Toom-Cook Multiplication and Toom-Cook TMVP

Mathematical Description with SageMath Demonstration

Cesare Huang Cheng Wei

Author Affiliation,
University of Author

July 12, 2024

Part I: Toom-Cook Multiplication

Part II: Toom-Cook TMVP

Part I

Toom-Cook Multiplication

Idea of Toom-Cook-3 Multiplication

Motivation

We want to compute the product $R(x)$ of degree 2 (length 3) polynomials $B(x)$ and $C(x)$.
Denote the polynomials by column vectors: If $B(x) = B_0 + B_1x + B_2x^2$, $C(x) = C_0 + C_1x + C_2x^2$ and $R(x) = R_0 + R_1x + R_2x^2 + R_3x^3 + R_4x^4$ then

$$B(x) = \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}, C(x) = \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} \text{ and } R(x) = \begin{bmatrix} R_0 \\ R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix}$$

Idea of Toom-Cook-3 Multiplication
Motivation

Since the result R has five coefficients, we can determine the polynomial R by five function values $R(s_i)$ for $i = 0, ..., 4$. This proccess is also known as "interpolation".
These function values

$$R(s_i) = B(s_i)C(s_i)$$

can be computed by function values of polynomial B and C.
And the function values $B(s_i)$ and $C(s_i)$ can be determined by simply evaluate polynomials B and C at s_i's.

Idea of Toom-Cook-3 Multiplication

Motivation

So far, we obtained a method to multiply polynomials:

1. Evaluate B and C at 5 points, $\{s_i\}$.
2. Compute $R(s_i) = B(s_i) \cdot C(s_i)$ for $i = 0, ..., 4$.
3. Interpolate R from the data $R(s_i)$'s.

These are the idea of Toom-Cook-3 multiplication. Let's dive into the detailed steps.

Idea of Toom-Cook-3 Multiplication

Detailed Steps

Our first step is "Evaluate B and C at 5 points, $\{s_i\}$". And we choose $\{s_i\} = \{0, 1, -1, 2, \infty\}$.
Here, $P(\infty)$ is defined as the leading coefficient of polynomial P.
This can be done by using the evaluation transform (matrix)[1]:

$$\begin{bmatrix} B(0) \\ B(1) \\ B(-1) \\ B(2) \\ B(\infty) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}$$

[1] Evaluation is itself a linear operation hence we can naturally write it as a matrix multiplication.

Idea of Toom-Cook-3 Multiplication

Detailed Steps

We will from now on denote the matrices of evaluations by **TC**'s.

$$\mathbf{TC}_{5\times 3} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix}, \quad \mathbf{TC}_{5\times 5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

So that

$$\begin{bmatrix} B(0) \\ B(1) \\ B(-1) \\ B(2) \\ B(\infty) \end{bmatrix} = \mathbf{TC}_{5\times 3} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \text{ and importantly } \begin{bmatrix} R(0) \\ R(1) \\ R(-1) \\ R(2) \\ R(\infty) \end{bmatrix} = \mathbf{TC}_{5\times 5} \begin{bmatrix} R_0 \\ R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix}$$

IDEA OF TOOM-COOK-3 MULTIPLICATION

DETAILED STEPS

Nextly, we do "Compute $R(s_i) = B(s_i) \cdot C(s_i)$ for $i = 0, ..., 4$"

$$\begin{bmatrix} R(0) \\ R(1) \\ R(-1) \\ R(2) \\ R(\infty) \end{bmatrix} = \begin{bmatrix} B(0)C(0) \\ B(1)C(1) \\ B(-1)C(-1) \\ B(2)C(2) \\ B(\infty)C(\infty) \end{bmatrix} = \begin{bmatrix} B(0) \\ B(1) \\ B(-1) \\ B(2) \\ B(\infty) \end{bmatrix} \odot \begin{bmatrix} C(0) \\ C(1) \\ C(-1) \\ C(2) \\ C(\infty) \end{bmatrix}$$

where $\odot$ denote the component-wise multiplication.
By using the matrices defined in the previous page, we can write the above equation as

$$\mathbf{TC}_{5\times 5} R = (\mathbf{TC}_{5\times 3} B) \odot (\mathbf{TC}_{5\times 3} C)$$

Idea of Toom-Cook-3 Multiplication

Detailed Steps

The last step is "Interpolate R from the data $R(s_i)$'s"
By the equation we just wrote

$$\mathbf{TC}_{5\times 5}R = (\mathbf{TC}_{5\times 3}B) \odot (\mathbf{TC}_{5\times 3}C)$$

this step is simply multiply both sides by $\mathbf{TC}_{5\times 5}^{-1}$:

$$\begin{aligned} \mathbf{TC}_{5\times 5}^{-1}(\mathbf{TC}_{5\times 5}R) &= \mathbf{TC}_{5\times 5}^{-1}((\mathbf{TC}_{5\times 3}B) \odot (\mathbf{TC}_{5\times 3}C)) \\ R &= \mathbf{TC}_{5\times 5}^{-1}((\mathbf{TC}_{5\times 3}B) \odot (\mathbf{TC}_{5\times 3}C)). \end{aligned}$$

Completes the computation.

Idea of Toom-Cook-3 Multiplication

Detailed Steps

$$R = \mathbf{TC}_{5\times 5}^{-1}\left((\mathbf{TC}_{5\times 3}B) \odot (\mathbf{TC}_{5\times 3}C)\right).$$

1. Evaluate B and C at 5 points, $\{s_i\}$.
2. Compute $R(s_i) = B(s_i) \cdot C(s_i)$ for $i = 0, ..., 4$.
3. Interpolate R from the data $R(s_i)$'s.

Idea of Toom-Cook-3 Multiplication

Demo for Toom-Cook-3

We use SageMath

Idea of Toom-Cook-k Multiplication

We can generalize the notion of Toom-Cook-3 into Toom-Cook-k.
We want to compute the product $R(x)$ of degree $k-1$ (length k) polynomials $B(x)$ and $C(x)$. Since the result $R(x)$ is of degree at most $2k-2$, we can interpolate $R(x)$ by $2k-1$ function values.

Idea of Toom-Cook-k Multiplication

Detailed Steps

The steps are similar to Toom-Cook-3 multiplication:

1. Evaluate B and C at $2k - 1$ points, $\{s_i\}$.
2. Compute $R(s_i) = B(s_i) \cdot C(s_i)$ for $i = 0, ..., 2k - 2$.
3. Interpolate R from the data $R(s_i)$'s.

Idea of Toom-Cook-k Multiplication

Detailed Steps

$$R = \mathbf{TC}^{-1}_{(2k-1)\times(2k-1)}\left(\left(\mathbf{TC}_{(2k-1)\times k} B\right) \odot \left(\mathbf{TC}_{(2k-1)\times k} C\right)\right).$$

1. Evaluate B and C at $2k-1$ points, $\{s_i\}$.
2. Compute $R(s_i) = B(s_i) \cdot C(s_i)$ for $i = 0, ..., 2k-2$.
3. Interpolate R from the data $R(s_i)$'s.

IDEA OF TOOM-COOK-k MULTIPLICATION

DETAIL FOR TOOM-COOK-5

So far, we have not made some description on choosing $\{s_i\}$'s. In principal, $\{s_i\}$'s are chosen such that the computation of **TC**'s are cheap.
Hence we select $\{0, 1, -1, 2, \infty\}$ in Toom-Cook-3 and the resulting **TC**'s involve only addition/subtraction and multiplication by powers of 2. And its inverse:

$$\mathbf{TC}_{5\times 5}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{3} & -\frac{1}{6} & 2 \\ -1 & \frac{1}{2} & \frac{1}{2} & 0 & -1 \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{6} & \frac{1}{6} & -2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

are also simple (excepts the division by 3).
But the situation is not trivial when we need more interpolation points. Hence we spend a subsection on Toom-Cook-5 multiplication.

Idea of Toom-Cook-k Multiplication

Detail for Toom-Cook-5

In Toom-Cook-5 multiplication, we need 9 interpolation points. A naive choice is $\{s_i\} = \{0, 1, -1, 2, -2, 3, -3, 4, \infty\}$. But then the resulting **TC** matrices will have very large entries. Now, the choise in the paper is $\{s_i\} = \left\{0, 1, -1, 2, -2, 3, \frac{1}{2}, -\frac{1}{2}, \infty\right\}$. A naive understanding of this will say that in the first step, the interpolation data

$$\begin{bmatrix} \vdots \\ B\left(\frac{1}{2}\right) \\ B\left(-\frac{1}{2}\right) \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \frac{1}{16} \\ 1 & -\frac{1}{2} & \frac{1}{4} & -\frac{1}{8} & \frac{1}{16} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix}$$

are computed. However, this produces division in the matrix.

So we will instead evaluate $2^4 B(\frac{1}{2})$ and $(-2)^4 B(-\frac{1}{2})$:

$$\begin{bmatrix} \vdots \\ 2^4 B\left(\frac{1}{2}\right) \\ (-2)^4 B\left(-\frac{1}{2}\right) \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots & \vdots \\ 16 & 8 & 4 & 2 & 1 \\ 16 & -8 & 4 & -2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix}$$

Idea of Toom-Cook-k Multiplication

Detail for Toom-Cook-5

The component-wise multiplication will yield

$$\begin{bmatrix} \vdots \\ 2^8 R\left(\frac{1}{2}\right) \\ (-2)^8 R\left(-\frac{1}{2}\right) \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ 2^4 B\left(\frac{1}{2}\right) \\ (-2)^4 B\left(-\frac{1}{2}\right) \\ \vdots \end{bmatrix} \odot \begin{bmatrix} \vdots \\ 2^4 C\left(\frac{1}{2}\right) \\ (-2)^4 C\left(-\frac{1}{2}\right) \\ \vdots \end{bmatrix}$$

and the final interpolation matrix will be

$$\begin{bmatrix} \vdots \\ 2^8 R\left(\frac{1}{2}\right) \\ (-2)^8 R\left(-\frac{1}{2}\right) \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 256 & 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 256 & -128 & 64 & -32 & 16 & -8 & 4 & -2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ \vdots \\ R_8 \end{bmatrix}.$$

Idea of Toom-Cook-k Multiplication
Demo for Toom-Cook-5

We use SageMath

Multilayer Toom-Cook Multiplication

Suppose we want to multiply degree 14 (length 15) polynomials.
One may consider using Toom-Cook-15 multiplication. But that requires 29 interpolation data, and leads to complicated **TC** and $\mathbf{TC}^{-1}$ matrices.
Rather, we propose a two-layer Toom-Cook multiplication method.

Multilayer Toom-Cook Multiplication

Firstly, we rewrite the polynomial B:

$$\begin{aligned}B(x) &= B_0 + B_1 x + B_2 x^2 + B_3 x^3 + B_4 x^4 + \cdots + B_{14} x^{14} \\ &= \left(B_0 + B_1 x + B_2 x^2\right) + \left(B_3 + B_4 x + B_5 x^2\right) y + \cdots + \left(B_{12} + B_{13} x + B_{14} x^2\right) y^4.\end{aligned}$$

and C:

$$C(x) = \left(C_0 + C_1 x + C_2 x^2\right) + \left(C_3 + C_4 x + C_5 x^2\right) y + \cdots + \left(C_{12} + C_{13} x + C_{14} x^2\right) y^4.$$

Multilayer Toom-Cook Multiplication

In vector representation:

$$B = \begin{bmatrix} B_0 + B_1 x + B_2 x^2 \\ B_3 + B_4 x + B_5 x^2 \\ \vdots \\ B_{12} + B_{13} x + B_{14} x^2 \end{bmatrix} = \begin{bmatrix} B_0 + B_1 x + B_2 x^2 \\ B_3 + B_4 x + B_5 x^2 \\ \vdots \\ B_{12} + B_{13} x + B_{14} x^2 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \\ \begin{bmatrix} B_3 \\ B_4 \\ B_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} B_{12} \\ B_{13} \\ B_{14} \end{bmatrix} \end{bmatrix} \text{ and } C = \begin{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} \\ \begin{bmatrix} C_3 \\ C_4 \\ C_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} C_{12} \\ C_{13} \\ C_{14} \end{bmatrix} \end{bmatrix}$$

Multilayer Toom-Cook Multiplication

We now perform the Toom-Cook-5 multiplication on

$$B = \begin{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \\ \begin{bmatrix} B_3 \\ B_4 \\ B_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} B_{12} \\ B_{13} \\ B_{14} \end{bmatrix} \end{bmatrix} \text{ and } C = \begin{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} \\ \begin{bmatrix} C_3 \\ C_4 \\ C_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} C_{12} \\ C_{13} \\ C_{14} \end{bmatrix} \end{bmatrix}$$

Multilayer Toom-Cook Multiplication

$$\left(\mathbf{TC}_{9\times 5} \begin{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \\ \begin{bmatrix} B_3 \\ B_4 \\ B_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} B_{12} \\ B_{13} \\ B_{14} \end{bmatrix} \end{bmatrix} \right) \text{ and } \left(\mathbf{TC}_{9\times 5} \begin{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} \\ \begin{bmatrix} C_3 \\ C_4 \\ C_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} C_{12} \\ C_{13} \\ C_{14} \end{bmatrix} \end{bmatrix} \right)$$

Multilayer Toom-Cook Multiplication

$$\left(\mathbf{TC}_{9\times 5} \begin{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \\ \begin{bmatrix} B_3 \\ B_4 \\ B_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} B_{12} \\ B_{13} \\ B_{14} \end{bmatrix} \end{bmatrix} \right) \odot \left(\mathbf{TC}_{9\times 5} \begin{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} \\ \begin{bmatrix} C_3 \\ C_4 \\ C_5 \end{bmatrix} \\ \vdots \\ \begin{bmatrix} C_{12} \\ C_{13} \\ C_{14} \end{bmatrix} \end{bmatrix} \right)$$

Multilayer Toom-Cook Multiplication

$$\mathbf{TC}_{9\times 9}^{-1}\left(\left(\mathbf{TC}_{9\times 5}\begin{bmatrix}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\\\begin{bmatrix}B_3\\B_4\\B_5\end{bmatrix}\\\vdots\\\begin{bmatrix}B_{12}\\B_{13}\\B_{14}\end{bmatrix}\end{bmatrix}\right)\odot\left(\mathbf{TC}_{9\times 5}\begin{bmatrix}\begin{bmatrix}C_0\\C_1\\C_2\end{bmatrix}\\\begin{bmatrix}C_3\\C_4\\C_5\end{bmatrix}\\\vdots\\\begin{bmatrix}C_{12}\\C_{13}\\C_{14}\end{bmatrix}\end{bmatrix}\right)\right)$$

MULTILAYER TOOM-COOK MULTIPLICATION

Let's go to the detail of point-wise multiplication: The evaluation matrix will produce the vector:

$$\begin{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \\ \\ \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} + \begin{bmatrix} B_3 \\ B_4 \\ B_5 \end{bmatrix} + \cdots + \begin{bmatrix} B_{12} \\ B_{13} \\ B_{14} \end{bmatrix} \\ \\ \vdots \end{bmatrix} \odot \begin{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} \\ \\ \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} + \begin{bmatrix} C_3 \\ C_4 \\ C_5 \end{bmatrix} + \cdots + \begin{bmatrix} C_{12} \\ C_{13} \\ C_{14} \end{bmatrix} \\ \\ \vdots \end{bmatrix}$$

Multilayer Toom-Cook Multiplication

The multiplication in the first entry is

$$\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} \times \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix}$$

It is just the polynomial multiplication

$$\left(B_0 + B_1 x + B_2 x^2\right) \left(C_0 + C_1 x + C_2 x^2\right)$$

One can use schoolbook multiplication or Toom-Cook-3 multiplication to complete this.

Multilayer Toom-Cook Multiplication

The multiplication in the second entry is

$$\left(\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} + \begin{bmatrix} B_3 \\ B_4 \\ B_5 \end{bmatrix} + \cdots + \begin{bmatrix} B_{12} \\ B_{13} \\ B_{14} \end{bmatrix}\right) \times \left(\begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} + \begin{bmatrix} C_3 \\ C_4 \\ C_5 \end{bmatrix} + \cdots + \begin{bmatrix} C_{12} \\ C_{13} \\ C_{14} \end{bmatrix}\right)$$

That is, by linearity (or simply the notion of addition)

$$\begin{bmatrix} B_0 + B_3 + \cdots + B_{12} \\ B_1 + B_4 + \cdots + B_{13} \\ B_2 + B_5 + \cdots + B_{14} \end{bmatrix} \times \begin{bmatrix} C_0 + C_3 + \cdots + C_{12} \\ C_1 + C_4 + \cdots + C_{13} \\ C_2 + C_5 + \cdots + C_{14} \end{bmatrix}$$

Then treat it as polynomial multiplication.

Multilayer Toom-Cook Multiplication

So each multiplication in point-wise multiplication are simply the (degree 2, length 3) polynomial multiplications, and can be done by Toom-Cook-3 (or schoolbook).
We choose Toom-Cook-3 and it is called multilayer Toom-Cook multiplication as a whole.
Now we also note that, after Toom-Cook-3, the result of point-wise multiplication is of degree 5, so

$$R = \mathbf{TC}_{9\times 9}^{-1} \begin{bmatrix} \text{(some degree 5 polynomial)} \\ \vdots \\ \text{(some degree 5 polynomial)} \end{bmatrix}$$

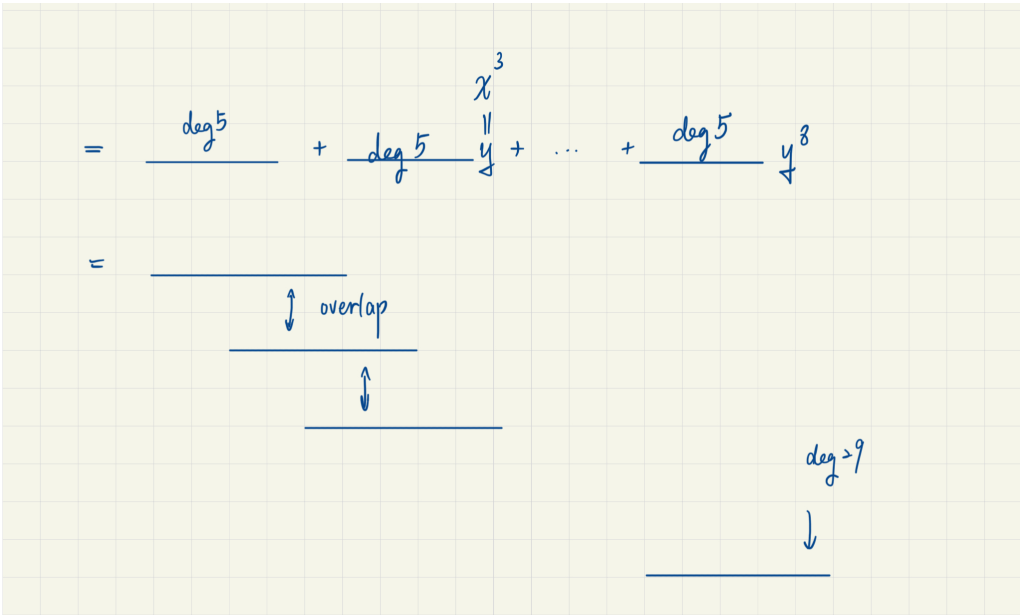
And it will yield the final result as:

$$R = \text{(degree 5 poly.)} + \text{(degree 5 poly.)}y + \cdots + \text{(degree 5 poly.)}y^8.$$

MULTILAYER TOOM-COOK MULTIPLICATION

Here we need to do some reduction:

$$R = (\text{degree 5 poly.}) + (\text{degree 5 poly.})y + \cdots + (\text{degree 5 poly.})y^8.$$



Part II

TOOM-COOK TMVP

What is TMVP?

Definition 1.1 (Toeplitz Matrix)

A Toeplitz matrix is the matrix of the form:

$$\begin{bmatrix} A_0 & A_{-1} & \cdots & A_{-(k-1)} \\ A_1 & A_0 & \cdots & A_{-(k-2)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & A_{k-2} & \cdots & A_0 \end{bmatrix}$$

Definition 1.2 (TMVP Toeplitz Matrix-Vector Product)

TMVP is a product of a Toeplitz matrix and a column vector

$$\begin{bmatrix} A_0 & A_{-1} & \cdots & A_{-(k-1)} \\ A_1 & A_0 & \cdots & A_{-(k-2)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & A_{k-2} & \cdots & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ \vdots \\ B_{k-1} \end{bmatrix}.$$

What is TMVP?

Why consider TMVP?
Recall the definition of weighted convolution, i.e., multiplications in the quotient ring

$$R/\langle x^n - \xi \rangle.$$

If $A = A_0 + A_1 x + \cdots + A_{n-1} x^{n-1}$ and $B = B_0 + B_1 x + \cdots + B_{n-1} x^{n-1}$, then their product is

$$C = \sum_{i=0}^{n} C_i x^i, \text{ where } C_i = \sum_{k=0}^{i} A_k B_{i-k} + \xi \sum_{k=i+1}^{n} A_k B_{n+i-k}.$$

What is TMVP?

Observe that the coefficients of their product

$$C = \sum_{i=0}^{n} C_i x^i, \text{ where } C_i = \sum_{k=0}^{i} A_k B_{i-k} + \xi \sum_{k=i+1}^{n} A_k B_{n+i-k}.$$

can be captured perfectly by a TMVP

$$\begin{bmatrix} C_0 \\ C_1 \\ \vdots \\ C_{n-1} \end{bmatrix} \begin{bmatrix} A_0 & \xi A_{n-1} & \cdots & \xi A_1 \\ A_1 & A_0 & \cdots & \xi A_2 \\ \vdots & \vdots & \ddots & \vdots \\ A_{n-1} & A_{n-2} & \cdots & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ \vdots \\ B_{n-1} \end{bmatrix}$$

We conclude that if we can compute TMVP efficiently, then we can compute weighted convolution (of course, including cyclic and negacyclic convolution) efficiently.

Examples of Fast Algorithm

Now we look at some Fast Algorithm on TMVP:
Consider decomposing the TMVP $A \cdot B$ as block matrices. Then a two-way decomposition

$$\begin{bmatrix} \mathbf{A}_0 & \mathbf{A}_{-1} \\ \mathbf{A}_1 & \mathbf{A}_0 \end{bmatrix} \begin{bmatrix} \mathbf{B}_0 \\ \mathbf{B}_1 \end{bmatrix} = \begin{bmatrix} \mathbf{A}_0\mathbf{B}_0 + \mathbf{A}_{-1}\mathbf{B}_1 \\ \mathbf{A}_1\mathbf{B}_0 + \mathbf{A}_0\mathbf{B}_1 \end{bmatrix} = \begin{bmatrix} (\mathbf{A}_0 + \mathbf{A}_{-1})\mathbf{B}_1 + \mathbf{A}_0(\mathbf{B}_0 - \mathbf{B}_1) \\ (\mathbf{A}_1 + \mathbf{A}_0)\mathbf{B}_0 - \mathbf{A}_0(\mathbf{B}_0 - \mathbf{B}_1) \end{bmatrix}$$

and a three way decomposition:

$$\begin{aligned} \begin{bmatrix} \mathbf{A}_0 & \mathbf{A}_{-1} & \mathbf{A}_{-2} \\ \mathbf{A}_1 & \mathbf{A}_0 & \mathbf{A}_{-1} \\ \mathbf{A}_2 & \mathbf{A}_1 & \mathbf{A}_0 \end{bmatrix} \begin{bmatrix} \mathbf{B}_0 \\ \mathbf{B}_1 \\ \mathbf{B}_2 \end{bmatrix} &= \begin{bmatrix} \mathbf{A}_0\mathbf{B}_0 + \mathbf{A}_{-1}\mathbf{B}_1 + \mathbf{A}_{-2}\mathbf{B}_2 \\ \mathbf{A}_1\mathbf{B}_0 + \mathbf{A}_0\mathbf{B}_1 + \mathbf{A}_{-1}\mathbf{B}_2 \\ \mathbf{A}_2\mathbf{B}_0 + \mathbf{A}_1\mathbf{B}_1 + \mathbf{A}_0\mathbf{B}_2 \end{bmatrix} \\ &= \begin{bmatrix} (\mathbf{A}_0 + \mathbf{A}_{-1} + \mathbf{A}_{-2})\,\mathbf{B}_2 + \mathbf{A}_{-1}(\mathbf{B}_1 - \mathbf{B}_2) - \mathbf{A}_0(\mathbf{B}_2 - \mathbf{B}_0) \\ (\mathbf{A}_1 + \mathbf{A}_0 + \mathbf{A}_{-1})\,\mathbf{B}_1 + \mathbf{A}_1(\mathbf{B}_0 - \mathbf{B}_1) - \mathbf{A}_{-1}(\mathbf{B}_1 - \mathbf{B}_2) \\ (\mathbf{A}_2 + \mathbf{A}_1 + \mathbf{A}_0)\,\mathbf{B}_0 + \mathbf{A}_0(\mathbf{B}_2 - \mathbf{B}_0) - \mathbf{A}_1(\mathbf{B}_0 - \mathbf{B}_1) \end{bmatrix} \end{aligned}$$

The three way decomposition formula allow us to complete the full TMVP with only six $\frac{1}{3}$-size TMVP.

Examples of Fast Algorithm

However, there exists a fast algorithm that completes the full TMVP with only five $\frac{1}{3}$-size TMVP:

$$
\begin{aligned}
P_0 &= \left(-A_0 + \frac{1}{2}A_{-1} - \frac{1}{2}A_1 + A_2\right) B_0 \\
P_1 &= \left(\frac{1}{2}A_0 - \frac{1}{2}A_{-1} + A_1\right)(B_0 + B_1 + B_2) \\
P_2 &= \left(\frac{1}{2}A_0 - \frac{1}{6}A_{-1} - \frac{1}{3}A_1\right)(B_0 - B_1 + B_2) \\
P_3 &= \left(\frac{1}{6}A_{-1} - \frac{1}{6}A_1\right)(B_0 + 2B_1 + 4B_2) \\
P_4 &= (-A_0 - 2A_{-1} + A_{-2} + 2A_1)(B_2)
\end{aligned}
$$

and

$$
\begin{bmatrix} A_0 & A_{-1} & A_{-2} \\ A_1 & A_0 & A_{-1} \\ A_2 & A_1 & A_0 \end{bmatrix}
\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}
=
\begin{bmatrix} P_0 + P_1 + P_2 + P_3 \\ P_1 - P_2 + 2P_3 \\ P_1 + P_2 + 4P_3 + P_4 \end{bmatrix}
$$

In the next section, we derive a general procedure that completes the full TMVP by $2k - 1$ $\frac{1}{k}$-size TMVP.

Derivation of Toom-Cook-3 Fast Algorithm

We first derive the above mentioned 3-way TMVP. The coefficients suggest that the derivation of that formula is heavily related to Toom-Cook multiplication.
Let's recall the Toom-Cook-3 multiplication:

$$R = \mathbf{TC}_{5\times 5}^{-1}\left((\mathbf{TC}_{5\times 3}B) \odot (\mathbf{TC}_{5\times 3}C)\right)$$

First we note that

$$R = \begin{bmatrix} R_0 \\ R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix} = \begin{bmatrix} B_0C_0 & & & & \\ B_1C_0 & + & B_0C_1 & & \\ B_2C_0 & + & B_1C_1 & + & B_0C_2 \\ & & B_2C_1 & + & B_1C_2 \\ & & & & B_2C_2 \end{bmatrix}$$

Derivation of Toom-Cook-3 Fast Algorithm

Multiply this R vector by $\vec{A} = \begin{bmatrix} A_2 & A_1 & A_0 & A_{-1} & A_{-2} \end{bmatrix}$.

$$\begin{bmatrix} A_2 & A_1 & A_0 & A_{-1} & A_{-2} \end{bmatrix} \begin{bmatrix} B_0 C_0 & & & & \\ B_1 C_0 & + & B_0 C_1 & & \\ B_2 C_0 & + & B_1 C_1 & + & B_0 C_2 \\ & & B_2 C_1 & + & B_1 C_2 \\ & & & & B_2 C_2 \end{bmatrix}$$

Then we have:

$$\begin{aligned} \text{coefficient of } C_0 &= A_2 B_0 + A_1 B_1 + A_0 B_2 \\ \text{coefficient of } C_1 &= A_1 B_0 + A_0 B_1 + A_{-1} B_2 \\ \text{coefficient of } C_2 &= A_0 B_0 + A_{-1} B_1 + A_{-2} B_2 \end{aligned}$$

which is just the reversed column vector of

$$\begin{bmatrix} A_0 & A_{-1} & A_{-2} \\ A_1 & A_0 & A_{-1} \\ A_2 & A_1 & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} A_0 B_0 + A_{-1} B_1 + A_{-2} B_2 \\ A_1 B_0 + A_0 B_1 + A_{-1} B_2 \\ A_2 B_0 + A_1 B_1 + A_0 B_2 \end{bmatrix}$$

Derivation of Toom-Cook-3 Fast Algorithm

Hence in right hand side,

$$\vec{A}\mathbf{TC}_{5\times5}^{-1}\left((\mathbf{TC}_{5\times3}B)\odot(\mathbf{TC}_{5\times3}C)\right)$$

its C_0 entry, C_1 entry and C_2 entry are reversed column vector elements of

$$\begin{bmatrix} A_0 & A_{-1} & A_{-2} \\ A_1 & A_0 & A_{-1} \\ A_2 & A_1 & A_0 \end{bmatrix}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} A_0B_0 + A_{-1}B_1 + A_{-2}B_2 \\ A_1B_0 + A_0B_1 + A_{-1}B_2 \\ A_2B_0 + A_1B_1 + A_0B_2 \end{bmatrix}$$

Let's focus on C_0's coefficients, it is finded by letting $C_0 = 1$ and $C_{\text{others}} = 0$:

$$C_0\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}\right)\odot\left(\mathbf{TC}_{5\times3}\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\right)\right)$$

Derivation of Toom-Cook-3 Fast Algorithm

$$C_0\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot\left(\mathbf{TC}_{5\times3}\begin{bmatrix}1\\0\\0\end{bmatrix}\right)\right)$$

and similarly

$$C_1\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot\left(\mathbf{TC}_{5\times3}\begin{bmatrix}0\\1\\0\end{bmatrix}\right)\right)$$

$$C_2\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot\left(\mathbf{TC}_{5\times3}\begin{bmatrix}0\\0\\1\end{bmatrix}\right)\right)$$

Derivation of Toom-Cook-3 Fast Algorithm

$$C_0\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}\right) \odot \left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}\right)\right)$$

$$C_1\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}\right) \odot \left(\begin{bmatrix} 0 \\ 1 \\ -1 \\ 2 \\ 0 \end{bmatrix}\right)\right)$$

$$C_2\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}\right) \odot \left(\begin{bmatrix} 0 \\ 1 \\ 1 \\ 4 \\ 1 \end{bmatrix}\right)\right)$$

Derivation of Toom-Cook-3 Fast Algorithm

Let $e_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ and $e_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, etc.. Then

$$C_0\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}\right) \odot \left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}\right)\right)$$

can be rewritten as

$$C_0\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix}\right) \odot (e_0 + e_1 + e_2 + e_3)\right)$$

Derivation of Toom-Cook-3 Fast Algorithm

And by linearity

$$C_0\text{'s coefficient} = \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_0\right) + \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_1\right)$$
$$+ \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_2\right) + \vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_3\right)$$

Hence we conclude that each of three coefficients can be written as a linear combination of the following materials

$$\vec{A}\mathbf{TC}_{5\times 5}^{-1}\left(\left(\mathbf{TC}_{5\times 3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_i\right) \text{ for } i = 0, 1, 2, 3, 4.$$

And it follows that five $\frac{1}{3}$-size TMVP are sufficient for the full TMVP.

Derivation of Toom-Cook-3 Fast Algorithm

We go through the detailed computation of TMVP-TC-3. Put

$$\mathrm{COMPONENT} = \begin{bmatrix} \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_0\right) \\ \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_1\right) \\ \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_2\right) \\ \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_3\right) \\ \vec{A}\mathbf{TC}_{5\times5}^{-1}\left(\left(\mathbf{TC}_{5\times3}\begin{bmatrix}B_0\\B_1\\B_2\end{bmatrix}\right)\odot e_4\right) \end{bmatrix}$$

Derivation of Toom-Cook-3 Fast Algorithm

Then

$$\begin{bmatrix} A_0B_0 + A_{-1}B_1 + A_{-2}B_2 \\ A_1B_0 + A_0B_1 + A_{-1}B_2 \\ A_2B_0 + A_1B_1 + A_0B_2 \end{bmatrix} = \underbrace{\begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}}_{\text{reverse}} \underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & -1 & 2 & 0 \\ 0 & 1 & 1 & 4 & 1 \end{bmatrix}}_{\mathbf{TC}^T_{5\times 3}} \text{COMPONENT}.$$

Derivation of Toom-Cook-k Fast Algorithm

We now want to generalize our idea to k-way decomposition formula for

$$\begin{bmatrix} A_0 & A_{-1} & \cdots & A_{-(k-1)} \\ A_1 & A_0 & \cdots & A_{-(k-2)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & A_{k-1} & \cdots & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ \vdots \\ B_{k-1} \end{bmatrix}.$$

Derivation of Toom-Cook-k Fast Algorithm

Begin from the Toom-Cook multiplication:

$$R = \mathbf{TC}^{-1}_{(2k-1)\times(2k-1)} \left(\left(\mathbf{TC}_{(2k-1)\times k} B \right) \odot \left(\mathbf{TC}_{(2k-1)\times k} C \right) \right)$$

Multiply the both sides by the row vector

$$\vec{A} = \begin{bmatrix} A_{k-1} & A_{k-2} & \cdots & A_{-(k-1)} \end{bmatrix}.$$

Derivation of Toom-Cook-k Fast Algorithm

Let's look at the C_{i_0} coefficient of the left-hand side

$$C_{i_0}\text{'s coefficient} = A_{-k+i_0+1}B_0 + A_{-k+i_0+2}B_1 + \cdots + A_{i_0}B_{k-1}$$

which is the last ith component of in the

$$\begin{bmatrix} A_0 & A_{-1} & \cdots & A_{-(k-1)} \\ A_1 & A_0 & \cdots & A_{-(k-2)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & A_{k-1} & \cdots & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ \vdots \\ B_{k-1} \end{bmatrix}.$$

Derivation of Toom-Cook-k Fast Algorithm

So the C_{i_0}'s coefficient of the

$$\vec{A}\mathbf{TC}^{-1}_{(2k-1)\times(2k-1)}\left(\left(\mathbf{TC}_{(2k-1)\times k}B\right)\odot\left(\mathbf{TC}_{(2k-1)\times k}C\right)\right)$$

is the last ith component of in the

$$\begin{bmatrix} A_0 & A_{-1} & \cdots & A_{-(k-1)} \\ A_1 & A_0 & \cdots & A_{-(k-2)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & A_{k-1} & \cdots & A_0 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ \vdots \\ B_{k-1} \end{bmatrix}.$$

Derivation of Toom-Cook-k Fast Algorithm

The C_{i_0}'s coefficient of the

$$\vec{A}\mathbf{TC}^{-1}_{(2k-1)\times(2k-1)}\left(\left(\mathbf{TC}_{(2k-1)\times k}B\right)\odot\left(\mathbf{TC}_{(2k-1)\times k}C\right)\right)$$

is

$$\vec{A}\mathbf{TC}^{-1}_{(2k-1)\times(2k-1)}\left(\left(\mathbf{TC}_{(2k-1)\times k}B\right)\odot\left(\mathbf{TC}_{(2k-1)\times k}\begin{bmatrix}0\\\vdots\\1\\\vdots\\0\end{bmatrix}\right)\right).$$

Derivation of Toom-Cook-k Fast Algorithm

$$\vec{A}\mathbf{TC}^{-1}_{(2k-1)\times(2k-1)}\left(\left(\mathbf{TC}_{(2k-1)\times k}B\right)\odot\left(\mathbf{TC}_{(2k-1)\times k}\begin{bmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{bmatrix}\right)\right).$$

By multiplying the blue part out, we can again write this expression as a linear combination of

$$\vec{A}\mathbf{TC}^{-1}_{(2k-1)\times(2k-1)}\left(\left(\mathbf{TC}_{(2k-1)\times k}B\right)\odot e_i\right)\ \text{for } i=0,1,\dots,2k-2$$

From here, we conclude that we can perform the full TMVP computation by computing $2k-1$ $\frac{1}{k}$-size TMVP.

Final Remark

The speed up of ratio

$$\frac{k^2}{2k-1}$$

looks very good. But please note that the formula is based on Toom-Cook multiplication which involves choosing $\{s_i\}$, the interpolation points. When we choose a large k, the resulting **TC** and $\mathbf{TC}^{-1}$ matrices will be complicated and hence slow down the process.
In the paper, two multiplication methods in the ring

$$\mathbb{Z}_{2048}/\left\langle x^{677}-1\right\rangle$$

are proposed:
Multilayer Toom-Cook and Multilayer TMVP-Toom-Cook both with the splitting sequence 5 -> 3 -> 3 -> 2.

Final Remark