Polynomial Multiplication Techniques

Bo-Yin Yang (with Matthias Kannwischer)

June 8, 2023 at Vodice

Polynomial Multiplications

Karatsuba and Toom(-Cook)

Our Goal

- Do multiplication over rings like $\mathbb{Z}_{3329}[x]/\langle x^{256}+1\rangle$ or $\mathbb{Z}_{4591}[x]/\langle x^{761}-x-1\rangle$

Our Goal

- Do multiplication over rings like $\mathbb{Z}_{3329}[x]/\langle x^{256} + 1\rangle$ or $\mathbb{Z}_{4591}[x]/\langle x^{761} - x - 1\rangle$
- For efficiency considerations, one would like to replace multiplication sub-steps by addition sub-steps as much as possible

Our Goal

- Do multiplication over rings like $\mathbb{Z}_{3329}[x]/\langle x^{256}+1\rangle$ or $\mathbb{Z}_{4591}[x]/\langle x^{761}-x-1\rangle$
- For efficiency considerations, one would like to replace multiplication sub-steps by addition sub-steps as much as possible
- This talk reviews some techniques for this purpose

Rule of Thumb

To make these techniques applicable to our specific rings/ polynomials, we can

Rule of Thumb

To make these techniques applicable to our specific rings/ polynomials, we can

- Ignore modular arithmetic
  e.g. $\mathbb{Z}_p[x]/\langle x^5 - x - 1\rangle \longrightarrow \mathbb{Z}_p[x]$

Rule of Thumb

To make these techniques applicable to our specific rings/ polynomials, we can

- Ignore modular arithmetic
  e.g. $\mathbb{Z}_p[x]/\langle x^5 - x - 1\rangle \longrightarrow \mathbb{Z}_p[x]$
- Replace things into variables
  e.g. $(10110101)_2 \in \mathbb{Z}_{257} \longrightarrow (1011)_2\, y + (0101)_2 \in \mathbb{Z}_{257}[y]$ with $y = 2^4$

Rule of Thumb

To make these techniques applicable to our specific rings/ polynomials, we can

- Ignore modular arithmetic

  e.g. $\mathbb{Z}_p[x]/\langle x^5 - x - 1\rangle \longrightarrow \mathbb{Z}_p[x]$
- Replace things into variables

  e.g. $(10110101)_2 \in \mathbb{Z}_{257} \longrightarrow (1011)_2\, y + (0101)_2 \in \mathbb{Z}_{257}[y]$ with $y = 2^4$
- Do redundant modular arithmetic

  e.g. $f(x), g(x) \in \mathbb{Z}_p[x]$ with $\deg(f) + \deg(g) < n \longrightarrow \bar{f}(x), \bar{g}(x) \in \mathbb{Z}_p[x]/\langle x^n - 1\rangle$

Karatsuba

- A simple observation: $(a_0 + a_1 x)(b_0 + b_1 x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + a_1 b_1 x^2$ where $a_0 b_1 + a_1 b_0 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$

Karatsuba

- A simple observation: $(a_0 + a_1 x)(b_0 + b_1 x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + a_1 b_1 x^2$ where $a_0 b_1 + a_1 b_0 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$
- The three products are evaluations of the resulting polynomial at $x = 0, 1, \infty$ We can recover the degree-2 polynomial by interpolation

Karatsuba

- A simple observation: $(a_0 + a_1 x)(b_0 + b_1 x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + a_1 b_1 x^2$ where $a_0 b_1 + a_1 b_0 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$
- The three products are evaluations of the resulting polynomial at $x = 0, 1, \infty$ We can recover the degree-2 polynomial by interpolation
- Improved form: $(a_0 + a_1 x)(b_0 + b_1 x) = (a_0 + a_1)(b_0 + b_1)x + (a_0 b_0 - a_1 b_1 x)(1 - x)$

Karatsuba

- A simple observation: $(a_0 + a_1 x)(b_0 + b_1 x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + a_1 b_1 x^2$ where $a_0 b_1 + a_1 b_0 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$
- The three products are evaluations of the resulting polynomial at $x = 0, 1, \infty$ We can recover the degree-2 polynomial by interpolation
- Improved form: $(a_0 + a_1 x)(b_0 + b_1 x) = (a_0 + a_1)(b_0 + b_1)x + (a_0 b_0 - a_1 b_1 x)(1 - x)$
- This applies when our operands are in the form of linear polynomials

Karatsuba to multiply $f(x), g(x)$ each having degree $< 2n$

- Change x^n to y, use Karatsuba in y: 3 polymuls in x of degree $< n$

$$(1 + 2x + 2x^2 + 2x^3) \cdot (3 + x + 4x^2 + x^3) = [(1 + 2x) + (2 + 2x)y] \cdot [(3 + x) + (4 + x)y]$$

Karatsuba to multiply $f(x), g(x)$ each having degree $< 2n$

- Change x^n to y, use Karatsuba in y: 3 polymuls in x of degree $< n$
- The resulting polynomial has degree ≤ 2 in y. Change y back to x^n

$$(1 + 2x + 2x^2 + 2x^3) \cdot (3 + x + 4x^2 + x^3) = [(1 + 2x) + (2 + 2x)y] \cdot [(3 + x) + (4 + x)y]$$

Karatsuba to multiply $f(x), g(x)$ each having degree $< 2n$

- Change x^n to y, use Karatsuba in y: 3 polymuls in x of degree $< n$
- The resulting polynomial has degree ≤ 2 in y. Change y back to x^n

$$(1 + 2x + 2x^2 + 2x^3) \cdot (3 + x + 4x^2 + x^3) = [(1 + 2x) + (2 + 2x)y] \cdot [(3 + x) + (4 + x)y]$$

$$= [(3 + 4x)(7 + 2x)]y + [(1 + 2x)(3 + x) - (2 + 2x)(4 + x)y](1 - y)$$

$$= [63x + (21 - 8x)(1 - x)]y + [12x + (3 - 2x)(1 - x) - [20x + (8 - 2x)(1 - x)]y](1 - y)$$

$$= [21 + (\tfrac{-8+63}{-21})x + 8x^2]y + [3 + (\tfrac{-2+12}{-3})x + 2x^2 - [8 + (\tfrac{-2+20}{-8})x + 2x^2]y](1 - y)$$

$$= [21 + 34x + 8x^2]y + [3 + 7x + 2x^2 - (8 + 10x + 2x^2)y](1 - y)$$

Karatsuba to multiply $f(x), g(x)$ each having degree $< 2n$

- Change x^n to y, use Karatsuba in y: 3 polymuls in x of degree $< n$
- The resulting polynomial has degree ≤ 2 in y. Change y back to x^n

$$(1 + 2x + 2x^2 + 2x^3) \cdot (3 + x + 4x^2 + x^3) = [(1 + 2x) + (2 + 2x)y] \cdot [(3 + x) + (4 + x)y]$$

$$= [(3 + 4x)(7 + 2x)]y + [(1 + 2x)(3 + x) - (2 + 2x)(4 + x)y](1 - y)$$

$$= [63x + (21 - 8x)(1 - x)]y + [12x + (3 - 2x)(1 - x) - [20x + (8 - 2x)(1 - x)]y](1 - y)$$

$$= [21 + \binom{-8+63}{-21}x + 8x^2]y + [3 + \binom{-2+12}{-3}x + 2x^2 - [8 + \binom{-2+20}{-8}x + 2x^2]y](1 - y)$$

$$= [21 + 34x + 8x^2]y + [3 + 7x + 2x^2 - (8 + 10x + 2x^2)y](1 - y)$$

$$= [3 + 7x + 2x^2] + [\binom{-8+21}{-3} + \binom{-10+34}{-7}x + \binom{-2+8}{-2}x^2]y + [8 + 10x + 2x^2]y^2$$

$$= 3 + 7x + (2 + 10)x^2 + 17x^3 + (4 + 8)x^4 + 10x^5 + 2x^6$$

Why "Improved" Karatsuba? i

Counting Additions: Why is $(a_0 + a_1x)(b_0 + b_1x) = (a_0 + a_1)(b_0 + b_1)x + (a_0b_0 - a_1b_1x)(1 - x)$ **better?**

- Suppose $x = t^{100}$, each of a_0, a_1, b_0, b_1 is a length 100 polynomial in t.
- Each product a_0b_0, a_1b_1, $(a_0 + a_1)(b_0 + b_1)$ is a length 199 polynomial in t.
- Can count 8 additions/subtractions in "standard" Karatsuba

$(a_0+a_1) \times (b_0+b_1)\,x$

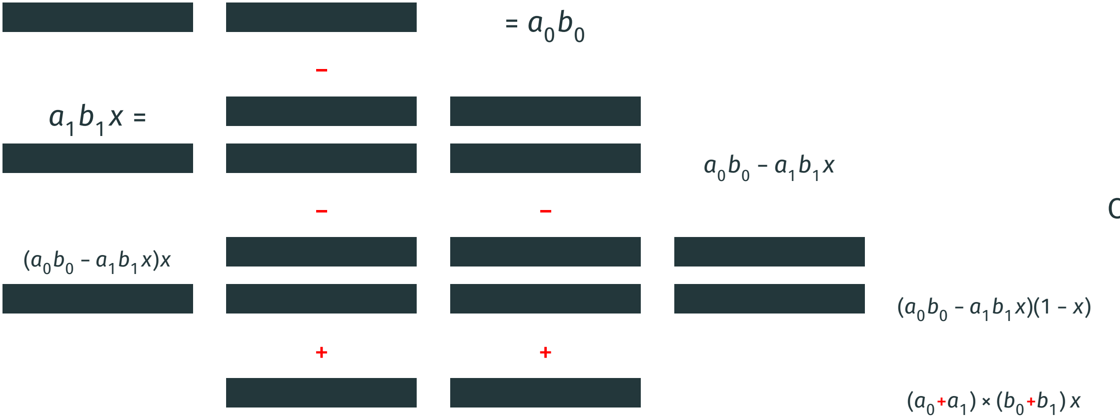
a_0b_0x

a_1b_1x

$a_0b_0 + a_1b_1x^2$

Why "Improved" Karatsuba? ii

Counting Additions: Why is $(a_0 + a_1 x)(b_0 + b_1 x) = (a_0 + a_1)(b_0 + b_1)x + (a_0 b_0 - a_1 b_1 x)(1 - x)$ **better?**



(actually 100) addition/subtraction has seemingly vanished into thin air!!

Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$

■ ■ ■ ■ ■ ■ ■ ■/

■ ■ ■ ■ ■ ■ ■ ■/

Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$

■ ■ ■ ■ ■ ■ ■ ■/■ ■ ■ ■/

■ ■ ■ ■ ■ ■ ■ ■/■ ■ ■ ■/

Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$

■ ■ ■ ■/■ ■ ■ ■/■ ■ ■ ■/

■ ■ ■ ■/■ ■ ■ ■/■ ■ ■ ■/

Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$

■ ■ ■ ■/■ ■ ■ ■/■ ■ ■ ■/■ ■/■ ■/■ ■/

■ ■ ■ ■/■ ■ ■ ■/■ ■ ■ ■/■ ■/■ ■/■ ■/

Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$

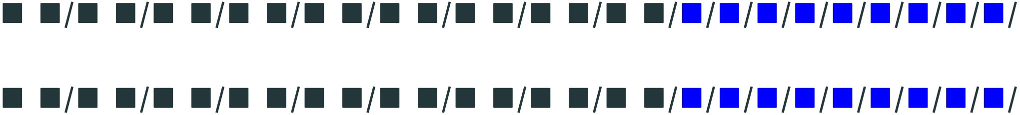
■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/

■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/■ ■/

Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$



Repeated Karatsuba: Memory Access

If we want to do three layers of Karatsuba for polynomials of degree $< 8n$

■: polynomial of degree $< n$

■/

■/

Apply (■ × ■) to the 27 pairs

Toom-3

- To multiply $(a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2)$, evaluate at 5 points
  A simple choice will be $x = 0, \pm 1, -2, \infty \longrightarrow F(0), F(1), F(-1), F(-2), F(\infty)$

Toom-3

- To multiply $(a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2)$, evaluate at 5 points
  A simple choice will be $x = 0, \pm 1, -2, \infty \longrightarrow F(0), F(1), F(-1), F(-2), F(\infty)$
- Interpolate the degree-4 polynomial $F(x) = \Sigma_{i=0}^{4} c_i x^i$. In matrix form,

$$\begin{bmatrix} F(0) \\ F(1) \\ F(-1) \\ F(-2) \\ F(\infty) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -2 & 4 & -8 & 16 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix}$$

The coefficients can be determined by applying the inverse matrix

Toom-3

- To multiply $(a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2)$, evaluate at 5 points
  A simple choice will be $x = 0, \pm 1, -2, \infty \longrightarrow F(0), F(1), F(-1), F(-2), F(\infty)$
- Interpolate the degree-4 polynomial $F(x) = \Sigma_{i=0}^{4} c_i x^i$. In matrix form,

$$\begin{bmatrix} F(0) \\ F(1) \\ F(-1) \\ F(-2) \\ F(\infty) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -2 & 4 & -8 & 16 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix}$$

  The coefficients can be determined by applying the inverse matrix
- This applies when our operands are in the form of polynomials of degree < 3

Toom-4 and Higher

- To multiply $f(x), g(x)$ each having degree $< 4n$, change x^n to y

Toom-4 and Higher

- To multiply $f(x), g(x)$ each having degree $< 4n$, change x^n to y
- Use Toom-4 in y: evaluate y at 7 points (= 7 mult. of poly. in x of degree $< n$)

Toom-4 and Higher

- To multiply $f(x), g(x)$ each having degree $< 4n$, change x^n to y
- Use Toom-4 in y: evaluate y at 7 points (= 7 mult. of poly. in x of degree $< n$)
- Interpolate the polynomial in y

Toom-4 and Higher

- To multiply $f(x), g(x)$ each having degree $< 4n$, change x^n to y
- Use Toom-4 in y: evaluate y at 7 points (= 7 mult. of poly. in x of degree $< n$)
- Interpolate the polynomial in y

- Sometimes uses plus-minus powers of 2, not integers as interpolation points.

"Evaluation and Interpolation at $1/a$"

Instead of computing $f(1/a) = \sum_{j=0}^{k-1} f_j (1/a)^j$, we compute $a^{k-1} f(1/a) = \sum_{j=0}^{k-1} f_j a^{k-1-j}$. After the point multiplication, we have $a^{2k-2} f(1/a) g(1/a) = \left(\sum_{j=0}^{k-1} f_j a^{k-1-j}\right)\left(\sum_{j=0}^{k-1} g_j a^{k-1-j}\right)$.

Summary: Pros and Cons

- Karatsuba: 3 polynomial multiplications instead of 4, small overhead

Summary: Pros and Cons

- Karatsuba: 3 polynomial multiplications instead of 4, small overhead
- Toom: fewer polynomial multiplications ($2k - 1$ instead of k^2), but incurs certain overhead

Summary: Pros and Cons

- Karatsuba: 3 polynomial multiplications instead of 4, small overhead
- Toom: fewer polynomial multiplications ($2k - 1$ instead of k^2), but incurs certain overhead
- Toom-k works better only when the degree of polynomial is large enough

Summary: Pros and Cons

- Karatsuba: 3 polynomial multiplications instead of 4, small overhead
- Toom: fewer polynomial multiplications ($2k - 1$ instead of k^2), but incurs certain overhead
- Toom-k works better only when the degree of polynomial is large enough
  - For larger systems Fast Fourier Transform methods dominate.

Summary: Pros and Cons

- Karatsuba: 3 polynomial multiplications instead of 4, small overhead
- Toom: fewer polynomial multiplications ($2k - 1$ instead of k^2), but incurs certain overhead
- Toom-k works better only when the degree of polynomial is large enough
  - For larger systems Fast Fourier Transform methods dominate.
  - May be best for NTRU type on Neon with Toeplitz variation.

Summary: Pros and Cons

- Karatsuba: 3 polynomial multiplications instead of 4, small overhead
- Toom: fewer polynomial multiplications ($2k - 1$ instead of k^2), but incurs certain overhead
- Toom-k works better only when the degree of polynomial is large enough
  - For larger systems Fast Fourier Transform methods dominate.
  - May be best for NTRU type on Neon with Toeplitz variation.
  - Note you need extra precision to divide by 2 mod 2^k.

Toeplitz Matrix Methods

Want these matrix-vector product, which cyclic convolutions are

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} a_0 & a_{-1} & a_{-2} & a_{-3} & \cdots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & a_{-2} & \cdots & a_{-n+2} \\ a_2 & a_1 & a_0 & a_{-1} & \cdots & a_{-n+3} \\ a_3 & a_2 & a_1 & a_0 & \cdots & a_{-n+4} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \end{bmatrix}$$

Such matrices are "Toeplitz". Submatrices of a Toeplitz matrix are Toeplitz. So

$$\begin{bmatrix} C_0 \\ C_1 \end{bmatrix} = \begin{bmatrix} A_0 & A_{-1} \\ A_1 & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \end{bmatrix} \text{ or } \begin{cases} C_0 & = & A_{-1}B_1 + A_0B_0 & = & (A_{-1} - A_0)B_1 + A_0(B_0 + B_1), \\ C_1 & = & A_0B_1 + A_1B_0 & = & A_0(B_0 + B_1) + (A_1 - A_0)B_0. \end{cases}$$

How to Obtain Toeplitz formulas from Toom/Karatsuba formulas

$$\begin{aligned} B_0C_0 &= B_0C_0 \\ B_0C_1 + B_1C_0 &= (B_0 + B_1)(C_0 + C_1) - B_0C_0 - B_1C_1 \\ B_1C_1 &= B_1C_1 \end{aligned}$$

Now multiply the three formulas by A_0, A_1, and A_2, add together

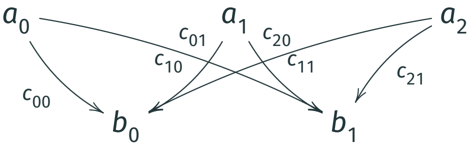
$$A_0B_0C_0 + A_1B_0C_1 + A_1B_1C_0 + A_2B_1C_1 = (A_0 - A_1)B_0C_0 + A_1(B_0 + B_1)(C_0 + C_1) + (A_2 - A_1)B_1C_1$$

Now collect the terms according to the C_i:

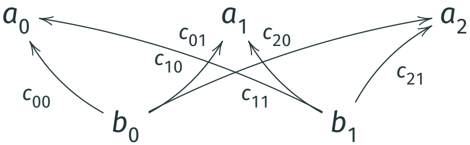
$$\begin{aligned} C_0 : A_0B_0 + A_1B_1 &= (A_0 - A_1)B_0 + A_1(B_0 + B_1) \\ C_1 : A_1B_0 + A_2B_1 &= A_1(B_0 + B_1) + (A_2 - A_1)B_1 \end{aligned}$$

Transposition of Linear Maps

A tagged arrow means to multiply by tag and add to target



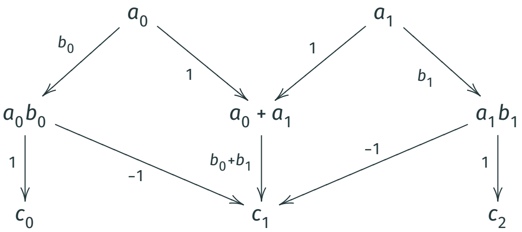
$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} c_{00} & c_{10} & c_{20} \\ c_{01} & c_{11} & c_{21} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix}$$



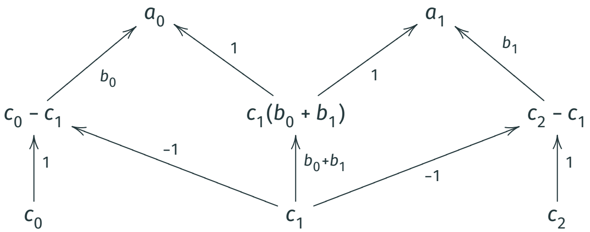
$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \\ c_{20} & c_{21} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

Transposition of Karatsuba

Transposition of usual polynomial product is Toeplitz-Matrix-to-Vector Product



$$
\begin{aligned}
c_0 &= a_0 b_0 \\
c_1 &= (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1 \\
c_2 &= a_1 b_1
\end{aligned}
$$



$$
\begin{aligned}
a_0 &= (c_0 - c_1)b_0 + c_1(b_0 + b_1) \\
a_1 &= c_1(b_0 + b_1) + (c_2 - c_1)b_1
\end{aligned}
$$

TMVP formulations for NTRU variants

$c = ab$ in NTRU Ring $\mathbb{Z}_q[x]/(x^p - 1)$ as TMVP

$$
\begin{array}{ccccccccccccc}
c_0 & = & a_0b_0 & + & a_1b_{p-1} & + & a_2b_{p-2} & + & \cdots & + & a_{p-2}b_2 & + & a_{p-1}b_1 \\
c_1 & = & a_0b_1 & + & a_1b_0 & + & a_2b_1 & + & \cdots & + & a_{p-2}b_3 & + & a_{p-1}b_2 \\
c_2 & = & a_0b_2 & + & a_1b_1 & + & a_2b_0 & + & \cdots & + & a_{p-2}b_4 & + & a_{p-1}b_3 \\
\vdots & & \vdots & & & & & & & & & & \vdots \\
c_{p-2} & = & a_0b_{p-2} & + & a_1b_{p-3} & + & a_2b_{p-4} & + & \cdots & + & a_{p-2}b_0 & + & a_{p-1}b_{p-1} \\
c_{p-1} & = & a_0b_{p-1} & + & a_1b_{p-2} & + & a_2b_{p-3} & + & \cdots & + & a_1b_{p-2} & + & a_{p-1}b_0
\end{array}
$$

$c = ab$ in NTRU Prime Ring $\mathbb{Z}_q[x]/(x^p - x - 1)$ as TMVP

$$
\begin{array}{ccccccccccccc}
c_0 + c_{p-1} & = & a_0(b_0 + b_{p-1}) & + & a_1(b_{p-1} + b_{p-2}) & + & a_2(b_{p-2} + b_{p-3}) & + & \cdots & + & a_{p-2}(b_2 + b_1) & + & a_{p-1}(b_1 + b_0 + b_{p-1}) \\
c_1 & = & a_0b_1 & + & a_1(b_0 + b_{p-1}) & + & a_2(b_1 + b_{p-2}) & + & \cdots & + & a_{p-2}(b_3 + b_2) & + & a_{p-1}(b_2 + b_1) \\
c_2 & = & a_0b_2 & + & a_1b_1 & + & a_2(b_0 + b_{p-1}) & + & \cdots & + & a_{p-2}(b_4 + b_3) & + & a_{p-1}(b_3 + b_2) \\
\vdots & & \vdots & & & & & & & & & & \vdots \\
c_{p-2} & = & a_0b_{p-2} & + & a_1b_{p-3} & + & a_2b_{p-4} & + & \cdots & + & a_{p-2}(b_0 + b_{p-1}) & + & a_{p-1}(b_{p-1} + b_{p-2}) \\
c_{p-1} & = & a_0b_{p-1} & + & a_1b_{p-2} & + & a_2b_{p-3} & + & \cdots & + & a_1b_{p-2} & + & a_{p-1}(b_0 + b_{p-1})
\end{array}
$$

Any Questions?

Applying Toom-4 to $f(x)^2$, $f(x) = -1 - 2x - 3x^2 - 4x^3 + 4x^4 + 3x^5 + 2x^6 + x^7$

$$[(-1 - 2x) + (-3 - 4x)y + (4 + 3x)y^2 + (2 + x)y^3] = F(x, y) = G(x, y)$$

Applying Toom-4 to $f(x)^2$, $f(x) = -1 - 2x - 3x^2 - 4x^3 + 4x^4 + 3x^5 + 2x^6 + x^7$

$$[(-1 - 2x) + (-3 - 4x)y + (4 + 3x)y^2 + (2 + x)y^3] = F(x, y) = G(x, y)$$

y_0		$H(y_0) := F(x, y_0) \cdot G(x, y_0)$

Applying Toom-4 to $f(x)^2$, $f(x) = -1 - 2x - 3x^2 - 4x^3 + 4x^4 + 3x^5 + 2x^6 + x^7$

$$[(-1 - 2x) + (-3 - 4x)y + (4 + 3x)y^2 + (2 + x)y^3] = F(x, y) = G(x, y)$$

y_0		$H(y_0) := F(x, y_0) \cdot G(x, y_0)$
0	$H(0)$	$(-1 - 2x)^2 = 1 + 4x + 4x^2$
1	$H(1)$	$(2 - 2x)^2 = 4 - 8x + 4x^2$
2	$H(2)$	$(25 + 10x)^2 = 625 + 500x + 100x^2$
∞	$H(\infty)$	$(2 + x)^2 = 4 + 4x + x^2$
-1	$H(-1)$	$(4 + 4x)^2 = 16 + 32x + 16x^2$
-2	$H(-2)$	$(5 + 10x)^2 = 25 + 100x + 100x^2$
-3	$H(-3)$	$(-10 + 10x)^2 = 100 - 200x + 100x^2$

Applying Toom-4 (cont'd)

Write $H = c_0(x) + c_1(x)y + \cdots + c_6(x)y^6$

$$\begin{bmatrix} c_0(x) \\ c_1(x) \\ c_2(x) \\ c_3(x) \\ c_4(x) \\ c_5(x) \\ c_6(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 & 64 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -2 & 4 & -8 & 16 & -32 & 64 \\ 1 & -3 & 9 & -27 & 81 & -243 & 729 \end{bmatrix}^{-1} \begin{bmatrix} H(0) \\ H(1) \\ H(2) \\ H(\infty) \\ H(-1) \\ H(-2) \\ H(-3) \end{bmatrix} = \begin{bmatrix} 1 + 4x + 4x^2 \\ 6 + 20x + 16x^2 \\ 1 + 2x + 4x^2 \\ -28 - 60x - 28x^2 \\ 4 + 2x + x^2 \\ 16 + 20x + 6x^2 \\ 4 + 4x + x^2 \end{bmatrix}$$

Applying Toom-4 (cont'd)

Write $H = c_0(x) + c_1(x)y + \cdots + c_6(x)y^6$

$$\begin{bmatrix} c_0(x) \\ c_1(x) \\ c_2(x) \\ c_3(x) \\ c_4(x) \\ c_5(x) \\ c_6(x) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 & 64 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -2 & 4 & -8 & 16 & -32 & 64 \\ 1 & -3 & 9 & -27 & 81 & -243 & 729 \end{bmatrix}^{-1} \begin{bmatrix} H(0) \\ H(1) \\ H(2) \\ H(\infty) \\ H(-1) \\ H(-2) \\ H(-3) \end{bmatrix} = \begin{bmatrix} 1 + 4x + 4x^2 \\ 6 + 20x + 16x^2 \\ 1 + 2x + 4x^2 \\ -28 - 60x - 28x^2 \\ 4 + 2x + x^2 \\ 16 + 20x + 6x^2 \\ 4 + 4x + x^2 \end{bmatrix}$$

$$\begin{aligned} f(x)g(x) = {} & 1 + 4x + (4+6)x^2 + 20x^3 + (16+1)x^4 + 2x^5 + (4-28)x^6 \\ & - 60x^7 + (-28+4)x^8 + 2x^9 + (1+16)x^{10} + 20x^{11} + (6+4)x^{12} + 4x^{13} + x^{14} \end{aligned}$$