Polynomial Multiplication Techniques (II)

Bo-Yin Yang (with Matthias Kannwischer)

June 8, 2023 at Vodice

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem over $\mathbb{Z}$)
If m, n are coprime, then $\mathbb{Z}/\langle mn\rangle \cong \mathbb{Z}/\langle m\rangle \times \mathbb{Z}/\langle n\rangle$ as rings

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem over $\mathbb{Z}$)
If m, n are coprime, then $\mathbb{Z}/\langle mn\rangle \cong \mathbb{Z}/\langle m\rangle \times \mathbb{Z}/\langle n\rangle$ as rings

Example ($m = 5,\ n = 7$)

- Let $\mathbb{Z}/\langle 35\rangle \to \mathbb{Z}/\langle 5\rangle \times \mathbb{Z}/\langle 7\rangle$ be defined by $a \mapsto (a \mod 5,\ a \mod 7)$
  Modular arithmetic preserves addition and multiplication

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem over $\mathbb{Z}$)
If m, n are coprime, then $\mathbb{Z}/\langle mn \rangle \cong \mathbb{Z}/\langle m \rangle \times \mathbb{Z}/\langle n \rangle$ as rings

Example ($m = 5,\ n = 7$)

- Let $\mathbb{Z}/\langle 35 \rangle \to \mathbb{Z}/\langle 5 \rangle \times \mathbb{Z}/\langle 7 \rangle$ be defined by $a \mapsto (a \mod 5,\ a \mod 7)$
  Modular arithmetic preserves addition and multiplication
- Extended GCD gives $3 * 5 + (-2) * 7 = 1$
  $(-2) * 7$ maps to $(1, 0)$ and $3 * 5$ maps to $(0, 1)$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem over $\mathbb{Z}$)
If m, n are coprime, then $\mathbb{Z}/\langle mn\rangle \cong \mathbb{Z}/\langle m\rangle \times \mathbb{Z}/\langle n\rangle$ as rings

Example ($m = 5,\ n = 7$)

- Let $\mathbb{Z}/\langle 35\rangle \to \mathbb{Z}/\langle 5\rangle \times \mathbb{Z}/\langle 7\rangle$ be defined by $a \mapsto (a \mod 5,\ a \mod 7)$
  Modular arithmetic preserves addition and multiplication
- Extended GCD gives $3 * 5 + (-2) * 7 = 1$
  $(-2) * 7$ maps to $(1, 0)$ and $3 * 5$ maps to $(0, 1)$
- The preimage of (b, c) is $(-14 * b + 15 * c)$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem over $\mathbb{Z}$)
If m, n are coprime, then $\mathbb{Z}/\langle mn \rangle \cong \mathbb{Z}/\langle m \rangle \times \mathbb{Z}/\langle n \rangle$ as rings

Example ($m = 5,\ n = 7$)

- Let $\mathbb{Z}/\langle 35 \rangle \to \mathbb{Z}/\langle 5 \rangle \times \mathbb{Z}/\langle 7 \rangle$ be defined by $a \mapsto (a \mod 5,\ a \mod 7)$
  Modular arithmetic preserves addition and multiplication
- Extended GCD gives $3 * 5 + (-2) * 7 = 1$
  $(-2) * 7$ maps to $(1, 0)$ and $3 * 5$ maps to $(0, 1)$
- The preimage of (b, c) is $(-14 * b + 15 * c)$
- If a, a' has the same image, then $a - a'$ maps to $(0, 0)$.
  Both $5, 7$ are divisors of $a - a'$, so $a = a' \pmod{35}$

CRT use case in $R[x]$: a multiplication converts to two half-sized multiplications

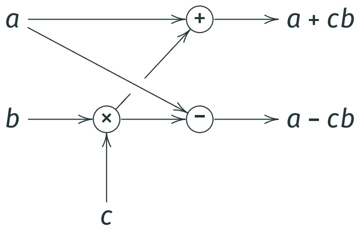
- $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$, since $\frac{-1}{2c}(x^n - c) + \frac{1}{2c}(x^n + c) = 1$

CRT use case in $R[x]$: a multiplication converts to two half-sized multiplications

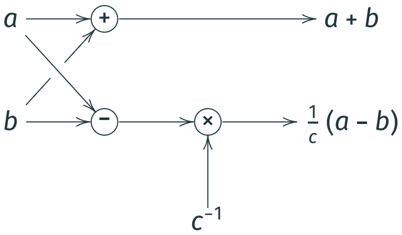
- $R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$, since $\frac{-1}{2c}(x^n - c) + \frac{1}{2c}(x^n + c) = 1$
- $\begin{bmatrix} a_0 + \cdots + a_{n-1}x^{n-1} \\ +a_n x^n + \cdots + a_{2n-1}x^{2n-1} \end{bmatrix} \longrightarrow \begin{bmatrix} (a_0 + a_n c) + \cdots + (a_{n-1} + a_{2n-1}c)x^{n-1} \\ (a_0 - a_n c) + \cdots + (a_{n-1} - a_{2n-1}c)x^{n-1} \end{bmatrix}$

CRT use case in $R[x]$: a multiplication converts to two half-sized multiplications

- $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$, since $\frac{-1}{2c}(x^n - c) + \frac{1}{2c}(x^n + c) = 1$
- $\begin{bmatrix} a_0 + \cdots + a_{n-1}x^{n-1} \\ +a_n x^n + \cdots + a_{2n-1}x^{2n-1} \end{bmatrix} \longrightarrow \begin{bmatrix} (a_0 + a_n c) + \cdots + (a_{n-1} + a_{2n-1}c)x^{n-1} \\ (a_0 - a_n c) + \cdots + (a_{n-1} - a_{2n-1}c)x^{n-1} \end{bmatrix}$
- $f(x) \cdot \frac{1}{2c}(x^n + c) + g(x) \cdot \frac{-1}{2c}(x^n - c) = \frac{f(x)+g(x)}{2} + \frac{f(x)-g(x)}{2c}x^n \longleftarrow \begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$



(a) Forward: Cooley–Tukey Butterfly



(b) Inverse: Gentleman–Sande Butterfly

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ by repeating CRT, if $\exists \zeta \in R$ with $\zeta^{2^{k-1}} = -1$.

$$R[x]/\langle x^{2^k} - 1\rangle = R[x]/\langle x^{2^{k-1}} - 1\rangle \times R[x]/\langle x^{2^{k-1}} + 1\rangle$$

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ **by repeating CRT, if** $\exists\zeta \in R$ **with** $\zeta^{2^{k-1}} = -1$**.**

$$R[x]/\langle x^{2^k} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{10\cdots0}^{k-1}{}_b}\rangle$$

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ **by repeating CRT, if** $\exists\zeta \in R$ **with** $\zeta^{2^{k-1}} = -1$**.**

$$R[x]/\langle x^{2^k} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{10\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}} - 1\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} + 1\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - i\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} + i\rangle}, \quad i = \zeta^{2^{k-2}}$$

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ by repeating CRT, if $\exists\zeta \in R$ with $\zeta^{2^{k-1}} = -1$.

$$R[x]/\langle x^{2^k} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{1\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} \zeta^{1\overbrace{0\cdots0}^{k-1}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{01\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{11\overbrace{0\cdots0}^{k-2}{}_b}\rangle}$$

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ by repeating CRT, if $\exists\zeta \in R$ with $\zeta^{2^{k-1}} = -1$.

$$R[x]/\langle x^{2^k} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{\overbrace{10\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{\overbrace{0\cdots0}^{k}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} \zeta^{1\overbrace{0\cdots0}^{k-1}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{01\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{11\overbrace{0\cdots0}^{k-2}{}_b}\rangle}$$

$$= \frac{R[x]}{\langle x^{2^{k-3}} - 1\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} + 1\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - i\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} + i\rangle}$$

$$\frac{R[x]}{\langle x^{2^{k-3}} - \omega_8\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \omega_8^5\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \omega_8^3\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \omega_8^7\rangle}, \quad \omega_8 = \zeta^{2^{k-3}}$$

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ by repeating CRT, if $\exists \zeta \in R$ with $\zeta^{2^{k-1}} = -1$.

$$R[x]/\langle x^{2^k} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{(1\overbrace{0\cdots0}^{k-1})_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} \zeta^{(1\overbrace{0\cdots0}^{k-1})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{(01\overbrace{0\cdots0}^{k-2})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{(11\overbrace{0\cdots0}^{k-2})_b}\rangle}$$

$$= \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(1\overbrace{0\cdots0}^{k-1})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(01\overbrace{0\cdots0}^{k-2})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(11\overbrace{0\cdots0}^{k-2})_b}\rangle}$$

$$\frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(001\overbrace{0\cdots0}^{k-3})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(101\overbrace{0\cdots0}^{k-3})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(011\overbrace{0\cdots0}^{k-3})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(111\overbrace{0\cdots0}^{k-3})_b}\rangle}$$

FFT/ NTT

multiplication in $R[x]/\langle x^{2^k} - 1\rangle$ by repeating CRT, if $\exists\zeta \in R$ with $\zeta^{2^{k-1}} = -1$.

$$R[x]/\langle x^{2^k} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{(1\overbrace{0\cdots0}^{k-1})_b}\rangle$$

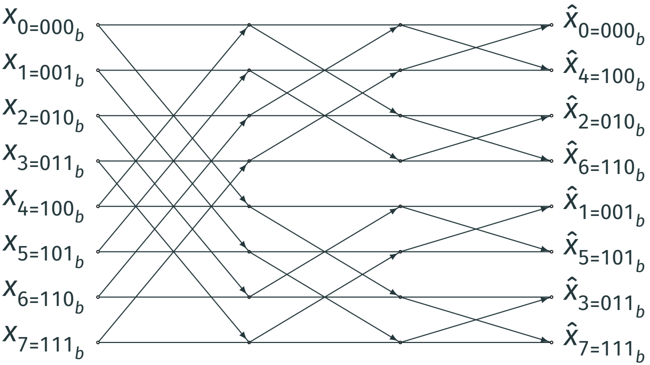
$$= \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} \zeta^{(1\overbrace{0\cdots0}^{k-1})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{(01\overbrace{0\cdots0}^{k-2})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{(11\overbrace{0\cdots0}^{k-2})_b}\rangle}$$

$$= \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(\overbrace{0\cdots0}^{k})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(1\overbrace{0\cdots0}^{k-1})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(01\overbrace{0\cdots0}^{k-2})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(11\overbrace{0\cdots0}^{k-2})_b}\rangle}$$

$$\frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(001\overbrace{0\cdots0}^{k-3})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(101\overbrace{0\cdots0}^{k-3})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(011\overbrace{0\cdots0}^{k-3})_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}} - \zeta^{(111\overbrace{0\cdots0}^{k-3})_b}\rangle}$$

$$= \prod_{t=0}^{2^\ell-1} \frac{R[x]}{\langle x^{2^{k-\ell}} - \zeta^{\mathrm{brv}_k(t)}\rangle} = \prod_{t=0}^{2^k-1} \frac{R[x]}{\langle x - \zeta^{\mathrm{brv}_k(t)}\rangle} \left(= \overbrace{R \times \cdots \times R}^{2^k} \right)$$

FFT/NTT: Bit-reversed output order in a radix-2 NTT.



It is standard to “bit-reverse” the inputs of the NTT or FFT. But for polynomial multiplication, the order of the output is irrelevant!

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists\zeta \in R$, $\zeta^{2^k} = -1$.

$$R[x]/\langle x^{2^k}+1\rangle = R[x]/\langle x^{2^{k-1}}-i\rangle \times R[x]/\langle x^{2^{k-1}}+i\rangle, \quad i = \zeta^{2^{k-1}}$$

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists \zeta \in R$, $\zeta^{2^k}=-1$.

$$R[x]/\langle x^{2^k} - \zeta^{1\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{01\overbrace{0\cdots0}^{k-1}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{11\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists\zeta\in R$, $\zeta^{2^k}=-1$.

$$R[x]/\langle x^{2^k}-\zeta^{1\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}}-\zeta^{01\overbrace{0\cdots0}^{k-1}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}}-\zeta^{11\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}}-\omega_8\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\omega_8^5\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\omega_8^3\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\omega_8^7\rangle}, \quad \omega_8=\zeta^{2^{k-2}}$$

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists\zeta \in R$, $\zeta^{2^k} = -1$.

$$R[x]/\langle x^{2^k} - \zeta^{1\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}} - \zeta^{01\overbrace{0\cdots0}^{k-1}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}} - \zeta^{11\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{001\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{101\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{011\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}} - \zeta^{111\overbrace{0\cdots0}^{k-2}{}_b}\rangle}$$

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists\zeta\in R$, $\zeta^{2^k}=-1$.

$$R[x]/\langle x^{2^k}-\zeta^{1\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}}-\zeta^{01\overbrace{0\cdots0}^{k-1}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}}-\zeta^{11\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{001\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{101\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{011\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{111\overbrace{0\cdots0}^{k-2}{}_b}\rangle}$$

$$= \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{9}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{5}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{13}\rangle}$$

$$\frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{3}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{11}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{7}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\omega_{16}^{15}\rangle}, \quad \omega_{16}=\zeta^{2^{k-3}}$$

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists\zeta\in R$, $\zeta^{2^k}=-1$.

$$R[x]/\langle x^{2^k}-\zeta^{1\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}}-\zeta^{01\overbrace{0\cdots0}^{k-1}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}}-\zeta^{11\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{001\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{101\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{011\overbrace{0\cdots0}^{k-2}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{111\overbrace{0\cdots0}^{k-2}{}_b}\rangle}$$

$$= \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0001\overbrace{0\cdots0}^{k-3}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1001\overbrace{0\cdots0}^{k-3}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0101\overbrace{0\cdots0}^{k-3}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1101\overbrace{0\cdots0}^{k-3}{}_b}\rangle}$$

$$\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0011\overbrace{0\cdots0}^{k-3}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1011\overbrace{0\cdots0}^{k-3}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0111\overbrace{0\cdots0}^{k-3}{}_b}\rangle} \times \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1111\overbrace{0\cdots0}^{k-3}{}_b}\rangle}$$

Negacyclic FFT/NTT: multiply in $R[x]/\langle x^{2^k}+1\rangle$, $\exists\zeta\in R$, $\zeta^{2^k}=-1$.

$$R[x]/\langle x^{2^k}-\zeta^{1\overbrace{0\cdots0}^{k}{}_b}\rangle = R[x]/\langle x^{2^{k-1}}-\zeta^{01\overbrace{0\cdots0}^{k-1}{}_b}\rangle \times R[x]/\langle x^{2^{k-1}}-\zeta^{11\overbrace{0\cdots0}^{k-1}{}_b}\rangle$$

$$= \frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{001\overbrace{0\cdots0}^{k-2}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{101\overbrace{0\cdots0}^{k-2}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{011\overbrace{0\cdots0}^{k-2}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-2}}-\zeta^{111\overbrace{0\cdots0}^{k-2}{}_b}\rangle}$$

$$= \frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0001\overbrace{0\cdots0}^{k-3}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1001\overbrace{0\cdots0}^{k-3}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0101\overbrace{0\cdots0}^{k-3}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1101\overbrace{0\cdots0}^{k-3}{}_b}\rangle}$$

$$\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0011\overbrace{0\cdots0}^{k-3}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1011\overbrace{0\cdots0}^{k-3}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{0111\overbrace{0\cdots0}^{k-3}{}_b}\rangle}\times\frac{R[x]}{\langle x^{2^{k-3}}-\zeta^{1111\overbrace{0\cdots0}^{k-3}{}_b}\rangle}$$

$$= \prod_{t=2^\ell}^{2^{\ell+1}-1}\frac{R[x]}{\langle x^{2^{k-\ell}}-\zeta^{\mathrm{brv}_{k+1}(t)}\rangle} = \prod_{t=2^k}^{2^{k+1}-1}\frac{R[x]}{\langle x-\zeta^{\mathrm{brv}_{k+1}(t)}\rangle}\left(=\overbrace{R\times\cdots\times R}^{2^k}\right)$$

FFT/ NTT (recap)

- We can multiply elements in $R[x]/\langle x^{2^k} - 1\rangle$ by applying the CRT repeatedly, if there is $\zeta \in R$ with $\zeta^{2^{k-1}} = -1$

FFT/ NTT (recap)

- We can multiply elements in $R[x]/\langle x^{2^k} - 1\rangle$ by applying the CRT repeatedly, if there is $\zeta \in R$ with $\zeta^{2^{k-1}} = -1$
- To multiply $f(x), g(x) \in R[x]/\langle x^{2^k} - 1\rangle$, we first map them into $v_f, v_g \in R^{2^k}$ Next, multiply the vectors v_f, v_g coordinate-wise to get $v_h \in R^{2^k}$, then an inverse mapping to get $h(x) \in R[x]/\langle x^{2^k} - 1\rangle$, which satisfies $h(x) = f(x) \cdot g(x)$

FFT/ NTT (recap)

- We can multiply elements in $R[x]/\langle x^{2^k} - 1\rangle$ by applying the CRT repeatedly, if there is $\zeta \in R$ with $\zeta^{2^{k-1}} = -1$
- To multiply $f(x), g(x) \in R[x]/\langle x^{2^k} - 1\rangle$, we first map them into $v_f, v_g \in R^{2^k}$ Next, multiply the vectors v_f, v_g coordinate-wise to get $v_h \in R^{2^k}$, then an inverse mapping to get $h(x) \in R[x]/\langle x^{2^k} - 1\rangle$, which satisfies $h(x) = f(x) \cdot g(x)$
- # ‘operations’:
  $O(k2^k)$ in mapping: there are k steps, each doing $3 \cdot 2^{k-1}$ basic operations
  $O(2^k)$ in vector coordinate-wise multiplication

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$, notice that $2^4 = -1 \pmod{17}$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4+1 = (x^2-4)(x^2+4) = (x-2)(x+2)(x-8)(x+8)$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4 + 1 = (x^2 - 4)(x^2 + 4) = (x - 2)(x + 2)(x - 8)(x + 8)$

Multiply $f(x) = 2x^3 + 7x^2 + x + 8$ and $g(x) = 2x^3 + 0x^2 + 4x + 8$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4+1 = (x^2-4)(x^2+4) = (x-2)(x+2)(x-8)(x+8)$

Multiply $f(x) = 2x^3+7x^2+x+8$ and $g(x) = 2x^3+0x^2+4x+8$

$f(x) \to (9x+36, -7x-20) \to (54, 18, -76, 36) = (3, 1, 9, 2)$

$g(x) \to (12x+8, -4x+8) \to (32, -16, -24, 40) = (-2, 1, -7, 6)$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4 + 1 = (x^2 - 4)(x^2 + 4) = (x - 2)(x + 2)(x - 8)(x + 8)$

Multiply $f(x) = 2x^3 + 7x^2 + x + 8$ and $g(x) = 2x^3 + 0x^2 + 4x + 8$

$f(x) \rightarrow (9x + 36, -7x - 20) \rightarrow (54, 18, -76, 36) = (3, 1, 9, 2)$

$g(x) \rightarrow (12x + 8, -4x + 8) \rightarrow (32, -16, -24, 40) = (-2, 1, -7, 6)$

$f(x)g(x) \leftarrow (-6, 1, 5, -5) = (-6, 1, -63, 12)$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4+1 = (x^2-4)(x^2+4) = (x-2)(x+2)(x-8)(x+8)$

Multiply $f(x) = 2x^3+7x^2+x+8$ and $g(x) = 2x^3+0x^2+4x+8$

$f(x) \to (9x+36, -7x-20) \to (54, 18, -76, 36) = (3, 1, 9, 2)$

$g(x) \to (12x+8, -4x+8) \to (32, -16, -24, 40) = (-2, 1, -7, 6)$

$f(x)g(x) \leftarrow (-6, 1, 5, -5) = (-6, 1, -63, 12)$

Apply inverse transform:

$(-6, 1, 5, -5) \to \frac{1}{2}(-5 + \frac{-7}{2}x, \quad 0 + \frac{10}{8}x) = \frac{1}{2}(-5+5x, \quad 0-3x)$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4+1 = (x^2-4)(x^2+4) = (x-2)(x+2)(x-8)(x+8)$

Multiply $f(x) = 2x^3+7x^2+x+8$ and $g(x) = 2x^3+0x^2+4x+8$

$f(x) \to (9x+36, -7x-20) \to (54, 18, -76, 36) = (3, 1, 9, 2)$

$g(x) \to (12x+8, -4x+8) \to (32, -16, -24, 40) = (-2, 1, -7, 6)$

$f(x)g(x) \leftarrow (-6, 1, 5, -5) = (-6, 1, -63, 12)$

Apply inverse transform:

$$(-6, 1, 5, -5) \to \frac{1}{2}(-5+\frac{-7}{2}x, \quad 0+\frac{10}{8}x) = \frac{1}{2}(-5+5x, \quad 0-3x)$$

$$\to \frac{1}{4}[(-5+2x)+\frac{-5+8x}{4}x^2] = \frac{1}{4}[2x^3+3x^2+2x-5]$$

$$= 9x^3+5x^2+9x+3$$

FFT/ NTT: Example

In $\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$, notice that $2^4 = -1 \pmod{17}$

We will use $x^4+1 = (x^2-4)(x^2+4) = (x-2)(x+2)(x-8)(x+8)$

Multiply $f(x) = 2x^3+7x^2+x+8$ and $g(x) = 2x^3+0x^2+4x+8$

$f(x) \to (9x+36, -7x-20) \to (54, 18, -76, 36) = (3, 1, 9, 2)$

$g(x) \to (12x+8, -4x+8) \to (32, -16, -24, 40) = (-2, 1, -7, 6)$

$f(x)g(x) \leftarrow (-6, 1, 5, -5) = (-6, 1, -63, 12)$

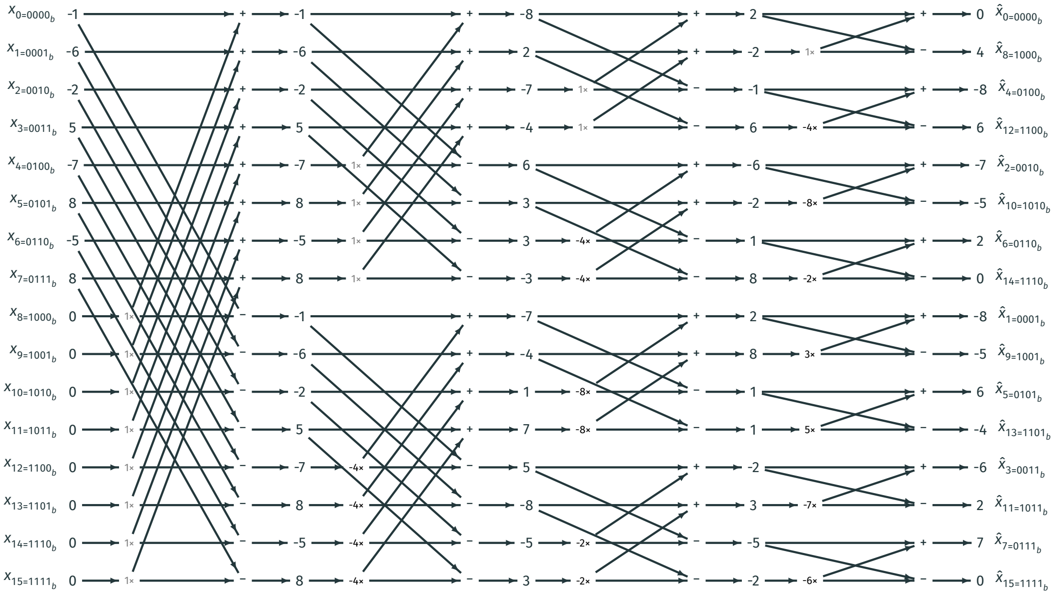
Apply inverse transform:

$$(-6,1,5,-5) \to \frac{1}{2}(-5+\frac{-7}{2}x, \quad 0+\frac{10}{8}x) = \frac{1}{2}(-5+5x, \quad 0-3x)$$

$$\to \frac{1}{4}[(-5+2x)+\frac{-5+8x}{4}x^2] = \frac{1}{4}[2x^3+3x^2+2x-5]$$

$$= 9x^3+5x^2+9x+3 = f(x)g(x)$$

Process of Splitting ($\mathbb{F}_{17}[x]/(x^{16} - 1), \zeta = 3$)

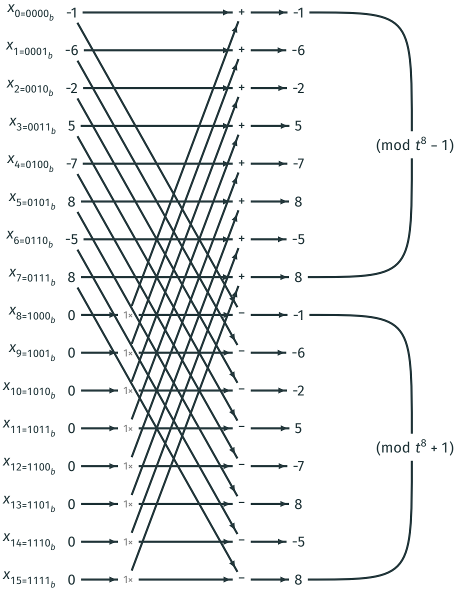


Process of Splitting ($\mathbb{F}_{17}[x]/(x^{16} - 1)$, $\zeta = 3$)

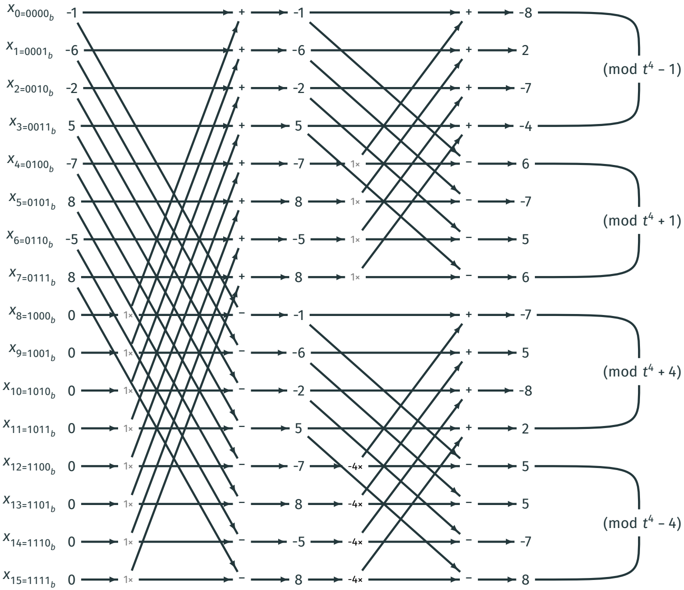
$x_{0=0000_b}$	-1
$x_{1=0001_b}$	-6
$x_{2=0010_b}$	-2
$x_{3=0011_b}$	5
$x_{4=0100_b}$	-7
$x_{5=0101_b}$	8
$x_{6=0110_b}$	-5
$x_{7=0111_b}$	8
$x_{8=1000_b}$	0
$x_{9=1001_b}$	0
$x_{10=1010_b}$	0
$x_{11=1011_b}$	0
$x_{12=1100_b}$	0
$x_{13=1101_b}$	0
$x_{14=1110_b}$	0
$x_{15=1111_b}$	0

(mod $t^{16} - 1$)

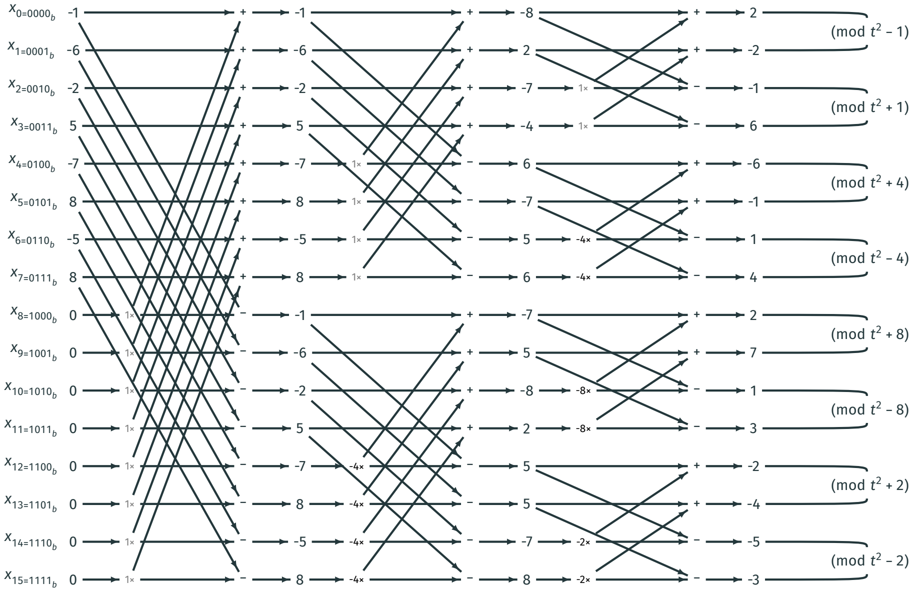
Process of Splitting ($\mathbb{F}_{17}[x]/(x^{16} - 1), \zeta = 3$)



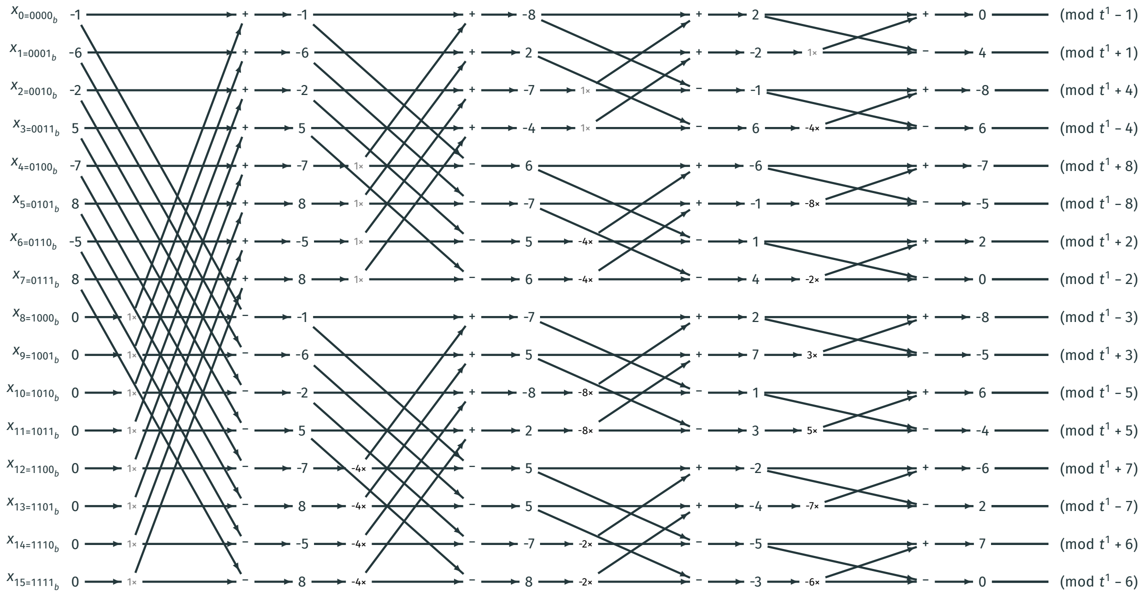
Process of Splitting ($\mathbb{F}_{17}[x]/(x^{16} - 1), \zeta = 3$)



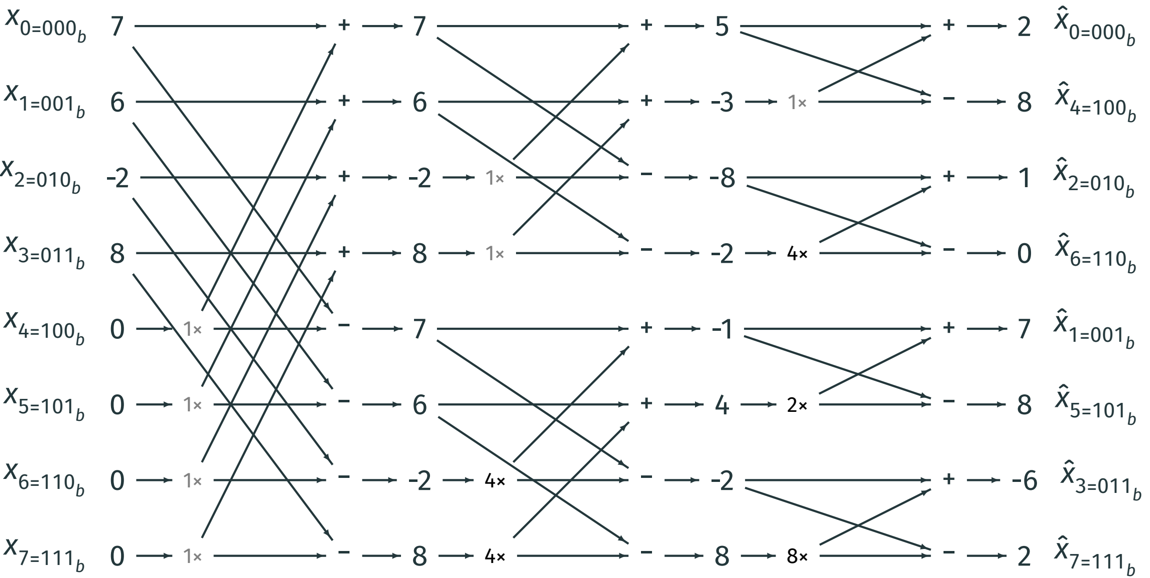
Process of Splitting ($\mathbb{F}_{17}[x]/(x^{16} - 1), \zeta = 3$)



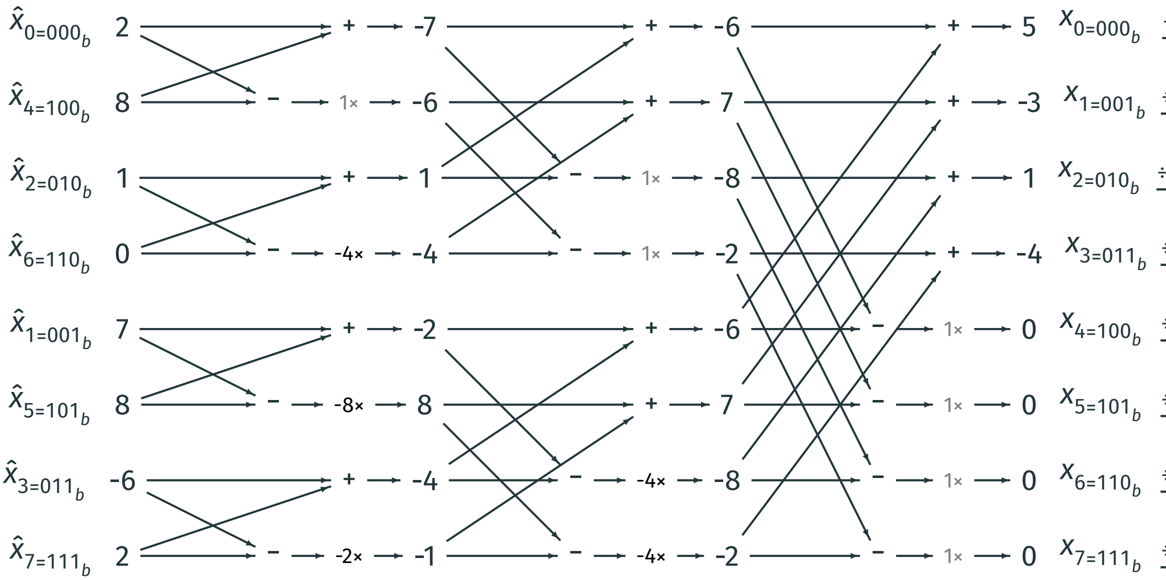
Process of Splitting ($\mathbb{F}_{17}[x]/(x^{16} - 1)$, $\zeta = 3$)



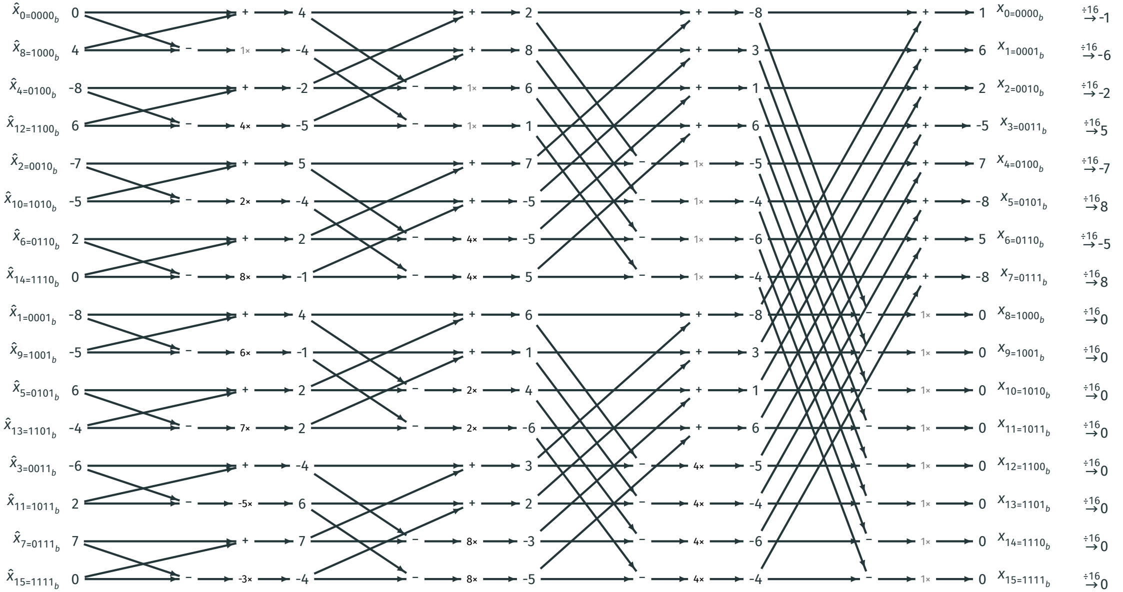
FFT/NTT Example ($\mathbb{F}_{17}[x]/(x^8 - 1), \zeta = 2$)



FFT/NTT Example ($\mathbb{F}_{17}[x]/(x^8 - 1), \zeta = 2$) ii



FFT/NTT Example ($\mathbb{F}_{17}[x]/(x^{16} - 1), \zeta = 3$)



FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 1

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 1

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 1

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 1

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

Step 1

keep going ...

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

Step 1

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16} + 1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■

keep going ...

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

keep going ...

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 2

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 3

■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

Step 3

- 1 step further → twice many blocks

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16} + 1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 3

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 3

keep going ...

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 3

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

Step 3

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 4

■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

  Step 4

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

  ■: scalar multiplication ■: addition/ subtraction

Step 4

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 4

keep going ...

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)

■: scalar multiplication ■: addition/ subtraction

Step 4

- 1 step further → twice many blocks & distance between pairs halved

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)
  ■: scalar multiplication ■: addition/ subtraction

■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■

- 1 step further → twice many blocks & distance between pairs halved
  One can keep track of the total number of blocks and the distance between pairs

FFT/ NTT: Memory Access

- Let's see how we access memory when doing FFT (*e.g.* in $R[x]/\langle x^{16}+1\rangle$)
  ■: scalar multiplication ■: addition/ subtraction

- 1 step further → twice many blocks & distance between pairs halved
  One can keep track of the total number of blocks and the distance between pairs
- Inverse transform does everything in the reverse order

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2
- An example: for $R = \mathbb{Z}_{73}[x]/\langle x^4 - x^3 - 2 \rangle$, what can we do?

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2
- An example: for $R = \mathbb{Z}_{73}[x]/\langle x^4 - x^3 - 2 \rangle$, what can we do?
- Ignore modulo $(x^4 - x^3 - 2)$: regard $f(x), g(x) \in \mathbb{Z}_{73}[x]$, having degree ≤ 3

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2
- An example: for $R = \mathbb{Z}_{73}[x]/\langle x^4 - x^3 - 2 \rangle$, what can we do?
- Ignore modulo $(x^4 - x^3 - 2)$: regard $f(x), g(x) \in \mathbb{Z}_{73}[x]$, having degree ≤ 3
- We know that $\deg[f(x)g(x)] \leq 6$, so modulo $(x^8 - 1)$ is redundant

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2
- An example: for $R = \mathbb{Z}_{73}[x]/\langle x^4 - x^3 - 2 \rangle$, what can we do?
- Ignore modulo $(x^4 - x^3 - 2)$: regard $f(x), g(x) \in \mathbb{Z}_{73}[x]$, having degree ≤ 3
- We know that $\deg[f(x)g(x)] \le 6$, so modulo $(x^8 - 1)$ is redundant
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{73}[x]/\langle x^8 - 1 \rangle$
  In this ring, we can do FFT since $10^4 = -1 \pmod{73}$

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2
- An example: for $R = \mathbb{Z}_{73}[x]/\langle x^4 - x^3 - 2 \rangle$, what can we do?
- Ignore modulo $(x^4 - x^3 - 2)$: regard $f(x), g(x) \in \mathbb{Z}_{73}[x]$, having degree ≤ 3
- We know that $\deg[f(x)g(x)] \leq 6$, so modulo $(x^8 - 1)$ is redundant
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{73}[x]/\langle x^8 - 1 \rangle$
  In this ring, we can do FFT since $10^4 = -1 \pmod{73}$
- The result is $f(x)g(x) \mod (x^8 - 1)$, but it is also just $f(x)g(x)$

Applying FFT: Changing Polynomial Modulus

- To do normal FFT, the ring must be of the form $R[x]/\langle x^{nm} - \zeta^n \rangle$, n being a power of 2
- An example: for $R = \mathbb{Z}_{73}[x]/\langle x^4 - x^3 - 2 \rangle$, what can we do?
- Ignore modulo $(x^4 - x^3 - 2)$: regard $f(x), g(x) \in \mathbb{Z}_{73}[x]$, having degree ≤ 3
- We know that $\deg[f(x)g(x)] \leq 6$, so modulo $(x^8 - 1)$ is redundant
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{73}[x]/\langle x^8 - 1 \rangle$
  In this ring, we can do FFT since $10^4 = -1 \pmod{73}$
- The result is $f(x)g(x) \mod (x^8 - 1)$, but it is also just $f(x)g(x)$
- The output is $f(x)g(x) \mod (x^4 - x^3 - 2)$

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?
- Ignore modulo 7: regard $f(x), g(x) \in \mathbb{Z}[x]/\langle x^4 + 1\rangle$, with coefficients in $[-3, 3]$

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?
- Ignore modulo 7: regard $f(x), g(x) \in \mathbb{Z}[x]/\langle x^4 + 1\rangle$, with coefficients in $[-3, 3]$
- We know each coefficient of $f(x)g(x)$ has absolute value $\leq 3^2 \cdot 4 = 36$

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?
- Ignore modulo 7: regard $f(x), g(x) \in \mathbb{Z}[x]/\langle x^4 + 1\rangle$, with coefficients in $[-3, 3]$
- We know each coefficient of $f(x)g(x)$ has absolute value $\leq 3^2 \cdot 4 = 36$
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$ and in $\mathbb{Z}_{41}[x]/\langle x^4 + 1\rangle$
  In both rings, we can do FFT since $2^4 = -1 \pmod{17}$ and $3^4 = -1 \pmod{41}$

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?
- Ignore modulo 7: regard $f(x), g(x) \in \mathbb{Z}[x]/\langle x^4 + 1\rangle$, with coefficients in $[-3, 3]$
- We know each coefficient of $f(x)g(x)$ has absolute value $\leq 3^2 \cdot 4 = 36$
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$ and in $\mathbb{Z}_{41}[x]/\langle x^4 + 1\rangle$
  In both rings, we can do FFT since $2^4 = -1 \pmod{17}$ and $3^4 = -1 \pmod{41}$
- We will result in $f(x)g(x) \mod 17$ and $f(x)g(x) \mod 41$

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?
- Ignore modulo 7: regard $f(x), g(x) \in \mathbb{Z}[x]/\langle x^4 + 1\rangle$, with coefficients in $[-3, 3]$
- We know each coefficient of $f(x)g(x)$ has absolute value $\leq 3^2 \cdot 4 = 36$
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$ and in $\mathbb{Z}_{41}[x]/\langle x^4 + 1\rangle$
  In both rings, we can do FFT since $2^4 = -1 \pmod{17}$ and $3^4 = -1 \pmod{41}$
- We will result in $f(x)g(x) \mod 17$ and $f(x)g(x) \mod 41$
- Applying Chinese remainder theorem, we recover $f(x)g(x) \mod (17 * 41)$

Applying FFT: Changing Coefficient Ring

- To do FFT, we need that there are suitable roots of -1 in the coefficient ring
- An example: for $R = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$, what can we do?
- Ignore modulo 7: regard $f(x), g(x) \in \mathbb{Z}[x]/\langle x^4 + 1\rangle$, with coefficients in $[-3, 3]$
- We know each coefficient of $f(x)g(x)$ has absolute value $\leq 3^2 \cdot 4 = 36$
- We first multiply $f(x), g(x)$ in $\mathbb{Z}_{17}[x]/\langle x^4 + 1\rangle$ and in $\mathbb{Z}_{41}[x]/\langle x^4 + 1\rangle$
  In both rings, we can do FFT since $2^4 = -1 \pmod{17}$ and $3^4 = -1 \pmod{41}$
- We will result in $f(x)g(x) \mod 17$ and $f(x)g(x) \mod 41$
- Applying Chinese remainder theorem, we recover $f(x)g(x) \mod (17 * 41)$
- Shifting coefficients back to the range $[-36, 36]$, we recover $f(x)g(x)$
  The output is $f(x)g(x) \mod 7$

Twisting an FFT/NTT

Transforming $(\bmod\ x^N - c)$ **to** $(\bmod\ x^N - 1)$

If $\exists \xi \in R$ such that $\xi^N = c$, then this is an isomorphism

$$\begin{aligned} \frac{R[x]}{(x^N - c)} &\to \frac{R[y]}{(y^N - 1)} \\ f(x) &\mapsto f(\xi y) \\ a_0 + a_1 x + \cdots + a_{N-1} x^{N-1} &\mapsto a_0 + (a_1 \xi) y + \cdots + (a_{N-1} \xi^{N-1}) y^{N-1} \\ (a_0, a_1, a_2, \ldots, a_{N-1}) &\mapsto (a_0, a_1 \xi, a_2 \xi^2, \ldots, a_{N-1} \xi^{N-1}) \end{aligned}$$

but both eventually leads to copies of R, so the results are one to one identical.

Advantages of Twisting: Array Entries Size Control

Twisting swaps $N/2$ mults for nearly N mults. Why then? An algorithmic reason to twist is array entries' going out of bounds.

Twisted FFT Trick

Compare to std. FFT: $R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$

Twisted FFT Trick

Compare to std. FFT: $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$

- Base case of twisted FFT: (ζ is an n-th root of -1)
  $R[x]/\langle x^{2n} - 1 \rangle \cong R[x]/\langle x^n - 1 \rangle \times R[x]/\langle x^n + 1 \rangle$ with the 2^{nd} component
  $R[x]/\langle x^n + 1 \rangle \cong R[y]/\langle y^n - 1 \rangle$, by $x \leftrightarrow \zeta y$,so that $x^n + 1 \leftrightarrow (\zeta y)^n + 1 = -y^n + 1$

Twisted FFT Trick

Compare to std. FFT: $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$

- Base case of twisted FFT: (ζ is an n-th root of -1)
  $R[x]/\langle x^{2n} - 1 \rangle \cong R[x]/\langle x^n - 1 \rangle \times R[x]/\langle x^n + 1 \rangle$ with the 2^{nd} component
  $R[x]/\langle x^n + 1 \rangle \cong R[y]/\langle y^n - 1 \rangle$, by $x \leftrightarrow \zeta y$,so that $x^n + 1 \leftrightarrow (\zeta y)^n + 1 = -y^n + 1$
- The entire twisted FFT Trick: (ζ is an 2^{k-1}-th root of -1)
  $R[x]/\langle x^{2^k} - 1 \rangle \cong R[x]/\langle x^{2^{k-1}} - 1 \rangle \times R[x]/\langle x^{2^{k-1}} - 1 \rangle\{\zeta\}$

Twisted FFT Trick

Compare to std. FFT: $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$

- Base case of twisted FFT: (ζ is an n-th root of -1)

  $R[x]/\langle x^{2n} - 1 \rangle \cong R[x]/\langle x^n - 1 \rangle \times R[x]/\langle x^n + 1 \rangle$ with the 2^{nd} component

  $R[x]/\langle x^n + 1 \rangle \cong R[y]/\langle y^n - 1 \rangle$, by $x \leftrightarrow \zeta y$,so that $x^n + 1 \leftrightarrow (\zeta y)^n + 1 = -y^n + 1$
- The entire twisted FFT Trick: (ζ is an 2^{k-1}-th root of -1)

  $R[x]/\langle x^{2^k} - 1 \rangle \cong R[x]/\langle x^{2^{k-1}} - 1 \rangle \times R[x]/\langle x^{2^{k-1}} - 1 \rangle\{\zeta\}$

  $\cong \prod^2 \left(R[x]/\langle x^{2^{k-2}} - 1 \rangle \times R[x]/\langle x^{2^{k-2}} - 1 \rangle\{\zeta^2\} \right)$

Twisted FFT Trick

Compare to std. FFT: $R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$

- Base case of twisted FFT: (ζ is an n-th root of -1)

  $R[x]/\langle x^{2n} - 1\rangle \cong R[x]/\langle x^n - 1\rangle \times R[x]/\langle x^n + 1\rangle$ with the 2^{nd} component

  $R[x]/\langle x^n + 1\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta y$,so that $x^n + 1 \leftrightarrow (\zeta y)^n + 1 = -y^n + 1$
- The entire twisted FFT Trick: (ζ is an 2^{k-1}-th root of -1)

  $R[x]/\langle x^{2^k} - 1\rangle \cong R[x]/\langle x^{2^{k-1}} - 1\rangle \times R[x]/\langle x^{2^{k-1}} - 1\rangle\{\zeta\}$

  $\cong \prod^2 \left(R[x]/\langle x^{2^{k-2}} - 1\rangle \times R[x]/\langle x^{2^{k-2}} - 1\rangle\{\zeta^2\} \right)$

  $\cong \prod^4 \left(R[x]/\langle x^{2^{k-3}} - 1\rangle \times R[x]/\langle x^{2^{k-3}} - 1\rangle\{\zeta^4\} \right)$

Twisted FFT Trick

Compare to std. FFT: $R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$

- Base case of twisted FFT: (ζ is an n-th root of -1)

  $R[x]/\langle x^{2n} - 1\rangle \cong R[x]/\langle x^n - 1\rangle \times R[x]/\langle x^n + 1\rangle$ with the 2^{nd} component

  $R[x]/\langle x^n + 1\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta y$,so that $x^n + 1 \leftrightarrow (\zeta y)^n + 1 = -y^n + 1$

- The entire twisted FFT Trick: (ζ is an 2^{k-1}-th root of -1)

  $$R[x]/\langle x^{2^k} - 1\rangle \cong R[x]/\langle x^{2^{k-1}} - 1\rangle \times R[x]/\langle x^{2^{k-1}} - 1\rangle\{\zeta\}$$

  $$\cong \prod^2 \left(R[x]/\langle x^{2^{k-2}} - 1\rangle \times R[x]/\langle x^{2^{k-2}} - 1\rangle\{\zeta^2\} \right)$$

  $$\cong \prod^4 \left(R[x]/\langle x^{2^{k-3}} - 1\rangle \times R[x]/\langle x^{2^{k-3}} - 1\rangle\{\zeta^4\} \right)$$

  $$\cong \cdots \cong \prod^{2^k} R[x]/\langle x - 1\rangle \cong \prod^{2^k} R$$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n} - 1\rangle \cong R[x]/\langle x^n - 1\rangle \times R[x]/\langle x^n - 1\rangle$, and $\zeta^n = -1$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n} - 1\rangle \cong R[x]/\langle x^n - 1\rangle \times R[x]/\langle x^n - 1\rangle$, and $\zeta^n = -1$

$$\begin{matrix} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_n x^n+\cdots+a_{2n-1}x^{2n-1} \end{matrix} \longrightarrow \begin{bmatrix} (a_0+a_n)+(a_1+a_{n+1})+\cdots+(a_{n-1}+a_{2n-1})x^{n-1} \\ (a_0-a_n)+(a_1-a_{n+1})\zeta x+\cdots+(a_{n-1}-a_{2n-1})\zeta^{n-1}x^{n-1} \end{bmatrix}$$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n}-1\rangle \cong R[x]/\langle x^n-1\rangle \times R[x]/\langle x^n-1\rangle$, and $\zeta^n = -1$

$$\begin{matrix} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_n x^n+\cdots+a_{2n-1}x^{2n-1} \end{matrix} \longrightarrow \begin{bmatrix} (a_0+a_n)+(a_1+a_{n+1})+\cdots+(a_{n-1}+a_{2n-1})x^{n-1} \\ (a_0-a_n)+(a_1-a_{n+1})\zeta x+\cdots+(a_{n-1}-a_{2n-1})\zeta^{n-1}x^{n-1} \end{bmatrix}$$

$$\frac{1}{2}\begin{pmatrix} (b_0+c_0)+(b_1+c_1/\zeta)x+\cdots+(b_{n-1}+c_{n-1}/\zeta^{n-1})x^{n-1} \\ (b_0-c_0)+(b_1-c_1/\zeta)x+\cdots+(b_{n-1}-c_{n-1}/\zeta^{n-1})x^{n-1} \end{pmatrix} \longleftarrow \begin{bmatrix} b_0+b_1x+\cdots+b_{n-1}x^{n-1} \\ c_0+c_1x+\cdots+c_{n-1}x^{n-1} \end{bmatrix}$$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n}-1\rangle \cong R[x]/\langle x^n-1\rangle \times R[x]/\langle x^n-1\rangle$, and $\zeta^n=-1$

$$\begin{matrix} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_nx^n+\cdots+a_{2n-1}x^{2n-1} \end{matrix} \longrightarrow \begin{bmatrix} (a_0+a_n)+(a_1+a_{n+1})+\cdots+(a_{n-1}+a_{2n-1})x^{n-1} \\ (a_0-a_n)+(a_1-a_{n+1})\zeta x+\cdots+(a_{n-1}-a_{2n-1})\zeta^{n-1}x^{n-1} \end{bmatrix}$$

$$\frac{1}{2}\begin{pmatrix} (b_0+c_0)+(b_1+c_1/\zeta)x+\cdots+(b_{n-1}+c_{n-1}/\zeta^{n-1})x^{n-1} \\ (b_0-c_0)+(b_1-c_1/\zeta)x+\cdots+(b_{n-1}-c_{n-1}/\zeta^{n-1})x^{n-1} \end{pmatrix} \longleftarrow \begin{bmatrix} b_0+b_1x+\cdots+b_{n-1}x^{n-1} \\ c_0+c_1x+\cdots+c_{n-1}x^{n-1} \end{bmatrix}$$

- In $\mathbb{Z}_{17}[x]/\langle x^8-1\rangle$, note that $2^4=-1$

  $f(x)=1+2x+8x^2+2x^3+5x^4+6x^5+5x^6+x^7$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n}-1\rangle \cong R[x]/\langle x^n-1\rangle \times R[x]/\langle x^n-1\rangle$, and $\zeta^n=-1$

$$\begin{matrix} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_nx^n+\cdots+a_{2n-1}x^{2n-1} \end{matrix} \longrightarrow \begin{bmatrix} (a_0+a_n)+(a_1+a_{n+1})+\cdots+(a_{n-1}+a_{2n-1})x^{n-1} \\ (a_0-a_n)+(a_1-a_{n+1})\zeta x+\cdots+(a_{n-1}-a_{2n-1})\zeta^{n-1}x^{n-1} \end{bmatrix}$$

$$\frac{1}{2}\begin{pmatrix} (b_0+c_0)+(b_1+c_1/\zeta)x+\cdots+(b_{n-1}+c_{n-1}/\zeta^{n-1})x^{n-1} \\ (b_0-c_0)+(b_1-c_1/\zeta)x+\cdots+(b_{n-1}-c_{n-1}/\zeta^{n-1})x^{n-1} \end{pmatrix} \longleftarrow \begin{bmatrix} b_0+b_1x+\cdots+b_{n-1}x^{n-1} \\ c_0+c_1x+\cdots+c_{n-1}x^{n-1} \end{bmatrix}$$

- In $\mathbb{Z}_{17}[x]/\langle x^8-1\rangle$, note that $2^4=-1$

$$f(x) = 1+2x+8x^2+2x^3+5x^4+6x^5+5x^6+x^7$$

$$\xrightarrow{\sqrt[4]{-1}=2} (6+8x+13x^2+3x^3, \quad -4-8x+12x^2+8x^3)$$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n}-1\rangle \cong R[x]/\langle x^n-1\rangle \times R[x]/\langle x^n-1\rangle$, and $\zeta^n=-1$

$$\begin{matrix} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_nx^n+\cdots+a_{2n-1}x^{2n-1}\end{matrix} \longrightarrow \begin{bmatrix} (a_0+a_n)+(a_1+a_{n+1})+\cdots+(a_{n-1}+a_{2n-1})x^{n-1} \\ (a_0-a_n)+(a_1-a_{n+1})\zeta x+\cdots+(a_{n-1}-a_{2n-1})\zeta^{n-1}x^{n-1}\end{bmatrix}$$

$$\frac{1}{2}\begin{pmatrix} (b_0+c_0)+(b_1+c_1/\zeta)x+\cdots+(b_{n-1}+c_{n-1}/\zeta^{n-1})x^{n-1} \\ (b_0-c_0)+(b_1-c_1/\zeta)x+\cdots+(b_{n-1}-c_{n-1}/\zeta^{n-1})x^{n-1}\end{pmatrix} \longleftarrow \begin{bmatrix} b_0+b_1x+\cdots+b_{n-1}x^{n-1} \\ c_0+c_1x+\cdots+c_{n-1}x^{n-1}\end{bmatrix}$$

- In $\mathbb{Z}_{17}[x]/\langle x^8-1\rangle$, note that $2^4=-1$

$$f(x)=1+2x+8x^2+2x^3+5x^4+6x^5+5x^6+x^7$$

$$\xrightarrow{\sqrt[4]{-1}=2} (6+8x+13x^2+3x^3,\quad -4-8x+12x^2+8x^3)$$

$$\xrightarrow{\sqrt[2]{-1}=4} (19+11x, -7+20x,\quad 8, -16-64x)$$

Twisted FFT Trick: Example

- $R[x]/\langle x^{2n}-1\rangle \cong R[x]/\langle x^n-1\rangle \times R[x]/\langle x^n-1\rangle$, and $\zeta^n=-1$

$$\begin{array}{c} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_nx^n+\cdots+a_{2n-1}x^{2n-1}\end{array} \longrightarrow \begin{bmatrix} (a_0+a_n)+(a_1+a_{n+1})+\cdots+(a_{n-1}+a_{2n-1})x^{n-1} \\ (a_0-a_n)+(a_1-a_{n+1})\zeta x+\cdots+(a_{n-1}-a_{2n-1})\zeta^{n-1}x^{n-1}\end{bmatrix}$$

$$\frac{1}{2}\begin{pmatrix} (b_0+c_0)+(b_1+c_1/\zeta)x+\cdots+(b_{n-1}+c_{n-1}/\zeta^{n-1})x^{n-1} \\ (b_0-c_0)+(b_1-c_1/\zeta)x+\cdots+(b_{n-1}-c_{n-1}/\zeta^{n-1})x^{n-1}\end{pmatrix} \longleftarrow \begin{bmatrix} b_0+b_1x+\cdots+b_{n-1}x^{n-1} \\ c_0+c_1x+\cdots+c_{n-1}x^{n-1}\end{bmatrix}$$

- In $\mathbb{Z}_{17}[x]/\langle x^8-1\rangle$, note that $2^4=-1$

$$f(x)=1+2x+8x^2+2x^3+5x^4+6x^5+5x^6+x^7$$

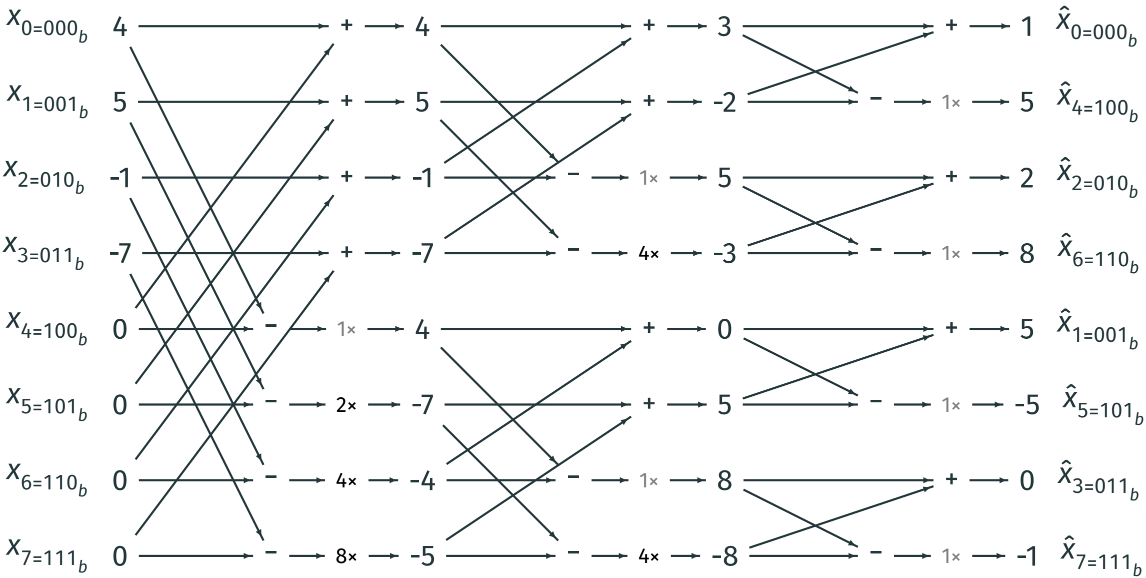
$$\xrightarrow{\sqrt[4]{-1}=2} (6+8x+13x^2+3x^3, \quad -4-8x+12x^2+8x^3)$$

$$\xrightarrow{\sqrt[2]{-1}=4} (19+11x, -7+20x, \quad 8, -16-64x)$$

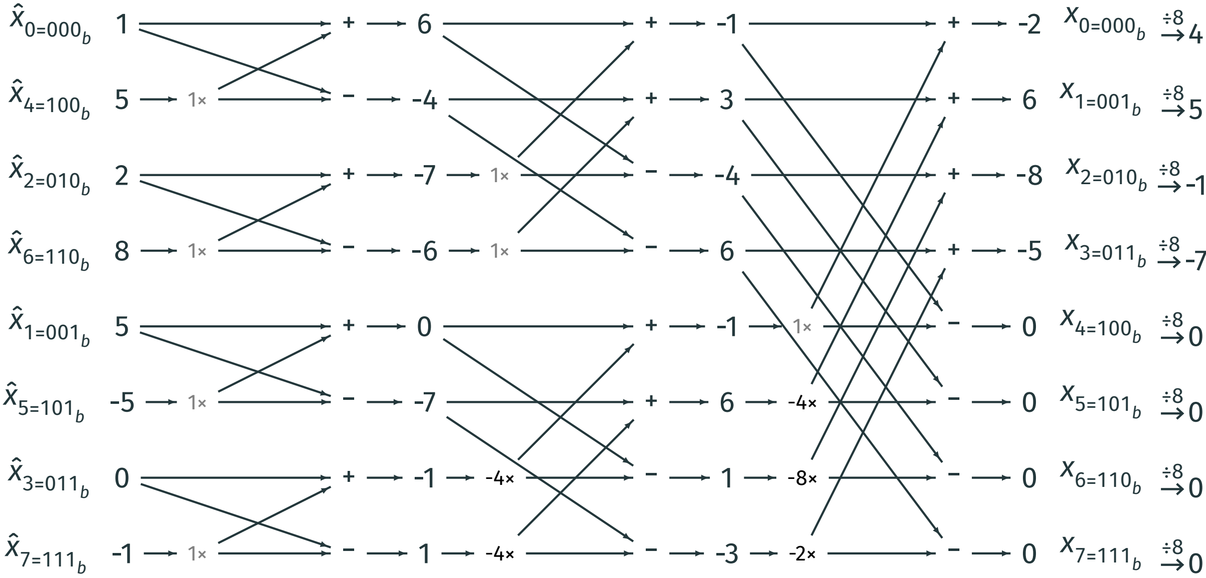
$$\xrightarrow{\sqrt[1]{-1}=-1} (30, 8, 13, -27, 8, 8, -80, 48)$$

Twisted FFT(NTT) uses the Gentleman-Sande butterflies.

Twisted FFT/NTT Example ($\mathbb{F}_{17}[x]/(x^8-1), \zeta = 2$)



Twisted FFT/NTT Example ($\mathbb{F}_{17}[x]/(x^8 - 1), \zeta = 2$) ii



Radix-3 FFT

- Base case of the usual FFT: (there exists some 2-power-th root of $\omega = -1$)
  $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$

Radix-3 FFT

- Base case of the usual FFT: (there exists some 2-power-th root of $\omega = -1$)
  $R[x]/\langle x^{2n} - c^2 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n + c \rangle$
- Base case of radix-3 FFT: (there exists some 3-power-th root of $\omega = \sqrt[3]{1}$)
  $R[x]/\langle x^{3n} - c^3 \rangle \cong R[x]/\langle x^n - c \rangle \times R[x]/\langle x^n - \omega c \rangle \times R[x]/\langle x^n - \omega^2 c \rangle$

Radix-3 FFT

- Base case of the usual FFT: (there exists some 2-power-th root of $\omega = -1$)

  $R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$
- Base case of radix-3 FFT: (there exists some 3-power-th root of $\omega = \sqrt[3]{1}$)

  $R[x]/\langle x^{3n} - c^3\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n - \omega c\rangle \times R[x]/\langle x^n - \omega^2 c\rangle$
- $$\begin{matrix} a_0 + \cdots + a_{n-1}x^{n-1} \\ +a_n x^n + \cdots + a_{2n-1}x^{2n-1} \\ +a_{2n}x^{2n} + \cdots + a_{3n-1}x^{3n-1} \end{matrix} \longrightarrow \begin{bmatrix} (a_0 + a_n c + a_{2n}c^2) + \cdots + (a_{n-1} + a_{2n-1}c + a_{3n-1}c^2)x^{n-1} \\ (a_0 + a_n \omega c + a_{2n}\omega^2 c^2) + \cdots + (a_{n-1} + a_{2n-1}\omega c + a_{3n-1}\omega^2 c^2)x^{n-1} \\ (a_0 + a_n \omega^2 c + a_{2n}\omega c^2) + \cdots + (a_{n-1} + a_{2n-1}\omega^2 c + a_{3n-1}\omega c^2)x^{n-1} \end{bmatrix}$$

Radix-3 FFT

- Base case of the usual FFT: (there exists some 2-power-th root of $\omega = -1$)

$$R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$$

- Base case of radix-3 FFT: (there exists some 3-power-th root of $\omega = \sqrt[3]{1}$)

$$R[x]/\langle x^{3n} - c^3\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n - \omega c\rangle \times R[x]/\langle x^n - \omega^2 c\rangle$$

- $$\begin{matrix} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_n x^n+\cdots+a_{2n-1}x^{2n-1} \\ +a_{2n}x^{2n}+\cdots+a_{3n-1}x^{3n-1} \end{matrix} \longrightarrow \begin{bmatrix} (a_0+a_n c+a_{2n}c^2)+\cdots+(a_{n-1}+a_{2n-1}c+a_{3n-1}c^2)x^{n-1} \\ (a_0+a_n\omega c+a_{2n}\omega^2c^2)+\cdots+(a_{n-1}+a_{2n-1}\omega c+a_{3n-1}\omega^2c^2)x^{n-1} \\ (a_0+a_n\omega^2c+a_{2n}\omega c^2)+\cdots+(a_{n-1}+a_{2n-1}\omega^2c+a_{3n-1}\omega c^2)x^{n-1} \end{bmatrix}$$

- $$\begin{matrix} f(x)\cdot\frac{1}{3c^2}(x^{2n}+cx^n+c^2) \\ +g(x)\cdot\frac{1}{3\omega^2c^2}(x^{2n}+\omega cx^n+\omega^2c^2) \\ +h(x)\cdot\frac{1}{3\omega c^2}(x^{2n}+\omega^2cx^n+\omega c^2) \end{matrix} = \begin{matrix} \frac{1}{3}(f(x)+g(x)+h(x)) \\ +\frac{1}{3c}(f(x)+\omega^2g(x)+\omega h(x))x^n \\ +\frac{1}{3c^2}(f(x)+\omega g(x)+\omega^2h(x))x^{2n} \end{matrix} \longleftarrow \begin{bmatrix} f(x) \\ g(x) \\ h(x) \end{bmatrix}$$

Radix-3 FFT

- Base case of the usual FFT: (there exists some 2-power-th root of $\omega = -1$)
  $R[x]/\langle x^{2n} - c^2\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n + c\rangle$
- Base case of radix-3 FFT: (there exists some 3-power-th root of $\omega = \sqrt[3]{1}$)
  $R[x]/\langle x^{3n} - c^3\rangle \cong R[x]/\langle x^n - c\rangle \times R[x]/\langle x^n - \omega c\rangle \times R[x]/\langle x^n - \omega^2 c\rangle$
- $$\begin{array}{c} a_0+\cdots+a_{n-1}x^{n-1} \\ +a_n x^n+\cdots+a_{2n-1}x^{2n-1} \\ +a_{2n}x^{2n}+\cdots+a_{3n-1}x^{3n-1} \end{array} \longrightarrow \begin{bmatrix} (a_0+a_n c+a_{2n}c^2)+\cdots+(a_{n-1}+a_{2n-1}c+a_{3n-1}c^2)x^{n-1} \\ (a_0+a_n\omega c+a_{2n}\omega^2c^2)+\cdots+(a_{n-1}+a_{2n-1}\omega c+a_{3n-1}\omega^2c^2)x^{n-1} \\ (a_0+a_n\omega^2 c+a_{2n}\omega c^2)+\cdots+(a_{n-1}+a_{2n-1}\omega^2 c+a_{3n-1}\omega c^2)x^{n-1} \end{bmatrix}$$
- $$\begin{array}{l} f(x)\cdot\frac{1}{3c^2}(x^{2n}+cx^n+c^2) \\ +g(x)\cdot\frac{1}{3\omega^2c^2}(x^{2n}+\omega cx^n+\omega^2c^2) \\ +h(x)\cdot\frac{1}{3\omega c^2}(x^{2n}+\omega^2cx^n+\omega c^2) \end{array} = \begin{array}{l} \frac{1}{3}(f(x)+g(x)+h(x)) \\ +\frac{1}{3c}(f(x)+\omega^2g(x)+\omega h(x))x^n \\ +\frac{1}{3c^2}(f(x)+\omega g(x)+\omega^2h(x))x^{2n} \end{array} \longleftarrow \begin{bmatrix} f(x) \\ g(x) \\ h(x) \end{bmatrix}$$
- $4n$ additions, $4n$ subtractions and $4n$ muls/divs by c, c^2, ω or ω^2

Radix-3 FFT: Example

- We can choose to start with $R[x]/\langle x^{2\cdot 3^k} + x^{3^k} + 1\rangle$ instead of $R[x]/\langle x^{3^{k+1}} - 1\rangle$

Radix-3 FFT: Example

- We can choose to start with $R[x]/\langle x^{2\cdot 3^k} + x^{3^k} + 1\rangle$ instead of $R[x]/\langle x^{3^{k+1}} - 1\rangle$
- Let's start with $\mathbb{Z}_{19}[x]\langle x^6 + x^3 + 1\rangle$

Radix-3 FFT: Example

- We can choose to start with $R[x]/\langle x^{2\cdot 3^k} + x^{3^k} + 1\rangle$ instead of $R[x]/\langle x^{3^{k+1}} - 1\rangle$
- Let's start with $\mathbb{Z}_{19}[x]\langle x^6 + x^3 + 1\rangle$
- Note that 4 is a 9-th root of 1, and 7, 11 are 3-rd roots of 1 in $\mathbb{Z}_{19}$

Radix-3 FFT: Example

- We can choose to start with $R[x]/\langle x^{2\cdot 3^k} + x^{3^k} + 1\rangle$ instead of $R[x]/\langle x^{3^{k+1}} - 1\rangle$
- Let's start with $\mathbb{Z}_{19}[x]\langle x^6 + x^3 + 1\rangle$
- Note that 4 is a 9-th root of 1, and 7, 11 are 3-rd roots of 1 in $\mathbb{Z}_{19}$
- $$\begin{aligned} x^6 + x^3 + 1 &= (x^3 - 7)(x^3 - 11) \\ &= (x - 4)(x - 7 * 4)(x - 11 * 4)(x - 16)(x - 7 * 16)(x - 11 * 16) \\ &= (x - 4)(x - 9)(x - 6)(x + 3)(x + 2)(x - 5) \end{aligned}$$

Radix-3 FFT: Example

- We can choose to start with $R[x]/\langle x^{2\cdot 3^k} + x^{3^k} + 1\rangle$ instead of $R[x]/\langle x^{3^{k+1}} - 1\rangle$
- Let's start with $\mathbb{Z}_{19}[x]\langle x^6 + x^3 + 1\rangle$
- Note that 4 is a 9-th root of 1, and 7, 11 are 3-rd roots of 1 in $\mathbb{Z}_{19}$
- $$\begin{aligned} x^6 + x^3 + 1 &= (x^3 - 7)(x^3 - 11) \\ &= (x - 4)(x - 7 * 4)(x - 11 * 4)(x - 16)(x - 7 * 16)(x - 11 * 16) \\ &= (x - 4)(x - 9)(x - 6)(x + 3)(x + 2)(x - 5) \end{aligned}$$
- $f(x) = -1 - 2x - 3x^2 + x^3 + 2x^4 + 3x^5$

  $\rightarrow (6 + 12x + 18x^2, \quad 10 + 20x + 30x^2)$

  $\rightarrow (0, 14, 4, 11, 14, 5)$

Radix-3 FFT: Example

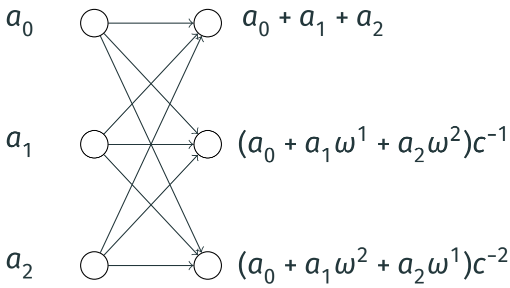
- We can choose to start with $R[x]/\langle x^{2\cdot 3^k} + x^{3^k} + 1\rangle$ instead of $R[x]/\langle x^{3^{k+1}} - 1\rangle$
- Let's start with $\mathbb{Z}_{19}[x]\langle x^6 + x^3 + 1\rangle$
- Note that 4 is a 9-th root of 1, and 7, 11 are 3-rd roots of 1 in $\mathbb{Z}_{19}$
- $$\begin{aligned} x^6 + x^3 + 1 &= (x^3 - 7)(x^3 - 11) \\ &= (x - 4)(x - 7 * 4)(x - 11 * 4)(x - 16)(x - 7 * 16)(x - 11 * 16) \\ &= (x - 4)(x - 9)(x - 6)(x + 3)(x + 2)(x - 5) \end{aligned}$$
- $f(x) = -1 - 2x - 3x^2 + x^3 + 2x^4 + 3x^5$

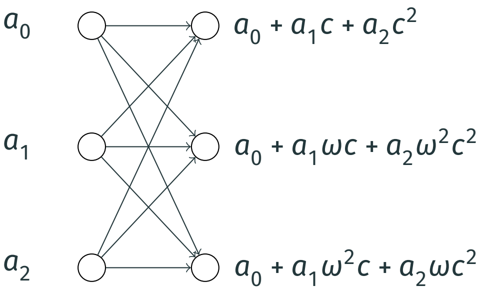
  $\rightarrow (6 + 12x + 18x^2, \quad 10 + 20x + 30x^2)$

  $\rightarrow (0, 14, 4, 11, 14, 5)$
- We can see that inversion formula also applies

Radix-3 and Higher Butterflies

Radix-3 butterfly diagrams for Gentleman-Sande (L) and Cooley-Tukey (R).





One can see from the above that C-T butterflies for higher sizes uses more multiplicands $(c, c^2, \omega c, \omega^2 c^2, \omega^2 c, \omega c^2)$ than G-S butterflies $(\omega, \omega^2, c^{-1}, c^{-2})$.

Incomplete NTT

- Standard NTT means “completely splitting”: factors down to linear factors.

Incomplete NTT

- Standard NTT means “completely splitting”: factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q - 1)$-cyclic group.

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q - 1)$-cyclic group.
  - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q - 1)$.

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
    - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
    - Galois: non-zero elements of a field F of size q form a $(q-1)$-cyclic group.
    - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q-1)$.
- Sometimes the ring polynomial is a cyclotomic polynomial $\Phi_n(x)$, which is defined as a monic polynomial dividing $x^n - 1$ but not any $x^m - 1$ with $m < n$. Galois theory: $\Phi_n(x)$ splits completely iff $x^n - 1$ splits completely, examples:

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q - 1)$-cyclic group.
  - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q - 1)$.
- Sometimes the ring polynomial is a cyclotomic polynomial $\Phi_n(x)$, which is defined as a monic polynomial dividing $x^n - 1$ but not any $x^m - 1$ with $m < n$. Galois theory: $\Phi_n(x)$ splits completely iff $x^n - 1$ splits completely, examples:
  - NewHope with $\mathbb{F}_{12289}[x]/(x^{1024} + 1)$, where the ring polynomial is $\Phi_{2048}(x)$.

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q-1)$-cyclic group.
  - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q-1)$.
- Sometimes the ring polynomial is a cyclotomic polynomial $\Phi_n(x)$, which is defined as a monic polynomial dividing $x^n - 1$ but not any $x^m - 1$ with $m < n$. Galois theory: $\Phi_n(x)$ splits completely iff $x^n - 1$ splits completely, examples:
  - NewHope with $\mathbb{F}_{12289}[x]/(x^{1024} + 1)$, where the ring polynomial is $\Phi_{2048}(x)$.
  - Dilithium with $\mathbb{F}_{2^{23}-2^{13}+1}/(x^{256} + 1)$, where the ring polynomial is $\Phi_{512}(x)$.

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q-1)$-cyclic group.
  - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q-1)$.
- Sometimes the ring polynomial is a cyclotomic polynomial $\Phi_n(x)$, which is defined as a monic polynomial dividing $x^n - 1$ but not any $x^m - 1$ with $m < n$. Galois theory: $\Phi_n(x)$ splits completely iff $x^n - 1$ splits completely, examples:
  - NewHope with $\mathbb{F}_{12289}[x]/(x^{1024} + 1)$, where the ring polynomial is $\Phi_{2048}(x)$.
  - Dilithium with $\mathbb{F}_{2^{23}-2^{13}+1}/(x^{256} + 1)$, where the ring polynomial is $\Phi_{512}(x)$.
- Sometimes the ring polynomial doesn't split down to linear factors, viz.:

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q - 1)$-cyclic group.
  - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q - 1)$.
- Sometimes the ring polynomial is a cyclotomic polynomial $\Phi_n(x)$, which is defined as a monic polynomial dividing $x^n - 1$ but not any $x^m - 1$ with $m < n$. Galois theory: $\Phi_n(x)$ splits completely iff $x^n - 1$ splits completely, examples:
  - NewHope with $\mathbb{F}_{12289}[x]/(x^{1024} + 1)$, where the ring polynomial is $\Phi_{2048}(x)$.
  - Dilithium with $\mathbb{F}_{2^{23}-2^{13}+1}/(x^{256} + 1)$, where the ring polynomial is $\Phi_{512}(x)$.
- Sometimes the ring polynomial doesn't split down to linear factors, viz.:
  - Kyber with $\mathbb{F}_{3329}[x]/(\Phi_{512}(x) = x^{256} + 1)$. $256 | 3328$, but $512 \nmid 3328$.

Incomplete NTT

- Standard NTT means "completely splitting": factors down to linear factors.
  - If the ring polynomial is $x^{2^k} - 1$, requires a primitive 2^k-th root of unity.
  - Galois: non-zero elements of a field F of size q form a $(q-1)$-cyclic group.
  - Therefore, there is a primitive 2^k-th root of unity if (and only if) $2^k | (q-1)$.
- Sometimes the ring polynomial is a cyclotomic polynomial $\Phi_n(x)$, which is defined as a monic polynomial dividing $x^n - 1$ but not any $x^m - 1$ with $m < n$. Galois theory: $\Phi_n(x)$ splits completely iff $x^n - 1$ splits completely, examples:
  - NewHope with $\mathbb{F}_{12289}[x]/(x^{1024}+1)$, where the ring polynomial is $\Phi_{2048}(x)$.
  - Dilithium with $\mathbb{F}_{2^{23}-2^{13}+1}/(x^{256}+1)$, where the ring polynomial is $\Phi_{512}(x)$.
- Sometimes the ring polynomial doesn't split down to linear factors, viz.:
  - Kyber with $\mathbb{F}_{3329}[x]/(\Phi_{512}(x) = x^{256}+1)$. $256 | 3328$, but $512 \nmid 3328$.
  - NTTRU with $\mathbb{F}_{7681}[x]/(\Phi_{2304}(x) = x^{768} - x^{384} + 1)$, $768 | 7680$, but $2304 \nmid 7680$.

Incomplete Splitting and why it is Good

- So ring polynomials splits down to low-degree but not linear:
  - Round 2 Kyber splits to (ω_{256} is the primitive 256th root of 1): $\bigoplus_{j=0}^{128} \frac{\mathbf{F}_{3329}[x]}{(x^2 - \omega_{256}^{2j+1})}$
  - NTTRU splits to $\bigoplus_{j=0}^{128} \frac{\mathbf{F}_{7681}[x]}{(x^3 - \beta_j)} \oplus \bigoplus_{j=0}^{128} \frac{\mathbf{F}_{7681}[x]}{(x^3 - \beta_j')}$, where the β_j' and β_j are the 128-th roots of −684 and 685, the primitive 6-th roots of unity $\pmod{7681}$.
- $(a + bx)(c + dx) \equiv (ac + bd\omega_j) + (ad + bc)x \pmod{x^2 - \omega_j}$ = 5 muls, 2 adds. An 2-FFT is 1 mul, 2 adds, so 2× 2-FFT's a 2-iFFT, 2× basemul = 5 muls (+ 6 adds).
- Computing $(a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2) \pmod{x^2 - \omega_j}$ by schoolbook as $(a_0b_0 + \omega_j(a_1b_2 + a_2b_1)) + (a_0b_1 + a_1b_0 + \omega_ja_2b_2)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2$ takes 11 muls (+ 6 adds). Each 3-FFT takes 2 muls (+ 8 adds).

Good's Trick i

Good proposed a method to perform a size-$(p_0 \cdot p_1)$ NTT as a combination of p_0 size-p_1 NTT's where p_0 and p_1 are coprime numbers. This technique maps polynomial multiplication in $\mathbb{F}_q[x]/(x^{p_0 \cdot p_1} - 1)$ into its isomorphic ring $\mathbb{F}_q[y]/(y^{p_0} - 1)[z]/(z^{p_1} - 1)$ where $x = yz$. This might require a permutation of the coefficients of the input polynomial.

Advantages of Good's Trick
We can do a y-FFT and a z-FFT independently. In particular, both these FFTs are in a ring modulo $y^{p_0} - 1$ and $z^{p_1} - 1$, making things simpler and more repetitive.

Good's Trick ii

Using the fact that p_0 and p_1 are relatively prime, the index calculation

$$i = ((p_1)^{-1} \bmod p_0) \cdot p_1 \cdot i_0 + ((p_0)^{-1} \bmod p_1) \cdot p_0 \cdot i_1$$

applies the CRT to obtain $x^i = y^{i_0} z^{i_1}$. As an example, the permutations of the indices for an input of size 6 and 12 is given in a table.

Good's Trick iii

i	0	1	2	3	4	5
i_0	0	1	2	0	1	2
i_1	0	1	0	1	0	1
$\hat{i}$	0	4	2	3	1	5
$\tilde{i}$	0	3	4	1	2	5

Good's Trick iv

i	0	1	2	3	4	5	6	7	8	9	10	11
i_0	0	1	2	0	1	2	0	1	2	0	1	2
i_1	0	1	2	3	0	1	2	3	0	1	2	3
$\hat{i}$	0	4	8	9	1	5	6	10	2	3	7	11
$\tilde{i}$	0	9	6	3	4	1	10	7	8	5	2	11

Table 1: Good's permutations for size 6 = 3 × 2 and 12 = 3 × 4.

Good's Trick v

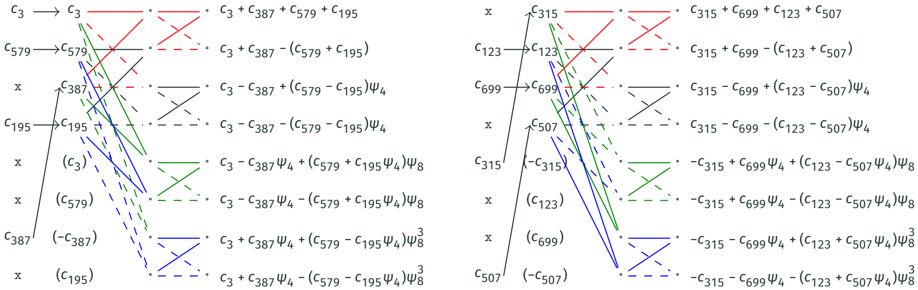
Using the above permutation after zero-padding of a polynomial of degree 5, the two-dimensional polynomial representation is

$$a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = (a_5z + a_2)y^2 + (a_1z + a_4)y + (a_3z + a_0).$$

Good's Trick vi

We can frequently permute on the fly, operate the NTT, and redeposit the entries in the correct locations. Below is Good's permutation combined with the first 3 rounds of a size 1536-NTT, with the first 761 coefficients in the polynomial nonzero:

Good's Trick vii

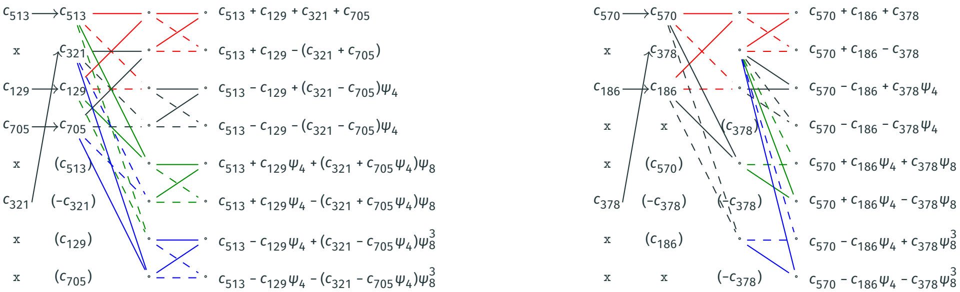


(a) Case with 4 zeros (I).

(b) Case with 4 zeros (II).

Figure 2: Goods permutation plus the initial rounds (I).

Good's Trick viii



(a) Case with 4 zeros (III).

(b) Case with 5 zeros.

Figure 3: Goods permutation plus the initial rounds (II).

Good's Trick ix

Note that where a set of coefficients go depends on the remainder mod3 of the lead location, plus there are residual cases where there are extra 0's. Good's Trick often increases code size; and need a code generator to make it less painful.

Good's Trick x

Using the Good's Trick on a 1536-NTT

1. apply Good's permutation to both multiplicands ($\to F[y,z]/(y^3-1, z^{512}-1)$))
2. do 512-NTT for per y^i-coefficient per multiplicand $\to \bigoplus_{i=0}^{511}\left(\frac{F[y][z]}{(y^3-1, z-\zeta_i)}\right)$
3. do "base multiplications" (each a schoolbook 3-convolution)
4. invert 512-NTTs per y^i-coefficient (back to $F[y,z]/(y^3-1, z^{512}-1)$))
5. reverse the Good's permutation

Notes, Steps 1 and 5 are frequently merged, and schoolbook 3-convolution (9 muls) no slower than via 3-NTTs. As described, this *doesn't need a 3rd root of unity*.

Incomplete Good's FFT Trick

Many Combinations to Try

We can combine Good's Trick with the Incomplete NTT. For example

$$\frac{\mathbb{F}_{769}[x]}{(x^{768}-1)} \to \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{64}-1)} \to \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{32}-1)} \oplus \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{32}+1)}$$

$$\to \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{16}-1)} \oplus \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{16}+1)} \oplus \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{16}-i)} \oplus \frac{\mathbb{F}_{769}[x,y,z]}{(x^4-yz,y^3-1,z^{16}+i)}$$

$$\to \cdots \to \bigoplus_{j=0}^{63} \frac{\mathbb{F}_{769}[x,y,z]}{\left(x^4-yz,y^3-1,z-\omega_{64}^{\mathrm{brv}(j)}\right)}$$

$$\to \bigoplus_{j=0}^{63} \frac{\mathbb{F}_{769}[x,y,z]}{\left(x^4-yz,y-1,z-\omega_{64}^{\mathrm{brv}(j)}\right)} \oplus \bigoplus_{j=0}^{63} \frac{\mathbb{F}_{769}[x,y,z]}{\left(x^4-yz,y-\omega_3,z-\omega_{64}^{\mathrm{brv}(j)}\right)} \oplus \bigoplus_{j=0}^{63} \frac{\mathbb{F}_{769}[x,y,z]}{\left(x^4-yz,y-\omega_3^2,z-\omega_{64}^{\mathrm{brv}(j)}\right)}$$

$$\to \bigoplus_{j=0}^{63} \bigoplus_{k=0}^{2} \frac{\mathbb{F}_{769}[x,y,z]}{\left(x^4-\omega_3^k\omega_{64}^{\mathrm{brv}(j)},y-\omega_3^k,z-\omega_{64}^{\mathrm{brv}(j)}\right)}$$

3-NTT on y, an incomplete 256-NTT on z, leaving 192 cubics in x.

Bruun's FFT/NTT: The factorization

The prototype of Bruun's FFT is this factorization

$$(x^4 + x^2 + 1) = (x^2 + x + 1)(x^2 - x + 1)$$

In general

$$(x^{2n} + ax^n + b^2) = \left(x^n + \sqrt{-a+2b}\,x^{n/2} + b\right)\left(x^n - \sqrt{-a+2b}\,x^{n/2} + b\right)$$

If prime $q = 4n + 3$, and $q^2 - 1 = 2^w \cdot (\text{odd number})$, then if $k < w$, then $x^{2^k} + 1$ factors into irreducible trinomials $x^2 + \gamma x + 1$ in $\mathbb{F}_q[x]$. On the other hand, if $k \geq w$, then $x^{2^k} + 1$ factors into irreducible trinomials $x^{2^{k-w+1}} + \gamma x^{2^{k-w}} - 1$ in $\mathbb{F}_q[x]$.

Bruun's FFT/NTT: radix-2 Bruun's butterflies. i

Define $Bruun_{\alpha,\beta}$: $\begin{cases} \frac{R[x]}{\langle x^4+(2\beta-\alpha^2)x^2+\beta^2\rangle} & \to \frac{R[x]}{\langle x^2+\alpha x+\beta\rangle} \times \frac{R[x]}{\langle x^2-\alpha x+\beta\rangle} \\ a_0 + a_1 x + a_2 x^2 + a_3 x^3 & \mapsto \left((\hat{a}_0 + \hat{a}_1 x), (\hat{a}_2 + \hat{a}_3 x)\right) \end{cases}$

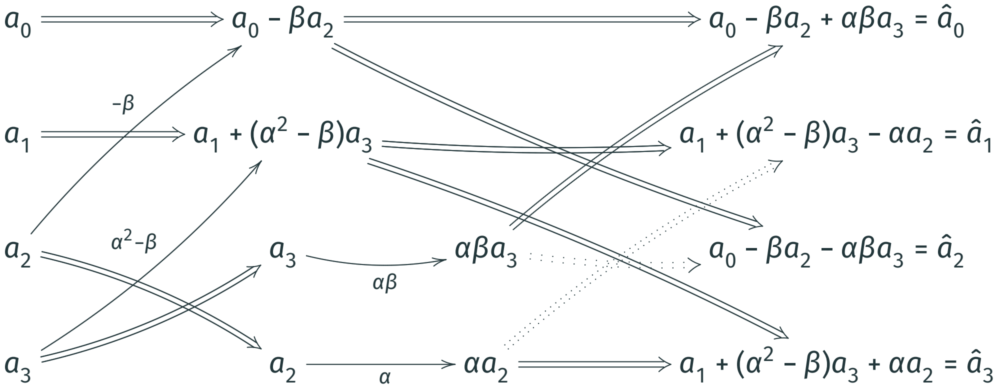
where

$$\begin{cases} (\hat{a}_0, \hat{a}_1) = & \left(a_0 - \beta a_2 + \alpha\beta a_3, a_1 + (\alpha^2 - \beta)a_3 - \alpha a_2\right), \\ (\hat{a}_2, \hat{a}_3) = & \left(a_0 - \beta a_2 - \alpha\beta a_3, a_1 + (\alpha^2 - \beta)a_3 + \alpha a_2\right). \end{cases}$$

We compute $\left(\hat{a}_0 + \hat{a}_2, \hat{a}_1 + \hat{a}_3, \hat{a}_0 - \hat{a}_2, \hat{a}_3 - \hat{a}_1\right)$, swap the last two values implicitly, multiply the constants $\alpha^{-1}, \beta^{-1}, \alpha^{-1}\beta^{-1}$, and $\left(\alpha^2 - \beta\right)^{-1}$, and perform add/subs.

Bruun's FFT/NTT: radix-2 Bruun's butterflies. ii

Double lines are simple adds (×1) and double dotted lines subtracts (×(−1)).



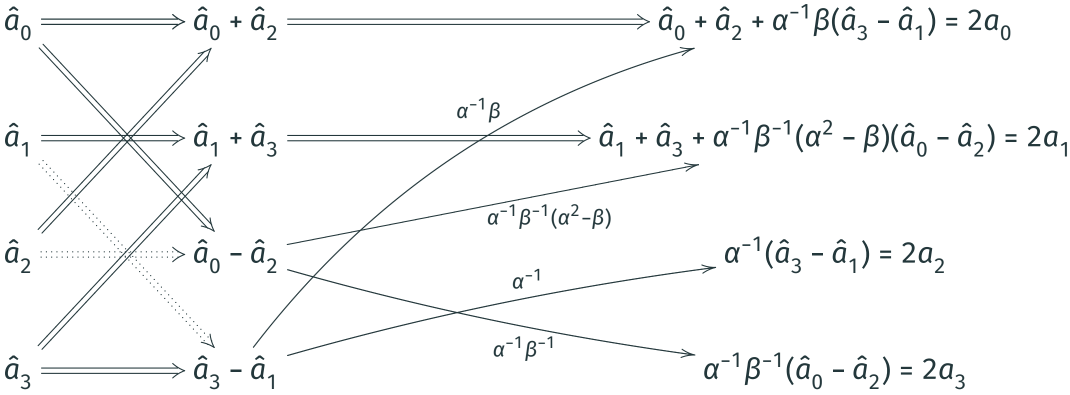
Bruun's FFT/NTT: radix-2 Bruun's butterflies. iii

Define $2Bruun^{-1}_{\alpha,\beta}$: $\begin{cases} \frac{R[x]}{\langle x^2+\alpha x+\beta\rangle} \times \frac{R[x]}{\langle x^2-\alpha x+\beta\rangle} & \to \frac{R[x]}{\langle x^4+(2\beta-\alpha^2)x^2+\beta^2\rangle} \\ \left((\hat{a}_0 + \hat{a}_1 x), (\hat{a}_2 + \hat{a}_3 x)\right) & \mapsto 2a_0 + 2a_1 x + 2a_2 x^2 + 2a_3 x^3 \end{cases}$

where this inverse maps $\begin{cases} 2a_0 = & \hat{a}_0 + \hat{a}_2 + \left(\hat{a}_3 - \hat{a}_1\right)\alpha^{-1}\beta^{-1}, \\ 2a_1 = & \hat{a}_1 + \hat{a}_3 - \left(\hat{a}_0 - \hat{a}_2\right)\alpha^{-1}\beta^{-1}\left(\alpha^2 - \beta\right), \\ 2a_2 = & \left(\hat{a}_3 - \hat{a}_1\right)\alpha^{-1}, \\ 2a_3 = & \left(\hat{a}_0 - \hat{a}_2\right)\alpha^{-1}\beta^{-1}. \end{cases}$

Compute $(a_0 - \beta a_2, a_1 + (\alpha^2 - \beta)a_3, \alpha a_2, \alpha\beta a_3)$, implicitly swap then add/sub.

Bruun's FFT/NTT: radix-2 Bruun's butterflies. iv



both $Bruun_{\alpha,\beta}$ and $2Bruun^{-1}_{\alpha,\beta}$, need 4 mults and 6 add/subs (3 if $\beta = 1$).

Truncated FFT, Alternative to Good's

Using Good's trick relies on having the right Principal Roots. When using Schönhage or Nussbaumer, you usually don't have these roots. A variation is to use the Truncated FFT Trick. Example: Instead of using $R[x]/(x^{1536} - 1)$, use $R[x]/\left((x^{1024}+1)(x^{512} \pm 1)\right)$

If $f(x) \bmod (x^{1024}+1) = f_0(x)$, $f(x) \bmod (x^{512}-1) = f_1(x)$, then we have

$$f(x) \equiv -\frac{x^{1024}-1}{2} f_0(x) + \frac{x^{1024}+1}{2} f_1(x) \bmod \left((x^{1024}+1)(x^{512}-1)\right)$$

Or rather

$$(a_0, a_1, \dots, a_{1023}), (b_0, b_1, \dots, b_{511}) \mapsto \Big(\tfrac{b_0+a_0-a_{512}}{2}, \tfrac{b_1+a_1-a_{513}}{2}, \dots, \tfrac{b_{511}+a_{511}-a_{1023}}{2}, a_{512}, a_{513}, \dots, a_{1023}, \tfrac{b_0-a_0-a_{512}}{2}, \tfrac{b_1-a_1-a_{513}}{2}, \dots, \tfrac{b_{511}-a_{511}-a_{1023}}{2}\Big).$$

Rader's Trick i

For any prime number p such that the p th-root of unity ψ exists, Rader's trick can map $Z_q[x]/(x^p - 1)$ to $(Z_q[x]/(x - 1)) \times \dots Z_q[x]/(x - \psi^{p-1})$.

Let $f = \sum_{i=0}^{p-1} f_i x^i$ be a polynomial in ring $Z_q[x]/(x^p - 1)$. The discrete Fourier transform (DFT) of f is

$$F_k = \sum_{i=0}^{p-1} f_i \psi^{ik}, k \in \{0, \dots, p - 1\}.$$

Rader's Trick ii

We only need to use additions to compute the F_0; we also can add f_0 separately later. The summation which we want to compute turns into

$$\hat{F}_k = F_k - f_0 = \sum_{i=1}^{p-1} f_i \psi^{ik}, k \in \{1, \dots, p-1\}.$$

There exists a primitive root of p which we call g because p is a prime number. Define (i.e., take discrete logs) new indices $\hat{\imath}$ and $\hat{\jmath}$:

$$i = g^{\hat{\imath}} \pmod{p}, \hat{\imath} \in \{1, \dots, p-1\} \quad \text{and} \quad j = g^{p-\hat{\jmath}} \pmod{p}, \hat{\jmath} \in \{1, \dots, p-1\}.$$

Rader's Trick iii

The summation above becomes $\hat{F}_{g^{p-\hat{j}}} = \sum_{\hat{i}=1}^{p-1} f_{g^{\hat{i}}} \psi^{g^{p-(\hat{j}-\hat{i})}}$. Define new sequences a_n, b_n:

$$a_n = f_{g^n}, b_n = \psi^{g^{p-n}}, n \in \{1, \ldots, p-1\}.$$

The cyclic convolution of the two sequences a_n and b_n is

$$\sum_{\hat{j}=1}^{p-1} t^{\hat{j}} \sum_{\hat{i}=1}^{p-1} a_{\hat{i}} b_{\hat{j}-\hat{i}} = \sum_{\hat{j}=1}^{p-1} t^{\hat{j}} \sum_{\hat{i}=1}^{p-1} f_{g^{\hat{i}}} \psi^{g^{p-(\hat{j}-\hat{i})}} = \sum_{\hat{j}=1}^{p-1} t^{\hat{j}} \hat{F}_{g^{p-\hat{j}}}.$$

Rader's Trick iv

There exists a bijection from $g^{p-\hat{j}}$ to non-zero j, hence we can use one convolution to compute all $\hat{F}_j$. We then add f_0 back to $\hat{F}_j$ and compute F_0 to get all the points of DFT.

Rader's Trick v

An example of Rader's for $p = 5$:

$$
\begin{aligned}
F_0 &= f_0 + f_1 + f_2 + f_3 + f_4 \\
F_1 &= f_0 + (f_1\psi + f_2\psi^2 + f_4\psi^4 + f_3\psi^3) \\
F_2 &= f_0 + (f_1\psi^2 + f_2\psi^4 + f_4\psi^3 + f_3\psi) \\
F_4 &= f_0 + (f_1\psi^4 + f_2\psi^3 + f_4\psi + f_3\psi^2) \\
F_3 &= f_0 + (f_1\psi^3 + f_2\psi + f_4\psi^2 + f_3\psi^4)
\end{aligned}
$$

Or $(\hat{F}_1, \hat{F}_2, \hat{F}_4, \hat{F}_3) = (f_1, f_2, f_4, f_3) \star (\psi, \psi^3, \psi^4, \psi^2)$, where $\star$ is a convolution.

Rader's Extensible to Prime Power Size NTTs: Example $p = 9$

We compute mainly $(f_1, f_2, f_4, f_8, f_7, f_5) \star (\psi, \psi^5, \psi^7, \psi^8, \psi^4, \psi^2)$**, where** ψ **is the 9th root of unity**

Total we have two 3-NTTs, one 6-convolution and a few adds.

$$
\begin{aligned}
F_0 &= (f_0 + f_3 + f_6) + (f_1 + f_4 + f_7) + (f_2 + f_5 + f_8) \\
F_3 &= (f_0 + f_3 + f_6) + (f_1 + f_4 + f_7)\psi^3 + (f_2 + f_5 + f_8)\psi^6 \\
F_6 &= (f_0 + f_3 + f_6) + (f_1 + f_4 + f_7)\psi^6 + (f_2 + f_5 + f_8)\psi^3 \\
F_1 &= (f_0 + f_3\psi^3 + f_6\psi^6) + f_1\psi + f_2\psi^2 + f_4\psi^4 + f_8\psi^8 + f_7\psi^7 + f_5\psi^5 \\
F_2 &= (f_0 + f_3\psi^6 + f_6\psi^3) + f_1\psi^2 + f_2\psi^4 + f_4\psi^8 + f_8\psi^7 + f_7\psi^5 + f_5\psi^1 \\
F_4 &= (f_0 + f_3\psi^3 + f_6\psi^6) + f_1\psi^4 + f_2\psi^8 + f_4\psi^7 + f_8\psi^5 + f_7\psi + f_5\psi^2 \\
F_8 &= (f_0 + f_3\psi^6 + f_6\psi^3) + f_1\psi^8 + f_2\psi^7 + f_4\psi^5 + f_8\psi + f_7\psi^2 + f_5\psi^4 \\
F_7 &= (f_0 + f_3\psi^3 + f_6\psi^6) + f_1\psi^7 + f_2\psi^5 + f_4\psi + f_8\psi^2 + f_7\psi^4 + f_5\psi^8 \\
F_5 &= (f_0 + f_3\psi^6 + f_6\psi^3) + f_1\psi^5 + f_2\psi + f_4\psi^2 + f_8\psi^4 + f_7\psi^8 + f_5\psi^7
\end{aligned}
$$

Applying FFT: Schönhage

- Build an FFT-friendly environment for ring of the form $R[x]/\langle x^{mn} + 1 \rangle$ where the roots of -1 will "come from the variable"

Applying FFT: Schönhage

- Build an FFT-friendly environment for ring of the form $R[x]/\langle x^{mn}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mn}+1\rangle$ becomes a 2-variable polynomial $F(x, y)$ with $\deg_x < m$

Applying FFT: Schönhage

- Build an FFT-friendly environment for ring of the form $R[x]/\langle x^{mn}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mn}+1\rangle$ becomes a 2-variable polynomial $F(x,y)$ with $\deg_x < m$
- Ignore *part of* the modulus: only modulo y^n+1 $\quad$ *i.e.* work in $R[x][y]/\langle y^n+1\rangle$

Applying FFT: Schönhage

- Build an FFT-friendly environment for ring of the form $R[x]/\langle x^{mn}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mn}+1\rangle$ becomes a 2-variable polynomial $F(x,y)$ with $\deg_x < m$
- Ignore *part of* the modulus: only modulo y^n+1 $\quad$ *i.e.* work in $R[x][y]/\langle y^n+1\rangle$
- Since multiplication of two such polynomials have $\deg_x \le 2m-2$, we can pick any $nk > 2m-2$ and redundantly modulo $x^{nk}+1$ $\quad$ *i.e.* work in $\left(R[x]/\langle x^{nk}+1\rangle\right)[y]/\langle y^n+1\rangle$

Applying FFT: Schönhage

- Build an FFT-friendly environment for ring of the form $R[x]/\langle x^{mn}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mn}+1\rangle$ becomes a 2-variable polynomial $F(x,y)$ with $\deg_x < m$
- Ignore *part of* the modulus: only modulo $y^n + 1$ $\quad$ *i.e.* work in $R[x][y]/\langle y^n+1\rangle$
- Since multiplication of two such polynomials have $\deg_x \le 2m-2$, we can pick any $nk > 2m-2$ and redundantly modulo $x^{nk}+1$ $\quad$ *i.e.* work in $\left(R[x]/\langle x^{nk}+1\rangle\right)[y]/\langle y^n+1\rangle$
- Treating $R' = R[x]/\langle x^{nk}+1\rangle$, now we have n-th root of -1 in R', namely x^k

Applying FFT: Schönhage

- Build an FFT-friendly environment for ring of the form $R[x]/\langle x^{mn}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mn}+1\rangle$ becomes a 2-variable polynomial $F(x,y)$ with $\deg_x < m$
- Ignore *part of* the modulus: only modulo y^n+1 *i.e.* work in $R[x][y]/\langle y^n+1\rangle$
- Since multiplication of two such polynomials have $\deg_x \le 2m-2$, we can pick any $nk > 2m-2$ and redundantly modulo $x^{nk}+1$ *i.e.* work in $\left(R[x]/\langle x^{nk}+1\rangle\right)[y]/\langle y^n+1\rangle$
- Treating $R' = R[x]/\langle x^{nk}+1\rangle$, now we have n-th root of -1 in R', namely x^k
- Since x is just the variable, multiplying powers of x is simply shifting R-coefficients

Schönhage: Memory Access

■: addition/ subtraction ■: notifies the original place

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

: addition/ subtraction   : notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

: addition/ subtraction　　: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

keep going ...

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 1

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■ / ■ ■ ■ ■

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

keep going ...

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

keep going ...

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2

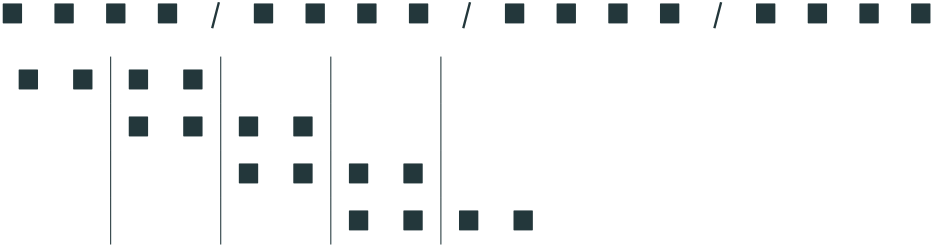
Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2



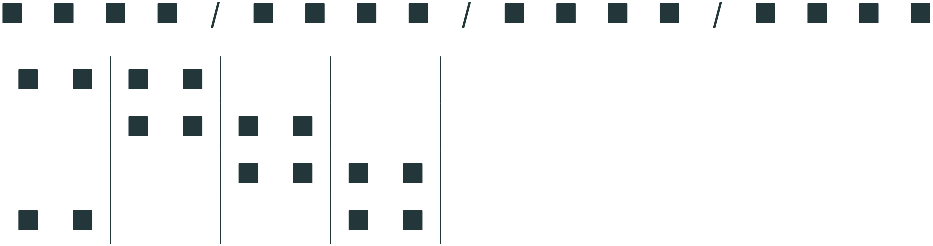
Schönhage: Memory Access

x is the required root such that $x^4 = -1$,

$t^4 + 1 = (t^2 + x^2)(t^2 - x^2) = (t - x)(t + x)(t - x^3)(t + x^3)$

■: addition/ subtraction ■: notifies the original place

Step 2



Applying FFT: Nussbaumer

- Build an FFT-friendly environment from ring of the form $R[x]/\langle x^{mnk} + 1\rangle$ where the roots of -1 will "come from the variable"

Applying FFT: Nussbaumer

- Build an FFT-friendly environment from ring of the form $R[x]/\langle x^{mnk}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mnk}+1\rangle$ becomes a 2-variable polynomial $F(y,x)$ with $\deg_x < m$

Applying FFT: Nussbaumer

- Build an FFT-friendly environment from ring of the form $R[x]/\langle x^{mnk}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mnk}+1\rangle$ becomes a 2-variable polynomial $F(y,x)$ with $\deg_x < m$
- Ignore *part of* the modulus: only mod $y^{nk}+1$ $\quad i.e.$ work in $\left(R[y]/\langle y^{nk}+1\rangle\right)[x]$

Applying FFT: Nussbaumer

- Build an FFT-friendly environment from ring of the form $R[x]/\langle x^{mnk}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mnk}+1\rangle$ becomes a 2-variable polynomial $F(y,x)$ with $\deg_x < m$
- Ignore *part of* the modulus: only mod $y^{nk}+1$ $\quad$ *i.e.* work in $\left(R[y]/\langle y^{nk}+1\rangle\right)[x]$
- A product of such polynomials have $\deg_x \le 2m-2$, so we can redundantly $\operatorname{mod}(x^{2n}-1)$ if $2n > 2m-2$ $\quad$ *i.e.* work in $\left(R[y]/\langle y^{nk}+1\rangle\right)[x]/\langle x^{2n}-1\rangle$

Applying FFT: Nussbaumer

- Build an FFT-friendly environment from ring of the form $R[x]/\langle x^{mnk} + 1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mnk} + 1\rangle$ becomes a 2-variable polynomial $F(y, x)$ with $\deg_x < m$
- Ignore *part of* the modulus: only mod $y^{nk} + 1$ *i.e.* work in $\left(R[y]/\langle y^{nk} + 1\rangle\right)[x]$
- A product of such polynomials have $\deg_x \leq 2m - 2$, so we can redundantly mod$(x^{2n} - 1)$ if $2n > 2m - 2$ *i.e.* work in $\left(R[y]/\langle y^{nk} + 1\rangle\right)[x]/\langle x^{2n} - 1\rangle$
- Treating $R' = R[y]/\langle y^{nk} + 1\rangle$, now we have $2n$-th root of 1 in R', namely y^k

Applying FFT: Nussbaumer

- Build an FFT-friendly environment from ring of the form $R[x]/\langle x^{mnk}+1\rangle$ where the roots of -1 will "come from the variable"
- Change x^m to y, so any polynomial $f(x) \in R[x]/\langle x^{mnk}+1\rangle$ becomes a 2-variable polynomial $F(y,x)$ with $\deg_x < m$
- Ignore *part of* the modulus: only mod $y^{nk}+1$ *i.e.* work in $\left(R[y]/\langle y^{nk}+1\rangle\right)[x]$
- A product of such polynomials have $\deg_x \le 2m-2$, so we can redundantly mod$(x^{2n}-1)$ if $2n > 2m-2$ *i.e.* work in $\left(R[y]/\langle y^{nk}+1\rangle\right)[x]/\langle x^{2n}-1\rangle$
- Treating $R' = R[y]/\langle y^{nk}+1\rangle$, now we have $2n$-th root of 1 in R', namely y^k
- Since y is a variable, multiplying powers of y is just shifting R-coefficients

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2
- One may also have to change the coefficient ring to do mults twice as long.

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2
- One may also have to change the coefficient ring to do mults twice as long.
- Although it requires only a linear number of small multiplications, there is also an overhead arising from $O(N \log N)$ adds/subs and scalar mults.

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2
- One may also have to change the coefficient ring to do mults twice as long.
- Although it requires only a linear number of small multiplications, there is also an overhead arising from $O(N \log N)$ adds/subs and scalar mults.
- Schönhage/ Nussbaumer expands the coefficient size by another factor of 2

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2
- One may also have to change the coefficient ring to do mults twice as long.
- Although it requires only a linear number of small multiplications, there is also an overhead arising from $O(N \log N)$ adds/subs and scalar mults.
- Schönhage/ Nussbaumer expands the coefficient size by another factor of 2
- For Schönhage/ Nussbaumer, we don't have to do scalar multiplication, but each small polynomial to be multiplied still has a certain degree

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2
- One may also have to change the coefficient ring to do mults twice as long.
- Although it requires only a linear number of small multiplications, there is also an overhead arising from $O(N \log N)$ adds/subs and scalar mults.
- Schönhage/ Nussbaumer expands the coefficient size by another factor of 2
- For Schönhage/ Nussbaumer, we don't have to do scalar multiplication, but each small polynomial to be multiplied still has a certain degree
- One might choose FFT, esp. Schönhage/Nussbaumer at 700+ degree

Summary: Pros and Cons

- To do FFT on a specific ring, one often has to switch the polynomial modulus, causing expansion of degree by at least a factor of 2
- One may also have to change the coefficient ring to do mults twice as long.
- Although it requires only a linear number of small multiplications, there is also an overhead arising from $O(N \log N)$ adds/subs and scalar mults.
- Schönhage/ Nussbaumer expands the coefficient size by another factor of 2
- For Schönhage/ Nussbaumer, we don't have to do scalar multiplication, but each small polynomial to be multiplied still has a certain degree
- One might choose FFT, esp. Schönhage/Nussbaumer at 700+ degree
- often the advantage comes from caching your NTT and delaying its NTT.

Any Questions?

FFT/NTT: Order of Input/Output

One can extend the binary case and define an index calculation function $R_{p_1,\dots,p_n}$ for an NTT using n layers with radix-p_i on layer $1 \le i \le n$ in a recursive manner as $R_p(k) = k$ for an index k and

$$R_{p_1,\dots,p_{n-1},p_n}(k) = \left(k - \left\lfloor \frac{k}{p_n} \right\rfloor p_n\right) \cdot \prod_{i=1}^{n} p_i + R_{p_1,\dots,p_{n-1}}\left(\left\lfloor \frac{k}{p_n} \right\rfloor\right).$$

This can be used to express the output order of an NTT. For example, the "digit reversed" index permutation dr_{270} of a 270-NTT that applies one radix-2, three radix-3, and finally one radix-5 stage can thus be expressed as

$$dr_{270} = [R_{2,3,3,3,5}(0), R_{2,3,3,3,5}(1), \dots, R_{2,3,3,3,5}(269)].$$

Split-radix FFT Trick

- Base case of split-radix FFT: (ζ is an n-th root of $i = \sqrt{-1}$)

$$R[x]/\langle x^{4n} - 1\rangle \cong R[x]/\langle x^{2n} - 1\rangle \times R[x]/\langle x^{2n} + 1\rangle$$
$$\cong R[x]/\langle x^{n} - 1\rangle \times R[x]/\langle x^{n} + 1\rangle \times R[x]/\langle x^{n} - i\rangle \times R[x]/\langle x^{n} + i\rangle$$

2^{nd} component: $R[x]/\langle x^n + 1\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta^2 y$

3^{rd} component: $R[x]/\langle x^n - i\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta y$

4^{th} component: $R[x]/\langle x^n + i\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta^3 y$

Split-radix FFT Trick

- Base case of split-radix FFT: (ζ is an n-th root of $i = \sqrt{-1}$)

  $$R[x]/\langle x^{4n} - 1\rangle \cong R[x]/\langle x^{2n} - 1\rangle \times R[x]/\langle x^{2n} + 1\rangle$$
  $$\cong R[x]/\langle x^{n} - 1\rangle \times R[x]/\langle x^{n} + 1\rangle \times R[x]/\langle x^{n} - i\rangle \times R[x]/\langle x^{n} + i\rangle$$

  2^{nd} component: $R[x]/\langle x^n + 1\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta^2 y$

  3^{rd} component: $R[x]/\langle x^n - i\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta y$

  4^{th} component: $R[x]/\langle x^n + i\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta^3 y$

- The complete mapping would be:

  $$R[x]/\langle x^{4n} - 1\rangle \cong \prod^4 R[x]/\langle x^{n} - 1\rangle$$

$$\begin{bmatrix} a_0 & \cdots & a_{n-1} \\ a_n & \cdots & a_{2n-1} \\ a_{2n} & \cdots & a_{3n-1} \\ a_{3n} & \cdots & a_{4n-1} \end{bmatrix} \longrightarrow \begin{bmatrix} ((a_0+a_{2n})+(a_n+a_{3n})) & \cdots & ((a_{n-1}+a_{3n-1})+(a_{2n-1}+a_{4n-1})) \\ ((a_0+a_{2n})-(a_n+a_{3n})) & \cdots & ((a_{n-1}+a_{3n-1})-(a_{2n-1}+a_{4n-1}))\zeta^{2(n-1)} \\ ((a_0-a_{2n})+i(a_n-a_{3n})) & \cdots & ((a_{n-1}-a_{3n-1})+i(a_{2n-1}-a_{4n-1}))\zeta^{(n-1)} \\ ((a_0-a_{2n})-i(a_n-a_{3n})) & \cdots & ((a_{n-1}-a_{3n-1})-i(a_{2n-1}-a_{4n-1}))\zeta^{3(n-1)} \end{bmatrix}$$

Split-radix FFT Trick

- Base case of split-radix FFT: (ζ is an n-th root of $i = \sqrt{-1}$)

  $R[x]/\langle x^{4n} - 1\rangle \cong R[x]/\langle x^{2n} - 1\rangle \times R[x]/\langle x^{2n} + 1\rangle$

  $\cong R[x]/\langle x^{n} - 1\rangle \times R[x]/\langle x^{n} + 1\rangle \times R[x]/\langle x^{n} - i\rangle \times R[x]/\langle x^{n} + i\rangle$

  2^{nd} component: $R[x]/\langle x^n + 1\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta^2 y$

  3^{rd} component: $R[x]/\langle x^n - i\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta y$

  4^{th} component: $R[x]/\langle x^n + i\rangle \cong R[y]/\langle y^n - 1\rangle$, by $x \leftrightarrow \zeta^3 y$

- The complete mapping would be:

  $R[x]/\langle x^{4n} - 1\rangle \cong \prod^4 R[x]/\langle x^n - 1\rangle$

$$\begin{bmatrix} a_0 & \cdots & a_{n-1} \\ a_n & \cdots & a_{2n-1} \\ a_{2n} & \cdots & a_{3n-1} \\ a_{3n} & \cdots & a_{4n-1} \end{bmatrix} \longrightarrow \begin{bmatrix} ((a_0+a_{2n})+(a_n+a_{3n})) & \cdots & ((a_{n-1}+a_{3n-1})+(a_{2n-1}+a_{4n-1})) \\ ((a_0+a_{2n})-(a_n+a_{3n})) & \cdots & ((a_{n-1}+a_{3n-1})-(a_{2n-1}+a_{4n-1}))\zeta^{2(n-1)} \\ ((a_0-a_{2n})+i(a_n-a_{3n})) & \cdots & ((a_{n-1}-a_{3n-1})+i(a_{2n-1}-a_{4n-1}))\zeta^{(n-1)} \\ ((a_0-a_{2n})-i(a_n-a_{3n})) & \cdots & ((a_{n-1}-a_{3n-1})-i(a_{2n-1}-a_{4n-1}))\zeta^{3(n-1)} \end{bmatrix}$$

- **This is useful mainly for complex numbers!!**

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and switch to modulo $y^4 + 1$. This gives
  $F(x, y) = (1 + 2x \quad) + (3 + 4x \quad)y$
  $\quad + (-1 - 2x \quad)y^2 + (-3 - 4x \quad)y^3$

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and switch to modulo $y^4 + 1$. This gives
  $F(x, y) = (1 + 2x \quad) + (3 + 4x \quad)y$
  $\quad + (-1 - 2x \quad)y^2 + (-3 - 4x \quad)y^3$
- Since $F(x, y)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 + 1$

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and switch to modulo $y^4 + 1$. This gives
  $$\begin{aligned} F(x,y) = &(1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y \\ &+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3 \end{aligned}$$
- Since $F(x,y)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 + 1$

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and switch to modulo $y^4 + 1$. This gives
  $$\begin{aligned} F(x,y) = &(1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y \\ &+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3 \end{aligned}$$
- Since $F(x,y)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 + 1$
- If we view $R' = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$ and $F(x,y) \in R'[y]/\langle y^4 + 1\rangle$, we can proceed FFT

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and switch to modulo $y^4 + 1$. This gives
  $$F(x, y) = (1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y$$
  $$+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3$$
- Since $F(x, y)^2$ have $\deg_x \le 2$, we can redundantly modulo $x^4 + 1$
- If we view $R' = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$ and $F(x, y) \in R'[y]/\langle y^4 + 1\rangle$, we can proceed FFT
- Finally, we get $F(x, y)^2 \in R'[y]/\langle y^4 + 1\rangle$ or simply $R[x, y]/\langle y^4 + 1\rangle$, since we knew modulo $x^4 + 1$ is redundant

Schönhage: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and switch to modulo $y^4 + 1$. This gives
  $$F(x, y) = (1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y$$
  $$+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3$$
- Since $F(x, y)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 + 1$
- If we view $R' = \mathbb{Z}_7[x]/\langle x^4 + 1\rangle$ and $F(x, y) \in R'[y]/\langle y^4 + 1\rangle$, we can proceed FFT
- Finally, we get $F(x, y)^2 \in R'[y]/\langle y^4 + 1\rangle$ or simply $R[x, y]/\langle y^4 + 1\rangle$, since we knew modulo $x^4 + 1$ is redundant
- Replace y back to x^2 will recover $f(x)^2$

Schönhage: Example (II)

$\mathbb{Z}_7[x]/\langle x^8 + 1\rangle$ | $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$

Schönhage: Example (II)

$\mathbb{Z}_7[x]/\langle x^8+1\rangle$	$f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$
$R'[y]/\langle y^4+1\rangle$	$F(x,y) = (1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y$ $+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3$

Schönhage: Example (II)

$\mathbb{Z}_7[x]/\langle x^8+1\rangle$	$f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$
$R'[y]/\langle y^4+1\rangle$	$F(x,y) = (1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y$ $+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3$
$R'[y]/\langle y^2-x^2\rangle$	$(1 + 2x - x^2 - 2x^3) + (3 + 4x - 3x^2 - 4x^3)y$
$R'[y]/\langle y^2+x^2\rangle$	$(1 + 2x + x^2 + 2x^3) + (3 + 4x + 3x^2 + 4x^3)y$

Schönhage: Example (II)

$\mathbb{Z}_7[x]/\langle x^8+1\rangle$	$f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$
$R'[y]/\langle y^4+1\rangle$	$F(x,y) = (1 + 2x + 0x^2 + 0x^3) + (3 + 4x + 0x^2 + 0x^3)y$ $+(-1 - 2x + 0x^2 + 0x^3)y^2 + (-3 - 4x + 0x^2 + 0x^3)y^3$
$R'[y]/\langle y^2-x^2\rangle$	$(1 + 2x - x^2 - 2x^3) + (3 + 4x - 3x^2 - 4x^3)y$
$R'[y]/\langle y^2+x^2\rangle$	$(1 + 2x + x^2 + 2x^3) + (3 + 4x + 3x^2 + 4x^3)y$
$R'[y]/\langle y-x\rangle$	$(5 + 5x + 3x^2 - 5x^3)$
$R'[y]/\langle y+x\rangle$	$(-3 - x - 5x^2 + x^3)$
$R'[y]/\langle y-x^3\rangle$	$(-3 - x - 3x^2 + 5x^3)$
$R'[y]/\langle y+x^3\rangle$	$(5 + 5x + 5x^2 - x^3)$

Schönhage: Example (III)

$R'[y]/\langle y - x\rangle$	$(3 + 3x + 2x^2 + x^3)$
$R'[y]/\langle y + x\rangle$	$(0 + 2x + 2x^2 + 4x^3)$
$R'[y]/\langle y - x^3\rangle$	$(3 + x + x^2 + 4x^3)$
$R'[y]/\langle y + x^3\rangle$	$(3 + 4x + 4x^2 - 2x^3)$

Schönhage: Example (III)

$R'[y]/\langle y - x\rangle$	$(3 + 3x + 2x^2 + x^3)$
$R'[y]/\langle y + x\rangle$	$(0 + 2x + 2x^2 + 4x^3)$
$R'[y]/\langle y - x^3\rangle$	$(3 + x + x^2 + 4x^3)$
$R'[y]/\langle y + x^3\rangle$	$(3 + 4x + 4x^2 - 2x^3)$
$R'[y]/\langle y^2 - x^2\rangle$	$(3 - 2x + 4x^2 - 2x^3) + (1 + 0x - 3x^2 - 3x^3)y$
$R'[y]/\langle y^2 + x^2\rangle$	$(-1 - 2x - 2x^2 + 2x^3) + (-1 + 0x + 3x^2 + 3x^3)y$

Schönhage: Example (III)

$R'[y]/\langle y - x\rangle$	$(3 + 3x + 2x^2 + x^3)$
$R'[y]/\langle y + x\rangle$	$(0 + 2x + 2x^2 + 4x^3)$
$R'[y]/\langle y - x^3\rangle$	$(3 + x + x^2 + 4x^3)$
$R'[y]/\langle y + x^3\rangle$	$(3 + 4x + 4x^2 - 2x^3)$
$R'[y]/\langle y^2 - x^2\rangle$	$(3 - 2x + 4x^2 - 2x^3) + (1 + 0x - 3x^2 - 3x^3)y$
$R'[y]/\langle y^2 + x^2\rangle$	$(-1 - 2x - 2x^2 + 2x^3) + (-1 + 0x + 3x^2 + 3x^3)y$
$R'[y]/\langle y^4 + 1\rangle$	$4F(x, y)^2 = (2 - 4x + 2x^2 + 0x^3) + (0 + 0x + 0x^2 + 0x^3)y$ $+(-1 - 4x - 4x^2 + 0x^3)y^2 + (1 + x - 2x^2 + 0x^3)y^3$

Schönhage: Example (III)

$R'[y]/\langle y - x \rangle$	$(3 + 3x + 2x^2 + x^3)$
$R'[y]/\langle y + x \rangle$	$(0 + 2x + 2x^2 + 4x^3)$
$R'[y]/\langle y - x^3 \rangle$	$(3 + x + x^2 + 4x^3)$
$R'[y]/\langle y + x^3 \rangle$	$(3 + 4x + 4x^2 - 2x^3)$
$R'[y]/\langle y^2 - x^2 \rangle$	$(3 - 2x + 4x^2 - 2x^3) + (1 + 0x - 3x^2 - 3x^3)y$
$R'[y]/\langle y^2 + x^2 \rangle$	$(-1 - 2x - 2x^2 + 2x^3) + (-1 + 0x + 3x^2 + 3x^3)y$
$R'[y]/\langle y^4 + 1 \rangle$	$4F(x, y)^2 = (2 - 4x + 2x^2 + 0x^3) + (0 + 0x + 0x^2 + 0x^3)y$ $+(-1 - 4x - 4x^2 + 0x^3)y^2 + (1 + x - 2x^2 + 0x^3)y^3$
$\mathbb{Z}_7[x]/\langle x^8 + 1 \rangle$	$4f(x)^2 = 4 - 4x + 2x^2 + 0x^3 - x^4 - 4x^5 - 3x^6 + x^7$ $f(x)^2 = 1 - x + 4x^2 + 0x^3 - 2x^4 - x^5 + x^6 + 2x^7$

Nussbaumer: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$

Nussbaumer: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and always modulo $y^4 + 1$. This gives
  $F(y, x) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$

Nussbaumer: Example (I)

- We want to square $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and always modulo $y^4 + 1$. This gives $F(y, x) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$
- Since $F(y, x)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 - 1$.

Nussbaumer: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and always modulo $y^4 + 1$. This gives
  $$F(y,x) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x + (0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$$
- Since $F(y,x)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 - 1$.

Nussbaumer: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and always modulo $y^4 + 1$. This gives
  $$F(y, x) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x + (0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$$
- Since $F(y, x)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 - 1$.
- If we view $R' = \mathbb{Z}_7[y]/\langle y^4 + 1\rangle$ and $F(y, x) \in R'[x]/\langle x^4 - 1\rangle$, we can proceed FFT

Nussbaumer: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and always modulo $y^4 + 1$. This gives
  $$F(y, x) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x + (0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$$
- Since $F(y, x)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 - 1$.
- If we view $R' = \mathbb{Z}_7[y]/\langle y^4 + 1\rangle$ and $F(y, x) \in R'[x]/\langle x^4 - 1\rangle$, we can proceed FFT
- Finally, we get $F(y, x)^2 \in R'[x]/\langle x^4 - 1\rangle$ or simply $R'[x] = R[x, y]/\langle y^4 + 1\rangle$, since we knew modulo $x^4 - 1$ is redundant

Nussbaumer: Example (I)

- We want to square
  $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7 \in \mathbb{Z}_7[x]/\langle x^8 + 1\rangle$
- Replace x^2 by y and always modulo $y^4 + 1$. This gives
  $F(y, x) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$
  $+ (0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$
- Since $F(y, x)^2$ have $\deg_x \leq 2$, we can redundantly modulo $x^4 - 1$.
- If we view $R' = \mathbb{Z}_7[y]/\langle y^4 + 1\rangle$ and $F(y, x) \in R'[x]/\langle x^4 - 1\rangle$, we can proceed FFT
- Finally, we get $F(y, x)^2 \in R'[x]/\langle x^4 - 1\rangle$ or simply $R'[x] = R[x, y]/\langle y^4 + 1\rangle$, since we knew modulo $x^4 - 1$ is redundant
- Replace y back to x^2 will recover $f(x)^2$

Nussbaumer: Example (II)

$\mathbb{Z}_7[x]/\langle x^8 + 1 \rangle$ | $f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$

Nussbaumer: Example (II)

$\mathbb{Z}_7[x]/\langle x^8+1\rangle$	$f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$
$R'[x]/\langle x^4-1\rangle$	$F(x,y) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$ $+(0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$

Nussbaumer: Example (II)

$\mathbb{Z}_7[x]/\langle x^8+1\rangle$	$f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$
$R'[x]/\langle x^4-1\rangle$	$F(x,y) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$ $+(0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$
$R'[x]/\langle x^2-1\rangle$	$(1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$
$R'[x]/\langle x^2+1\rangle$	$(1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$

Nussbaumer: Example (II)

$\mathbb{Z}_7[x]/\langle x^8+1\rangle$	$f(x) = 1 + 2x + 3x^2 + 4x^3 - x^4 - 2x^5 - 3x^6 - 4x^7$
$R'[x]/\langle x^4-1\rangle$	$F(x,y) = (1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$ $+(0 + 0y + 0y^2 + 0y^3)x^2 + (0 + 0y + 0y^2 + 0y^3)x^3$
$R'[x]/\langle x^2-1\rangle$	$(1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$
$R'[x]/\langle x^2+1\rangle$	$(1 + 3y - y^2 - 3y^3) + (2 + 4y - 2y^2 - 4y^3)x$
$R'[x]/\langle x-1\rangle$	$(3 + 0y - 3y^2 + 0y^3)$
$R'[x]/\langle x+1\rangle$	$(-1 - y + y^2 + y^3)$
$R'[x]/\langle x-y^2\rangle$	$(1 + 3y - 0y^2 + 0y^3)$
$R'[x]/\langle x+y^2\rangle$	$(3 + 0y + y^2 + y^3)$