Lec13A

March 2, 2021 1:48 PM

Assignment #4 posted
Due Monday March 15th.

The Fast Fourier Transform (FFT)

Let F be a field and $\omega \in F$ be a primitive n'th root of unity.
So $\omega^n = 1$ and $\omega^i \neq 1$ for $1 \le i \le n-1$
Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in F$.

$$FFT(n=2^k, \omega, A)$$

evaluation.

(discrete) Fourier transform of $a(x)$.

$$A = [a_0, a_1, \ldots, a_{n-1}]^T \in F^n \qquad B = [a(1), a(\omega), \ldots, a(\omega^{n-1})]^T \in F^n$$

interpolation.

$$FFT^{-1} = \tfrac{1}{n} FFT(n, \omega^{-1}, B)$$

The FFT computes B using $O(n \log n)$ arithmetic operations in F.
A3. $\frac{1}{2} n \log_2 n + O(n)$ multiplications in F

Fast multiplication in $F[x]$.

Let $a, b \in F[x]$ and $c = a \times b$.

$$\varphi_{x=\omega^i}(a(x) \cdot b(x)) = \varphi_{x=\omega^i}(a) \cdot \varphi_{x=\omega^i}(b).$$

$$\begin{array}{ccc} c(x) & = & a(x) \cdot b(x). \\ \uparrow FFT^{-1} & & 1 \cdot FFT \downarrow \quad FFT \downarrow \\ c(\omega^i) & \Leftarrow & a(\omega^i) \cdot b(\omega^i) \\ & & \uparrow_F \end{array}$$

Cost: 3 FFTs $+ 2n$
$= O(n \log n)$. arithmetic ops in F.

$n \geq deg(c(x)) + 1 = deg(a) + deg(b) + 1.$
$n = 2^k$

Case $F = \mathbb{Z}_p$, $\omega \in F \iff n \mid p-1.$
Need primes of the form $p = \underset{\underset{2^k}{\parallel}}{n} \cdot q + 1$. These primes are called Fourier primes.

Let $a, b \in \mathbb{Z}^+$. How can we compute $c = a \times b$ using the FFT?
Let $a = \sum_{i=0}^{\ell} a_i B^i$, $b = \sum_{i=0}^{m} b_i B^i$ where $0 \le a_i, b_i < B$ and $B = 2^{64}$.

64bits 64bits

$i=0$ $\qquad$ $i=0$

$$a = \boxed{\overbrace{a_0}^{64\text{ bits}} \mid a_1 \mid a_2 \mid \overbrace{a_3}^{64\text{ bits}}}$$

Let $a(x) = \sum_{i=0}^{l} a_i x^i$ and $b = \sum_{i=0}^{m} b_i x^i \in \mathbb{Z}[x]$, with $x = B$.

$$\begin{tikzcd}
C(x) \arrow[r, phantom, "\overset{\text{FFT } ②}{=}"] \arrow[d, "③\ x=B"'] & a(x) \cdot b(x) \\
C = C(B) \arrow[r, phantom, "="] & a \cdot b \arrow[u, "①"']
\end{tikzcd}$$

$O(n) \to$ ③ $\qquad$ ① $\leftarrow O(n)$

Use the FFT to multiply $C(x) = a(x) \cdot b(x)$ in $\mathbb{Z}[x]$ then evaluate $C(B)$.

Ex. $a = 768 \longrightarrow 7 \cdot x^2 + 6x + 8$
$b = 436 \longrightarrow 4x^2 + 3x + 6$
$B = 10.$

$\longrightarrow C(x) = 28x^4 + 45x^3 + 92x^2 + 60x + 48$

$C(10) = \boxed{28}0000 + \boxed{45}000 + \boxed{92}00 + \boxed{60}0 + \boxed{48}$

$= 334848$

10^5	10^4	10^3	10^2	10	1
3	3	4	8	4	8

Let $n = 2^k \geq l + m + 1$. Pick 3 primes $p_1, p_2, p_3 < 2^{64} = B$ s.t. $n \mid p-1$ (for FFT)
and $M = p_1 p_2 p_3 > \|C\|_\infty \leq \|a\|_\infty \cdot \|b\|_\infty \min(l+1, m+1)$.
$< B \cdot B \cdot \underbrace{\min(l+1, m+1)}_{\sim 10^9 \approx 2^{30}}$, $B = 2^{64}$

Suppose $B = 2^{64}$

For $l = m = 10^9 < 2^{30}$ $\deg(c) < 2^{32}$.
So $n = 2^{32}$ is sufficient.

$$\|C\|_\infty < B^2 \cdot 2^{32} = 2^{128} \cdot 2^{32} = 2^{160}.$$

$p_1 = 2^{57} \cdot 29 + 1$
$p_2 = 2^{56} \cdot 87 + 1$
$p_3 = 2^{56} \cdot 27 + 1$
$M = p_1 p_2 p_3 > 2^{185}$

So compute $a(x) \times b(x) \bmod p_1, p_2, p_3$ using the FFT then use CRT.

This method is called the "3 primes" method.
It does $3 \times$ in $\mathbb{Z}_{p_1}[x]$ $\mathbb{Z}_{p_2}[x]$ $\mathbb{Z}_{p_3}[x]$ then uses the CRT.

Cost $\quad$ 9 FFTs + $\underline{n \text{ CRTs}}$ ($\underline{3 \text{ primes}}$).
$= O(n \log n) + n O(1)$
$= \underline{O(n \log n)}.$