Z}/mn\mathbb{Z}} \cong u^{\mathbb{Z}/m\mathbb{Z}} \times v^{\mathbb{Z}/n\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{mn}-1) &\cong \mathbb{K}[u]/(u^m-1) \otimes \mathbb{K}[v]/(v^n-1) \\ &\cong \mathbb{K}[u,v]/(u^m-1, v^n-1) \end{aligned}$$

$$\mathrm{F}(n\,m) \leqslant n\,\mathrm{F}(m) + m\,\mathrm{F}(n) + [\text{data rearrangements}]$$

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/n\mathbb{Z}$$

$$x^{\mathbb{Z}/mn\mathbb{Z}} \cong u^{\mathbb{Z}/m\mathbb{Z}} \times v^{\mathbb{Z}/n\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{mn}-1) &\cong \mathbb{K}[u]/(u^m-1) \otimes \mathbb{K}[v]/(v^n-1) \\ &\cong \mathbb{K}[u,v]/(u^m-1, v^n-1) \end{aligned}$$

$$\mathsf{F}(n\,m) \leqslant n\,\mathsf{F}(m) + m\,\mathsf{F}(n) + [\text{data rearrangements}]$$

Advantage: multiplication only doubles degree of original variable

Lifting the Chinese remainder theorem

$$\gcd(m, n) = 1$$

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/n\mathbb{Z}$$

$$x^{\mathbb{Z}/mn\mathbb{Z}} \cong u^{\mathbb{Z}/m\mathbb{Z}} \times v^{\mathbb{Z}/n\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{mn}-1) &\cong \mathbb{K}[u]/(u^m-1) \otimes \mathbb{K}[v]/(v^n-1) \\ &\cong \mathbb{K}[u,v]/(u^m-1, v^n-1) \end{aligned}$$

$$\mathsf{F}(n\,m) \leqslant n\,\mathsf{F}(m) + m\,\mathsf{F}(n) + [\text{data rearrangements}]$$

Advantage: multiplication only doubles degree of original variable

Problem: $\gcd(m, n) = 1 \Longrightarrow$ we cannot share primitive roots of unity

Wishful thinking

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

Wishful thinking

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

$$\rightsquigarrow$$

$$\mathbb{K}[x]/(x^{n_1 \cdots n_d} - 1)$$

Wishful thinking

$$\mathbb{K}[x]/(x^N - 1)$$
$$\rightsquigarrow$$
$$\mathbb{K}[x]/(x^{n_1 \cdots n_d} - 1)$$
$$\rightsquigarrow$$
$$\mathbb{K}[u_1, \ldots, u_d]/(u_1^{n_1} - 1, \ldots, u_d^{n_d} - 1)$$

Wishful thinking

$$\mathbb{K}[x]/(x^N - 1)$$
$$\rightsquigarrow$$
$$\mathbb{K}[x]/(x^{n_1 \cdots n_d} - 1)$$
$$\rightsquigarrow$$
$$\mathbb{K}[u_1, \ldots, u_d]/(u_1^{n_1} - 1, \ldots, u_d^{n_d} - 1)$$
$$\rightsquigarrow$$
$$\mathbb{K}[u_1, \ldots, u_d]/(u_1^{n} - 1, \ldots, u_d^{n} - 1)$$

Wishful thinking

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

$$\rightsquigarrow$$

$$\mathbb{K}[x]/(x^{n_1 \cdots n_d} - 1)$$

$$\rightsquigarrow$$

$$\mathbb{K}[u_1, \ldots, u_d]/(u_1^{n_1} - 1, \ldots, u_d^{n_d} - 1)$$

$$\rightsquigarrow$$

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

$$\rightsquigarrow$$

$$(\mathbb{K}[u_1]/(u_1^n - 1))\,[u_2, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1)$$

Thank you !

http://www.TeXmacs.org