Toom-Cook and FFT

Noelia Sánchez Ruiz

Universitat de Barcelona

7th April 2022

Toom-Cook

- It's a generalization of Karatsuba's multiplication.
- Toom-Cook divides the degree's bound of the input polynomials by 3 or more.
- Idea: Evaluate $P(X)$ and $Q(X)$ at some points, multiply these values, interpolate.
- Example: Toom-3.

Toom- 3

- P and Q of degrees $< n = 3^k$.
- $N = \frac{n}{3} = 3^{k-1}$.
- Objective: Do the product multiplying polynomials of degree $< N$.

$$\begin{cases} P = P_2 X^{2N} + P_1 X^N + P_0 \\ Q = Q_2 X^{2N} + Q_1 X^N + Q_0 \end{cases} \text{ with } \deg(P_i) \text{ and } \deg(Q_i) < N$$

How many points?

$$\begin{cases} \Pi_0 = P_0 Q_0 \\ \Pi_1 = (P_2 + P_1 + P_0)(Q_2 + Q_1 + Q_0) \\ \Pi_{-1} = (P_2 + (-1)^N P_1 + P_0)(Q_2 + (-1)^N Q_1 + Q_0) \\ \Pi_2 = (2^{2N} P_2 + 2^N P_1 + P_0)(2^{2N} Q_2 + 2^N Q_1 + Q_0) \\ \Pi_\infty = P_2 Q_2 \end{cases}$$

A polynomial of degree α is uniquely determined by $\alpha + 1$ points.

The product

$$\begin{cases} \Pi = \sum_{i=0}^{4} R_i X^{iN} \\ \Pi_\alpha = \sum_{i=0}^{4} R_i \alpha^{iN} \text{ if } \alpha \in \{0, 1, -1, 2\} \\ \Pi_\infty = R_4. \end{cases}$$

We define $R_m = \sum_{0 \leq i,j \leq 2 | i+j=m} P_i Q_j$, where $\deg(R_m) < 2N - 1$

The product

$$
\begin{aligned}
R_1 &= \Pi_1 - \Pi_0 - \Pi_\infty - R_2 - R_3 \\
R_2 &= \frac{\Pi_{-1} - 2\Pi_0 + \Pi_1 - 2\Pi_\infty}{2} \\
R_3 &= \frac{\Pi_2 + (2^{2N} - 1)}{2^{3N} - 2^N}\Pi_0 \\
&\quad + \frac{(2^{N-1} - 2^N - 2^{2N-1})}{2^{3N} - 2^N}\Pi_1 \\
&\quad + \frac{(2^{2N} - 2^{4N})}{2^{3N} - 2^N}\Pi_\infty \\
&\quad + \frac{(2^{2N-1} - 2^{N-1})}{2^{3N} - 2^N}\Pi_{-1}
\end{aligned}
$$

The product can be done by means of 5 products of two polynomials of degree $< N$.

Algebraic Complexity

$$
\begin{aligned}
T(n) = T(3^k) &= 5(5T(3^{k-1}) + C3^{m-1}) + C3^m \\
&= 5^2 T(3^{m-1}) + C3^m + 5 \cdot 3^{m-1} \cdot C \\
&= \cdots \\
&= 5^m T(1) + 3^m C \left(1 + 5 + \cdots + \left(\frac{5}{3}\right)^{m-1}\right) \\
&= 5^m + 3^m C \frac{(5/3)^m - 1}{2/3} \\
&= 5^m + C\left(\frac{3 \cdot 5^m - 3^{m+1}}{2}\right) \\
&\approx \hat{C} 5^m \\
&= \hat{C} 3^{n^{\log_3 5}} \\
&= O(n^{\log_3 5})
\end{aligned}
$$

$n < N^k$ with $N \geq 3$

- $2(N-1)+1 = 2N-1$ points are needed.
- $\Pi = \sum_{i=0}^{2N-1} R_i X^{iN}$
- Write R_i as a combination of the differents Π_α.
- Only $2N-1$ products are needed to compute the product of $P \cdot Q$

Fast Fourier Transform

Discrete Fourier Transform

Let $n = 2^k$ with $k > 0$, $\mathbb{C}$ the commutative ring. Let $\omega = e^{\frac{2\pi i}{n}}$, $R = \sum R_j X^j \in \mathbb{C}[X]$ with degree $< n$. Let $R = (R_0, \ldots, R_{n-1}) \in \mathbb{C}^n$.

$$DFT_\omega(R) = (R(1), R(\omega), \ldots, R(\omega^{n-1}))$$

is called the Discrete Fourier Transform.

Fast Fourier Transform

- A fast way to compute DFT is by FFT.
- Compute two DFT's of polynomials of degrees $< n/2$

$$\begin{cases} R(\omega^p) = \sum_{j=0}^{m-1} R_{2j}\alpha^j p + \omega^p \sum_{j=0}^{m-1} R_{2j+1}\alpha^{jp} \\ R(\omega^{p+m}) = \sum_{j=0}^{m-1} R_{2j}\alpha^{jp} - \omega^p \sum_{j=0}^{m-1} R_{2j+1}\alpha^{jp} \end{cases}$$

with $0 \leq p < m$ and $\alpha = \omega^2$.