Lecture 25

Gidon Rosalki

2025-01-26

1 DFT, FFT, operations on polynomials

We are considering the complex polynomials of power $\leq n-1$. We will write this polynomial space as $V_{n-1}^{\mathbb{C}}$. We are interested to carry out on them 2 operations, multiplication, and value representation in time $O\left(n\log\left(n\right)\right)$.
The two representations of a polynomial: coefficient representation, and value representation at n different complex points $z_0,\ldots,z_{n-1}$.
The operation of value representation is efficient, and costs $O\left(n\right)$. In coefficient representation the multiplication operation is efficient in the value representation. We will focus on the value representation of the polynomials at the n roots of unity of power n.
Let us write $\omega_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. We will call ω_n the primitive root of unity of order n. So the powers ω_n^k where $0\leq k\leq n-1$ are the roots of unity of order n. We will look at the values of the polynomial p at these points $z_0,\ldots,z_{n-1}$ where $z_k = \omega_n^k : 0\leq k\leq n-1$.
Let there be $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1}\end{bmatrix}$ the coefficient vector of p, which is to say

$$p\left(z\right) = \sum_{k=0}^{n-1} a_k z^k$$

So $\begin{bmatrix} p\left(\omega_n^0\right) \\ \vdots \\ p\left(\omega_n^{n-1}\right)\end{bmatrix}$ will be called **the discrete fourier transform** of the vector $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1}\end{bmatrix}$, and we will write

$$\begin{bmatrix} p\left(\omega_n^0\right) \\ \vdots \\ p\left(\omega_n^{n-1}\right)\end{bmatrix} = DFT_n \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1}\end{bmatrix}$$

Theorem 1 (FFT)**.** *Let there be n, a power of two, and $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1}\end{bmatrix} \in \mathbb{C}^n$. Then we can find*

$$DFT_n \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1}\end{bmatrix}$$

in $O\left(n\log\left(n\right)\right)$.
Additionally, let there be $\begin{bmatrix} p_0 \\ \vdots \\ p_{n-1}\end{bmatrix} \in \mathbb{C}^n$. Then we can find $DFT_n^{-1}\begin{bmatrix} p_0 \\ \vdots \\ p_{n-1}\end{bmatrix}$ in $O\left(n\log\left(n\right)\right)$

Proof intuition. We saw that the change between coefficient representation, and value representation of the polynomial p at the points $z_0,\ldots,z_{n-1}$ is the multiplying by the Vandermonde matrix. When the points $z_0,\ldots,z_{n-1}$ are the nth roots of unity, which is to say $0\leq k\leq n-1$ $z_k = \omega_n^k$ we will get the matrix M (Vandermonde) such that

$$M = \left(z_k^m\right)_{k,m:0\leq k,m\leq n-1} = \left(\omega_n^{km}\right)_{k,m}$$

Example: $n = 4$: $\omega_n = i$, so $\omega_n^0 = 1,\ \omega_n^1 = i,\ \omega_n^2 = -1,\ \omega_n^3 = -i$. So

$$M_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

Lemma:

$$M_n^{-1} = \frac{1}{n} \cdot \left(\omega_n^{-km}\right)_{k,m}$$

Also

$$\begin{bmatrix} A & B \\ A & -B \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} AX + BY \\ AX - BY \end{bmatrix}$$
$$T(n) \leq 2T\left(\frac{n}{2}\right) + O(n)$$

So if we count the rows and columns from 0, let us look for sub matrices of the shape

$$M_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

. So rows 0 and 2 of our matrix M_4 form 2 such matrices. Additionally from rows 1 and 3, we may take the matrices

$$B = \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$$
$$-B = \begin{bmatrix} -1 & -i \\ -1 & i \end{bmatrix}$$

So we have split up M into the three required matrices, A which appears twice which is M_2, and B and $-B$ □

Proof. Given a vector $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \in \mathbb{C}^n$, (where n is a power of 2), we want to find $\begin{bmatrix} p\left(\omega_n^0\right) \\ \vdots \\ p\left(\omega_n^{n-1}\right) \end{bmatrix}$ in $O(n \log(n))$ (when $p(z) = \sum_{k=0}^{n-1} a_k z^k$)

Theorem 2 (Lemma)**.** *Let n be an even number, let $p(z) = \sum_{k=0}^{n-1} a_k z^k \in V_{n-1}$. We will define $p_0(y) = \sum_{j=0}^{\frac{n}{2}-1} a_{2j} y^j$ and $p_1(y) = \sum_{m=0}^{\frac{n}{2}-1} a_{2m+1} y^m$. So*

$$p(z) = p_0\left(z^2\right) + z p_1\left(z^2\right)$$

Example: $n = 4,\ p(z) = 2z^3 - 3z^2 + z + 1$

$$\begin{aligned} 2z^3 - 3z^2 + z + 1 &= \left(-3z^2 + 1\right) + \left(2z^3 + z\right) \\ &= \left(-3x^2 + 1\right) + z \cdot \left(2z^2 + 1\right) \\ &= p_0\left(z^2\right) + z \cdot p_1\left(z^2\right) \\ p_0(y) &= -3y + 1 \\ p_1(y) &= 2y + 1 \end{aligned}$$

Proof .

$$\begin{aligned}
p_0\left(z^2\right) + z p_1\left(z^2\right) &= \sum_{j=0}^{\frac{n}{2}-1} a_{2j}\left(z^2\right)^j + z \cdot \sum_{m=0}^{\frac{n}{2}-1} a_{2m+1}\left(z^2\right)^m \\
&= \sum_{j=0}^{\frac{n}{2}-1} a_{2j} z^{2j} + \sum_{m=0}^{\frac{n}{2}-1} a_{2m+1} z^{2m+1} \\
&= \sum_{k=0}^{n-1} a_k z^k \\
&= p(z)
\end{aligned}$$

□

Theorem 3 (Lemma)**.** *Let there be n an even number, then*

1. $\omega_n^2 = \omega_{\frac{n}{2}}$
2. *For all $0 \leq j \leq \frac{n}{2} - 1$: $\left(\omega_n^j\right)^2 = \omega_{\frac{n}{2}}^j$, and also $\left(\omega_n^{\frac{n}{2}+j}\right)^2 = \omega_{\frac{n}{2}}^j$. In other words, when we raise the nth root of unity to the power of 2, we pass twice on the $\frac{n}{2}$ roots of unity*

Proof . 1. $\omega_n = \cos\left(\frac{2\pi}{2}\right) + i\sin\left(\frac{2\pi}{2}\right)$. Therefore

$$\begin{aligned}
\omega_n^2 &= \cos\left(\frac{2\pi}{\frac{n}{2}}\right) + i\sin\left(\frac{2\pi}{\frac{n}{2}}\right) \\
&= \omega_{\frac{n}{2}}
\end{aligned}$$

2. For all $0 \leq j \leq \frac{n}{2} - 1$ it is true that

$$\left(\omega_n^j\right)^2 = \omega_n^{2j} = \left(\omega_n^2\right)^j = \omega_{\frac{n}{2}}^j$$

and so

$$\left(\omega_n^{\frac{n}{2}+j}\right)^2 = \omega_n^{2\left(\frac{n}{2}+j\right)} = \omega_n^n \cdot \omega_n^{2j} = \omega_{\frac{n}{2}}^j$$

□

We may now finally prove the theorem:

$$\begin{bmatrix} p\left(\omega_n^0\right) \\ \vdots \\ p\left(\omega_n^{n-1}\right) \end{bmatrix} = \begin{bmatrix} p_0\left(\left(\omega_n^0\right)^2\right) + \omega_n^0 \cdot p_1\left(\left(\omega_n^0\right)^2\right) \\ \vdots \\ p_0\left(\left(\omega_n^{n-1}\right)^2\right) + \omega_n^{n-1} \cdot p_1\left(\left(\omega_n^{n-1}\right)^2\right) \end{bmatrix}$$

$$= \begin{bmatrix} p_0\left(\left(\omega_n^0\right)^2\right) \\ \vdots \\ p_0\left(\left(\omega_n^{n-1}\right)^2\right) \end{bmatrix} + \begin{bmatrix} \omega_n^0 \\ \vdots \\ \omega_n^{n-1} \end{bmatrix} \bullet \begin{bmatrix} p_1\left(\left(\omega_n^0\right)^2\right) \\ \vdots \\ p_1\left(\left(\omega_n^{n-1}\right)^2\right) \end{bmatrix} \text{Multiplying coordinate - coordinate}$$

$$= \begin{bmatrix} p_0\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots \\ p_0\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \\ p_0\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots p_0\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \end{bmatrix} + \begin{bmatrix} \omega_n^0 \\ \vdots \\ \omega_n^{n-1} \end{bmatrix} \bullet \begin{bmatrix} p_1\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots \\ p_1\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \\ p_1\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots p_1\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \end{bmatrix}$$

We will note that p_0 is a polynomial of power $\frac{n}{2} - 1$, with the coefficient vectors $\begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix}$, and therefore the vector $\begin{bmatrix} p_0\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots \\ p_0\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \end{bmatrix}$ which is the value vector of the polynomial p_0, of the $\frac{n}{2}$ roots of unity.

Therefore, from the definition of the DFT of order $\frac{n}{2}$

$$\begin{bmatrix} p_0\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots \\ p_0\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \end{bmatrix} = DFT_{\frac{n}{2}} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix}$$

and similarly

$$\begin{bmatrix} p_2\left(\omega_{\frac{n}{2}}^0\right) \\ \vdots \\ p_2\left(\omega_{\frac{n}{2}}^{\frac{n}{2}-1}\right) \end{bmatrix} = DFT_{\frac{n}{2}} \begin{bmatrix} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

and therefore we have the equivalence

$$DFT_n \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} DFT\frac{n}{2} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix} \\ DFT\frac{n}{2} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix} \end{bmatrix} + \begin{bmatrix} \omega_n^0 \\ \vdots \\ \omega_n^{n-1} \end{bmatrix} \bullet \begin{bmatrix} DFT\frac{n}{2} \begin{bmatrix} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{bmatrix} \\ DFT\frac{n}{2} \begin{bmatrix} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{bmatrix} \end{bmatrix}$$

□