

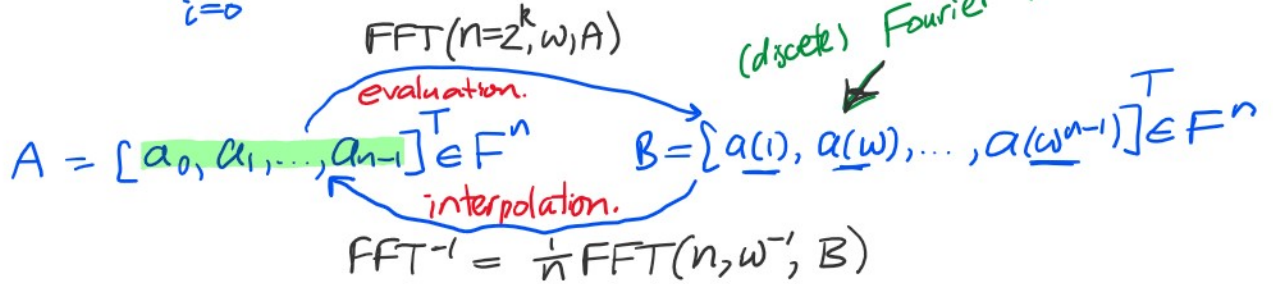
Assignment #4 posted
Due Monday March 15th.

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 $1 \leq i \leq n-1$

Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in F$.

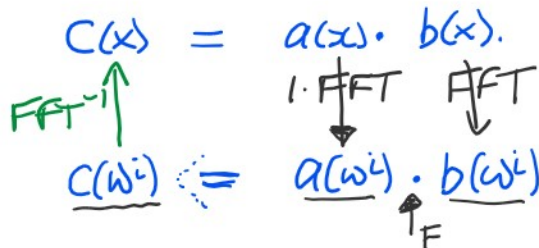


The FFT computes B using $O(n \log n)$ arithmetic operations in F .
A3. $\frac{1}{2} n \log_2 n + O(n)$ multiplications in F

Fast multiplication in $F[x]$.

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

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



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

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

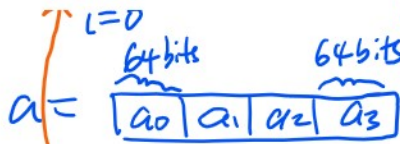
Case $F = \mathbb{Z}_p$, $\omega \in F \Leftrightarrow n | p-1$.

Need primes p to form $p = n \cdot q + 1$. These primes are called Fourier primes.

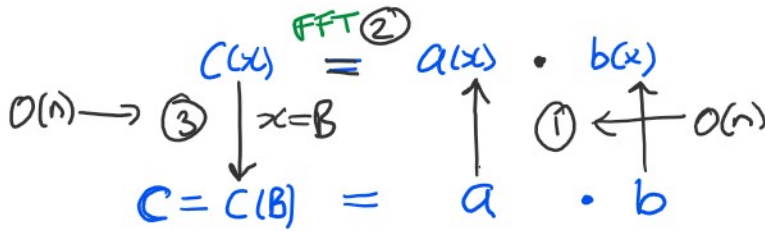
Let $a, b \in \mathbb{Z}^+$ How can we compute $c = a \cdot b$ using the FFT?

Let $a = \sum_{i=0}^r a_i B^i$, $b = \sum_{i=0}^m b_i B^i$ where $0 \leq a_i, b_i < B$ and $B = 2^{64}$.

64 bits 64 bits



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



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

$$\begin{matrix} 5 & 4 & 3 & 2 & 1 & 0 \\ 10^5 & 10^4 & 10^3 & 10^2 & 10^1 & 1 \\ 3 & 3 & 4 & 8 & 4 & 8 \end{matrix}$$

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

$C(x) = 28x^4 + 45x^3 + 92x^2 + 60x + 48$
 $C(10) = 28 \cdot 10000 + 45 \cdot 1000 + 92 \cdot 100 + 600 + 48 = 334848$

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

Suppose $B = 2^{64}$

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

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

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

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

This method is called the "3 primes" method.

It does 3 x m $\mathbb{Z}_{p_1}[x]$ $\mathbb{Z}_{p_2}[x]$ $\mathbb{Z}_{p_3}[x]$ then uses the CRT.

Cost **9 FFTs** + n CRTs (3 primes).

$$= O(n \log n) + nO(1)$$

$$= \underline{\underline{O(n \log n)}}$$