Introduction

Consider two polynomial functions of degree n-1 , A(x) and B(x) where

$$A(x) = a_0x^0+a_1x^1+\cdots+a_{n-1}x^{n-1} \ = \Sigma a_ix^i$$

and,

$$B(x) = b_0x^0+b_1x^1+\cdots+b_{n-1}x^{n-1} = \ = \Sigma b_ix^i$$

The task is to multiply these two polynomials. The naive approach is that we multiply each term of A(x) polynomial with each term of B(x) polynomial. The time complexity of the naive approach is $O(n^2)$ whereas FFT(fast Fourier transform) multiplies the two polynomials in O(nlogn) time.

To understand the FFT, we need to understand the point value of a polynomial first.

Point Value Form

Consider the polynomial $A(x)=a_0x^0+a_1x^1+\cdots+a_{n-1}x^{n-1} \ = \Sigma a_ix^i$, this polynomial representation is **coefficient value form.**

The **point value-form** is

$A(x) = \{(x_0,y_0), (x_1,y_1), \ldots(x_{n-1},y_{n-1})\}$ where $y_k = A(x_k)$ and x_k are all distinct arbitrary integers.

Example: Let $A(x) = x^2 + x + 1$

$A(0) = 0 + 0 + 1 = 1$, $y_0 = 1$ and $x_0 = 0$ as $y_0 = A(x_0)$

What this means is that

If you have $A(x) = a_0x^0+a_1x^1+a_2x^{2.}$, and you know y_0, y_1, y_2, x_0, x_1 and x_2, you will have 3 equations

$y_0 = a_0 + a_1x_0^1 + a_2x_0^{2.}$

$y_1 = a_0 + a_1x_1^1 + a_2x_1^{2.}$

$y_2 = a_0 + a_1x_2^1 + a_2x_2^{2.}$

with three unknowns a_o, a_1, and a_2, that can be computed easily.

The equation can be represented as

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & \vdots & \vdots & & \vdots \\ 1 & \vdots & \vdots & & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ \vdots \\ y_{n-1} \end{pmatrix}$$

Thus we can find a_0, a_1, a_2 ... a_{n-1} as

$$\begin{pmatrix} a_0 \\ a_1 \\ | \\ | \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & x_0 & x_0^2 & ---- & x_0^{n-1} \\ 1 & x_1 & x_1^2 & ---- & x_1^{n-1} \\ 1 & | & | & & | \\ 1 & | & | & & | \\ 1 & x_{n-1} & x_{n-1}^2 & ---- & x_{n-1}^{n-1} \end{pmatrix}^{-1} \begin{pmatrix} y_0 \\ y_1 \\ | \\ | \\ y_{n-1} \end{pmatrix}$$

Applying Point Value Form

Given,

$$A(x) = \Sigma a_i x^i$$
$$B(x) = \Sigma b_i x^i$$

Find C(x), where C(x) = A(x)B(x).

Let $A(x) = x^2 + x + 1$ and $B(x) = x^2 - 1$. A(x) and B(x) can be represented as

A(x) = {(0,1), (1,3), (2,7)} and B(x) = {(0,-1), (1,0), (2,3)} in point value form.

Now since C(x) = A(x)B(x),
Therefore C(0) = A(0) B(0) = -1
C(1) = A(1) B(1) = 0
C(2) = A(2) B(2)= 21

We can get three-point value forms of C(x), but do we need only 3 pairs or more?
On multiplying A(x) and B(x) we get $C(x) = x^4 + x^3 - x - 1$, therefore we can easily see that we need 2n-1 pairs for A(x) and B(x).
Now since we have 2n-1 pairs, we can easily compute coefficients of C(x) by calculating the inverse.

Before moving onto FFT, we need to understand some lemma’s of complex numbers.

Complex Numbers

- **The n^{th} root of unity**
  $(\text{number})^k = 1$, one of the roots is 1 and other are complex numbers
  Principle: n^{th} root of unity is given as
  $$w_n = e^{i2\pi/n}$$
  Now, n roots of unity are given by different powers of W_n
  $$w_n^0, w_n^1, w_n^2, w_n^3, \ldots\, w_n^{n-1},$$

Also $e^{ix} = \cos x + i \sin x$, therefore

$$\mathbf{e^{i2\pi/n} = \cos (2\pi/n) + i \sin (2\pi/n)}$$

Therefore, n^{th} roots of unity can be given as

$$e^{i2\pi k/n}, k=0 \ldots n-1$$

Also

$$w_n^n = w_n^0 = 1$$

So, I can say that

$$\mathbf{w_n^k * w_n^j = w_n^{j+k} = w_n^{(j+k)\,\%\,n} = w_n^n * w_n^{j+k-n}}$$

- **Lemma 1**

  For n >= 0, k >= 0, d >= 0

  $$\mathbf{w_{d*n}^{d*k} = w_n^k}$$

  Proof:

  $$\mathbf{(w_{d*n}^k)^d = (e^{i2\pi k/dn})^d = e^{i2\pi k/n} = w_n^k}$$

- **Lemma 2**

  For n>0, n is even

  $$\mathbf{w_n^{n/2} = w_2^1 = -1}$$

  Proof:

  $$\mathbf{w_n^{n/2} = (e^{i2\pi/n})^{n/2} = e^{i\pi} = \cos \pi + i \sin \pi = -1}$$

- **Lemma 3**

  For n>0, n is even, square of n complex $n^{th\ roots}$ of unity is (n/2) complex $(n/2)^{th}$ roots of unity

  $$\mathbf{w_n^k = e^{i2\pi k/n}, k = 0 \ldots 1}$$

  Then for all k in $(W_n^k)^2 = W_n^{2*k} = W_{2(n/2)}^{2*k}$

  Now from lemma 1 where d=2

  We can say that

  $$\mathbf{w_{2(n/2)}^{2*k} = w_{n/2}^k}$$

  which (n/2) complex $(n/2)^{th}$ roots of unity where each term is repeated twice

- **Lemma 4**

  $$\mathbf{[w_n^{(k+n/2)}]^2 = w_{n/2}^k}$$

  Let k + n/2 = y

  $$\mathbf{W_n^{2y} = w_n^{2(k+n/2)} = e^{i2\pi y/n}}$$

  $$\mathbf{= e^{i2\pi(2k+n)/n} = e^{i4\pi k/n} * e^{i2\pi}}$$

  $$\mathbf{= w_n^{2k} * (\cos 2\pi + i \sin 2\pi) = w_n^{2k} = w_{n/2}^k}$$

- **Lemma 5**

For n>=0, k>=0

$$w_n^{(k + n/2)} = -w_n^k$$

$$w_n^{(k + n/2)} = e^{i2\pi/n * (k + n/2)} = e^{i2\pi k/n} * e^{\pi i} = -w_n^k$$