Talker: 張志謙

PQC Final Report

2022/6/17

Toom-cook

Definition:
要計算兩個多項式$A(x), B(x)$，分別將其分成k部分（每部分長度固定），再對這些部分執行運算。隨著k的增長，可以組合許多乘法子運算，從而降低算法的整體複雜度，然後再次使用$Toom-k$算法遞歸計算乘法子運算，依此類推。
流程:

1. 拆分&求值$\Rightarrow$ Linear Transformation
2. 點乘
3. 插值$\Rightarrow$ Linear Transformation

Toom-cook

拆分&求值:

Let $A(x)=a_{n-1}x^{n-1}+,...,a_0, B(x)=b_{n-1}x^{n-1}+,...,b_0$,and we set $y=x^{\frac{n}{k}}$,

$\alpha_{k-1}=a_{n-1}x^{\frac{n}{k}-1}+...+a_{n-\frac{n}{k}}, \alpha_{k-2}=a_{n-1-\frac{n}{k}}x^{\frac{n}{k}-1}+...+a_{n-\frac{2n}{k}}, ...$

$\beta_{k-1}=b_{n-1}x^{\frac{n}{k}-1}+...+b_{n-\frac{n}{k}}, ...$

then $\begin{cases} A(y)=\alpha_{k-1}x^{k-1}+...\alpha_0 \\ B(y)=\beta_{k-1}x^{k-1}+...+\beta_0 \end{cases}$

Toom-cook

拆分&求值:

choose $2k-1$ points $p_0, ..., p_{2k-2}$ on $A(y)$

$$\begin{bmatrix} A(p_0) \\ A(p_1) \\ . \\ . \\ A(p_{2k-2}) \end{bmatrix} = \begin{bmatrix} (p_0)^0 & (p_0)^1 & ... & (p_0)^{k-1} \\ (p_1)^0 & (p_1)^1 & ... & (p_1)^{k-1} \\ ... & .... & ... & ... \\ (p_{2k-2})^0 & (p_{2k-2})^1 & ... & (p_{2k-2})^{k-1} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{k-1} \end{bmatrix}$$

Toom-cook

點乘: Let $C(x) = A(x) \times B(x)$,then

$$\begin{bmatrix} C(p_0) \\ C(p_1) \\ . \\ . \\ C(p_{2k-2}) \end{bmatrix} = \begin{bmatrix} A(p_0)B(p_0) \\ A(p_1)B(p_1) \\ . \\ . \\ A(p_{2k-2})B(p_{2k-2}) \end{bmatrix}$$

Toom-cook

插值:

Use $C(p_0), ..., C(p_{2k-2})$ to recover $C(y) = c_{2k-2}y^{2k-2}+, ..., c_0$

$$\begin{bmatrix} C(p_0) \\ C(p_1) \\ . \\ . \\ C(p_{2k-2}) \end{bmatrix} = \begin{bmatrix} (p_0)^0 & (p_0)^1 & \dots & (p_0)^{k-1} \\ (p_1)^0 & (p_1)^1 & \dots & (p_1)^{k-1} \\ \dots & \dots. & \dots & \dots \\ (p_{2k-2})^0 & (p_{2k-2})^1 & \dots & (p_{2k-2})^{k-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ . \\ . \\ c_{2k-2} \end{bmatrix}$$

Toom-cook

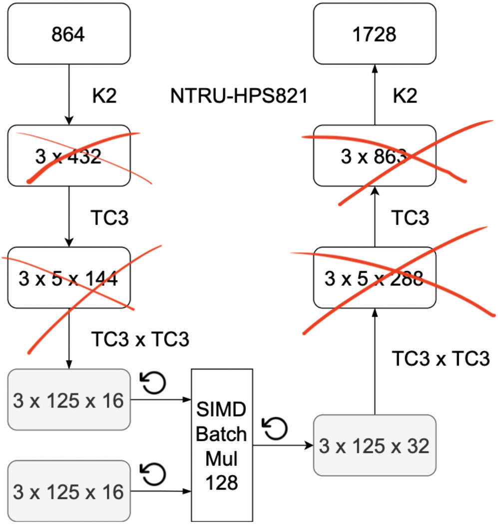
插值:

Use $C(p_0), ..., C(p_{2k-2})$ to recover $C(y) = c_{2k-2}y^{2k-2} +, ..., c_0$

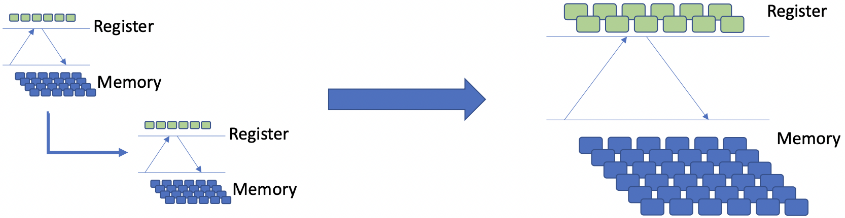
$$\begin{bmatrix} c_0 \\ c_1 \\ . \\ . \\ c_{2k-2} \end{bmatrix} =$$

$$\begin{bmatrix} (p_0)^0 & (p_0)^1 & \dots & (p_0)^{k-1} \\ (p_1)^0 & (p_1)^1 & \dots & (p_1)^{k-1} \\ \dots & .... & \dots & \dots \\ (p_{2k-2})^0 & (p_{2k-2})^1 & \dots & (p_{2k-2})^{k-1} \end{bmatrix}^{-1} \begin{bmatrix} C(p_0) \\ C(p_1) \\ . \\ . \\ C(p_{2k-2}) \end{bmatrix}$$

Improvement



Improvement



Improvement

Consider all column vectors in

$$\begin{bmatrix} (p_0)^0 & (p_0)^1 & \dots & (p_0)^{k-1} \\ (p_1)^0 & (p_1)^1 & \dots & (p_1)^{k-1} \\ \dots & \dots. & \dots & \dots \\ (p_{2k-2})^0 & (p_{2k-2})^1 & \dots & (p_{2k-2})^{k-1} \end{bmatrix}:$$

if $\forall i, j$ satisfy $p_i \neq p_j$,then these vectors are independent. Hence, Toom-Cook multiplication and interpolation are fundamentally linear maps of the form:

$$\begin{cases} \mathrm{TC}_k : R^{k}_{\frac{n}{k}-1}(x) \to R^{2k-1}_{\frac{n}{k}-1}(x) \\ \mathrm{TC}_k^{-1} : R^{2k-1}_{\frac{2n}{k}-2}(x) \to R^{2k-1}_{\frac{2n}{k}-2}(x) \end{cases}$$

Improvement

- $\hat{TC}(A(x)) = TC_{k_\eta}(TC_{k_{\eta-1}}(\ldots TC_{k_1}(A(x))))$
- $\theta = \hat{TC}(A(x)) * \hat{TC}(B(x))$
- $C(x) = TC_{k_1}^{-1}(TC_{k_2}^{-1}(\ldots TC_{k_\eta}^{-1}(\theta)))$

Improvement

Definition:

$$O_n = \begin{bmatrix} 0 & \dots & 0 \\ . & \dots & . \\ . & \dots & . \\ 0 & \dots & 0 \end{bmatrix}_{n \times n}, I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & \dots & \dots & . \\ . & \dots & \dots & . \\ 0 & \dots & \dots & 1 \end{bmatrix}_{n \times n},$$

$$\mathrm{T}_n = \begin{bmatrix} I_n & \\ I_n & I_n \\ & I_n \end{bmatrix}_{3n \times 2n}$$

Improvement

$$T_{\frac{n}{2}} = \begin{bmatrix} I_{\frac{n}{2}} & \\ I_{\frac{n}{2}} & I_{\frac{n}{2}} \\ & I_{\frac{n}{2}} \end{bmatrix}_{\frac{3}{2}n\times n}$$

$$\Rightarrow \begin{bmatrix} T_{\frac{n}{4}} & & \\ & T_{\frac{n}{4}} & \\ & & T_{\frac{n}{4}} \end{bmatrix}_{\frac{3}{2}n\times n} \qquad T_{\frac{n}{2}} =$$

$$\begin{bmatrix} I_{\frac{n}{4}} & & & & & \\ I_{\frac{n}{4}} & I_{\frac{n}{4}} & & & & \\ & I_{\frac{n}{4}} & & & & \\ & & I_{\frac{n}{4}} & & & \\ & & I_{\frac{n}{4}} & I_{\frac{n}{4}} & & \\ & & & I_{\frac{n}{4}} & & \\ & & & & I_{\frac{n}{4}} & \\ & & & & I_{\frac{n}{4}} & I_{\frac{n}{4}} \\ & & & & & I_{\frac{n}{4}} \end{bmatrix}_{\frac{9}{4}n\times\frac{3}{2}n} \begin{bmatrix} I_{\frac{n}{2}} & \\ I_{\frac{n}{2}} & I_{\frac{n}{2}} \\ & I_{\frac{n}{2}} \end{bmatrix}_{\frac{3}{2}n\times n}$$

Reference

Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography