Week 03

THE FAST FOURIER TRANSFORM

大数乘法的时候，分成n份会导致x_i^n 计算复杂度过高......

Our strategy to multiply polynomials fast:

- Given two polynomials of degree at most n,

$$P_A(x) = A_n x^n + \ldots + A_0; \qquad P_B(x) = B_n x^n + \ldots + B_0$$

1. convert them into value representation at $2n+1$ distinct points $x_0, x_1, \ldots, x_{2n}$:

$$P_A(x) \leftrightarrow \{(x_0, P_A(x_0)), (x_1, P_A(x_1)), \ldots, (x_{2n}, P_A(x_{2n}))\}$$
$$P_B(x) \leftrightarrow \{(x_0, P_B(x_0)), (x_1, P_B(x_1)), \ldots, (x_{2n}, P_B(x_{2n}))\}$$

2. multiply them point by point using $2n+1$ multiplications:

$$\Big\{(x_0, \underbrace{P_A(x_0)P_B(x_0)}_{P_C(x_0)}),\ \ (x_1, \underbrace{P_A(x_1)P_B(x_1)}_{P_C(x_1)}), \ldots, (x_{2n}, \underbrace{P_A(x_{2n})P_B(x_{2n})}_{P_C(x_{2n})})\Big\}$$

3. Convert such value representation of $P_C(x)$ to its coefficient form

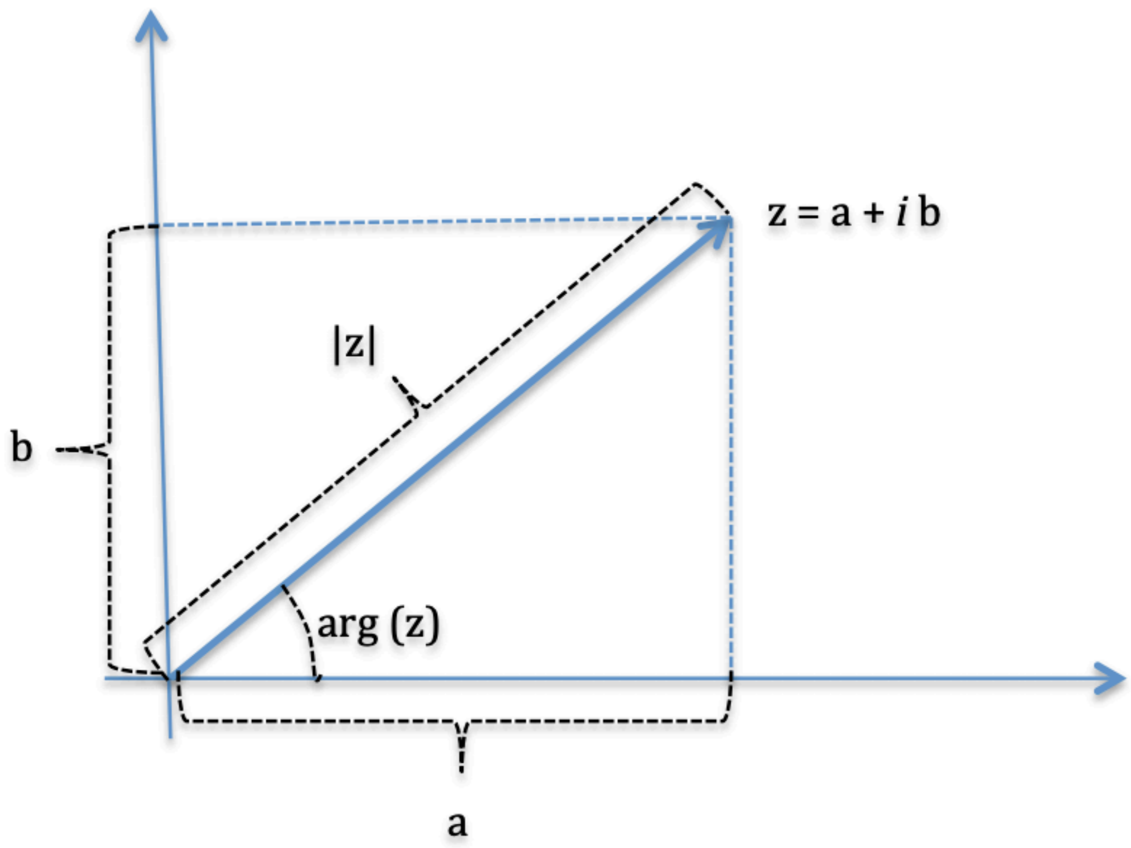
$$P_C(x) = C_{2n}x^{2n} + C_{2n-1}x^{2n-1} + \ldots + C_1 x + C_0;$$

- **Key Question:** What values should we take for $x_0, \ldots, x_{2n}$ to avoid "explosion" of size when we evaluate x_i^n while computing $P_A(x_i) = A_0 + A_1 x + \ldots + A_n x_i^n$?

Complex number revisited

复数的复习

Complex numbers $z = a + ib$ can be represented using their modulus $|z| = \sqrt{a^2 + b^2}$ and their argument, $arg(z)$, which is an angle taking values in $(-\pi, \pi]$ and satisfying:
$z = |z|e^{i\arg(z)} = |z|(\cos\arg(z) + i\sin\arg(z))$,



Complex roots of unity

Roots of unity of order n are complex numbers which satisfy $z^n = 1$.

If $z^n = |z|^n(\cos(n\arg(z)) + i\sin(n\arg(z))) = 1$ then $|z| = 1$ and $n\arg(z)$ is a multiple of 2π; Thus, $n\arg(z) = 2\pi k$, i.e., $\arg(z) = \frac{2\pi k}{n}$ We denote $\omega_n = e^{i2\pi/n}$; such ω_n is called a primitive root of unity of order n.

$$((\omega_n)^k)^n = (\omega_n)^{nk} = ((\omega_n)^n)^k = 1^k = 1.$$

for all k such that 0 ≤ k ≤ n − 1

- $\omega_n^k \omega_n^m = \omega_n^{k+m}$
- If $k + m \geq n$ then $k + m = n + l$ for $l = (k + m) \mod n$ and we have $\omega_n^k \omega_n^m = \omega_n^{k+m} = \omega_n^{n+l} = \omega_n^n \omega_n^l = 1 \cdot \omega_n^l = \omega_n^l$ where $0 \leq l < n$.
- The Cancelation Lemma:$\omega_{kn}^{km} = \omega_n^m$ for all integers k, m, n.

The Discrete Fourier Transform --- DFT

Let $A =< A_0, A_1, \ldots, A_{n-1} >$ be a sequence of n real or complex numbers.

We can form the corresponding polynomial $P_A(x) = \Sigma_{j=0}^{n-1} A_j x^j$, We can evaluate it at all complex roots of unity of order n, i.e., we compute $P_A(\omega_n^k)$ for all $0 \le k \le n-1$.

The sequence of values $< P_A(1), P_A(\omega_n), P_A(\omega_n^2), \ldots, P_A(\omega_n^{n-1}) >$, is called **the Discrete Fourier Transform (DFT)** of the sequence $A =< A_0, A_1, \ldots, A_{n-1} >$.

$P_A(\omega_n^k)$ is usually denoted by $\widehat{A}_k$.

The DFT $\widehat{A}$ of a sequence A can be computed VERY FAST using a divide-and-conquer algorithm called the **Fast Fourier Transform**.

New way of fast multiplication of polynomials

- If we multiply a polynomial

$$P_A(x) = A_0 + \ldots + A_{n-1}x^{n-1}$$

of degree $n-1$ with a polynomial

$$P_B(x) = B_0 + \ldots + B_{m-1}x^{m-1}$$

of degree $m-1$ we get a polynomial

$$C(x) = P_A(x)P_B(x) = C_0 + \ldots + C_{m+n-2}x^{m+n-2}$$

of degree $n-1+m-1 = m+n-2$ with $m+n-1$ coefficients.

- To uniquely determine such a polynomial $C(x)$ of degree $m+n-2$ we need $m+n-1$ many values.
- Thus, we will evaluate both $P_A(x)$ and $P_B(x)$ at all the roots of unity of order $n+m-1$ (instead of at $-(n-1), \ldots, -1, 0, 1, \ldots, m-1$ as we would in Karatsuba's method!)

见slides11-14

tutorial question 8

Matrix representation of polynomial evaluation

Slides 20

tutorial question 9, 10, 11, 13,15...