Discrete Fourier Transform.

$$b_i = \sum_{j=0}^{n-1} \omega^{ij} \cdot a_j .$$

• Ring $\left(R, +, \times, \underset{0}{\underline{\text{a-id}}}, \underset{1}{\text{m-id}} \right)$ $\Big\}$ R

$$\begin{tikzcd}
\vec{a} \arrow[r, "DFT"] \arrow[d, "\phi"] & \vec{b} = DFT(\vec{a}) \arrow[d, "\phi"] \\
\phi(\vec{a}) = \vec{a}' & \phi(\vec{b}) \arrow[l, "InvDFT"]
\end{tikzcd}$$

$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$

$\mathbb{Z}_m = \mathbb{Z} \bmod m$

Input: $\vec{a} = (a_0, a_1, \dots, \underline{a_{n-1}})$

Discrete Fourier Transform $\left(DFT(\vec{a}) \right) = A \cdot (\vec{a})^T$.

Assume that $\frac{1}{n}$ is available in our ring R. Assume that n is a power of 2.

$\forall \; i,j \in [0, n-1], \quad A_{i,j} = \underset{\sim}{\omega}^{i \cdot j}.$

Primitive n^{th} root of unity

$\omega^k \neq 1 \;\; \forall \; k \in [1, n-1].$

$(A^{-1})_{i,j} = \dfrac{\omega^{-i \cdot j}}{n}.$

$\underbrace{DFT : R^n \to \mathbb{C}^n}_{\text{invertible linear map.}}$

Want: To compute the linear transform $(DFT(\vec{a}))$.

Remark: Naively, $\vec{b}$ needs $\underbrace{O(n^2)}$ operations.

Rather any linear transformation takes at most $O(n^2)$ operations

$$\boxed{\begin{aligned} DFT(InvDFT(\vec{a})) &= \vec{a} \\ InvDFT(DFT(\vec{a})) &= \vec{a} \end{aligned}}$$

Cooley-Tukey: If we consider a linear transformation by the DFT matrix, it can be done in $O(n \log n)$ operations.

$$(b_i) = \sum_{j=0}^{n-1} \omega^{ij} \cdot a_j$$

$$P_a(x) = \sum_{j=0}^{n-1} a_j x^j .$$

$$A \cdot (\vec{a})^T$$

$$b_0 = \sum_{i=0}^{n-1} (\omega^0)^j \cdot a_j = P_a(\omega^0)$$

$$\begin{bmatrix} b_0 \\ \\ \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} \omega^0 & \omega^0 & \cdots & \omega^0 \\ \omega^0 & \omega^1 & \cdots & \omega^{n-1} \\ \omega^0 & \omega^2 & \cdots & \omega^{2(n-1)} \\ & & & \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \\ a_{n-1} \end{bmatrix}$$

Evaluation of $P_a(x)$ at points $\omega^0, \omega^1, \dots, \omega^{n-1}$.

$$\begin{bmatrix} P_a(\omega^0) \\ \\ P_a(\omega^{n-1}) \end{bmatrix} = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix} \begin{bmatrix} a_0 \\ \\ a_{n-1} \end{bmatrix}$$

$n' = 2^k$

$$P'_a(x) = \sum_{j=0}^{n'-1} a_j x^j \quad \text{s.t } a_j = 0 \;\forall\; j > n-1 .$$

$(a_0, \dots, a_{n-1})$

$(a_0, \dots, a_{n-1}, 0, \dots)$

↳ A which is of size $n' \times n'$.

Given two polynomials $\underbrace{P(x) \text{ and } Q(x)}_{\text{degree at most } n-1.}$: Compute their product

$$P(x) = A + x^{n/2} B \qquad\qquad Q(x) = A' + x^{n/2} B'$$

$$PQ(x) = AA' + BB' \cdot x^n + \underbrace{(AB' + BA')}\, x^{n/2}$$

↳ $n^{\log_2 3} \sim n^{1.\sim}$

$P(x) \xrightarrow{\text{DFT}}$ evaluations of P at $\{\omega^i\}_{i \in [0, 2n-2]}$

$Q(x) \xrightarrow{\text{DFT}}$ evals of Q at $\{\omega^i\}_{i \in [0, 2n-2]}$

Evaluations of $P(x) \cdot Q(x)$ at $\{\omega^i\}$

↓ InvDFT

Obtain coef. of the product.

$w^i \rightarrow P(w^i) \cdot Q(w^i)$

$R(x) = P(x) \cdot Q(x)$

$$\sum_{i=0}^{n-1} p_i \cdot x^i \cdot \sum_{j=0}^{n-1} q_j x^j$$

Suff: Consider $2n^{th}$ root of unity.

$\leq 2n-2$

$$\left.\begin{array}{l} P = (\underbrace{p_0, \ldots, p_{n-1}, 0, \ldots, 0}_{2n}) \\ Q = (\underbrace{q_0, \ldots, q_{n-1}, 0, \ldots, 0}_{2n}) \end{array}\right\} \xrightarrow{DFT} \left.\begin{array}{l} P(w^0), \ldots, P(w^{2n-1}) \\ Q(w^0), \ldots, Q(w^{2n-1}) \end{array}\right\}$$

$R(w^0), \ldots, R(w^{2n-1})$

$\downarrow$ Recover

Polynomial R.

$$\begin{array}{ccc} P \cdot Q & \xrightarrow[O(n \log n)]{DFT} & evals(P), eval(Q) \\ O(n^2) \downarrow & & \downarrow O(n) \\ R & \xleftarrow[O(n \log n)]{invDFT} & evals(R) \end{array}$$

$O(n \log n)$ algorithm

$$b_i = \sum_{j=0}^{n-1} w^{ij} \cdot a_j$$

$$= \sum_{j=0}^{n/2-1} w^{ij} a_j + \sum_{j=n/2}^{n-1} w^{ij} \cdot a_j$$

$j = \frac{n}{2} + j'$

$n-1 = \frac{n}{2} + j'$

$$= \underbrace{\sum_{j=0}^{n/2-1} w^{ij} a_j}_{} + w^{n/2 \, i} \cdot \underbrace{\sum_{j'=0}^{\frac{n}{2}-1} w^{ij'} \cdot a_{j'+\frac{n}{2}}}_{}$$

$w^k \neq 1 \; \forall k \in [0, n-1]$. $w^n = 1$.

$\sqrt{w^n}$

Obs: w^2 is $\frac{n}{2}^{th}$ prim root of unity if w is n^{th} prim root of unity.

Obs: $w^{n/2} = (-1)$

$w^n = 1$.

$$= \sum_{j=0}^{\frac{n}{2}-1} \omega^{ij} \cdot a_j + (-1)^i \cdot \sum_{j'=0}^{\frac{n}{2}-1} \omega^{ij'} \cdot a_{j'+\frac{n}{2}}$$

Say i is even. $i = 2p$.

$$b_i = \sum_{j=0}^{\frac{n}{2}-1} (\omega^2)^{p \cdot j} a_j + \sum_{j'=0}^{\frac{n}{2}-1} (\omega^2)^{p \cdot j'} \cdot a_{j'+\frac{n}{2}}.$$

$$= \sum_{j=0}^{\frac{n}{2}-1} (\omega^2)^{p \cdot j} \left(a_j + a_{j+\frac{n}{2}}\right).$$

$$= \sum_{j=0}^{\frac{n}{2}-1} (\omega^2)^{p \cdot j} \cdot C_j$$

$C_j = a_j + a_{j+\frac{n}{2}}$.

$\vec{C} = (C_0, \ldots, C_{\frac{n}{2}-1})$.

If i is odd

$$b_i = \sum_{j=0}^{n/2-1} \omega^{(2p+1)j} \cdot a_j - \sum_{j'=0}^{\frac{n}{2}-1} \omega^{(2p+1)j'} \cdot a_{j'+\frac{n}{2}}$$

$$= \sum_{j=0}^{\frac{n}{2}-1} (\omega^{2p+1})^j \left(a_j - a_{j+\frac{n}{2}}\right)$$

$$A^{-1}_{ij} = \frac{\omega^{-ij}}{n}$$

$$= \sum_{j=0}^{n/2-1} (\omega^2)^{p \cdot j} \underbrace{(\omega^j) \cdot \left(a_j - a_{j+\frac{n}{2}}\right)}$$

$$= \sum_{j=0}^{n/2-1} (\omega^2)^{p \cdot j} D_j$$

where $D_j = \omega^j \cdot \left(a_j - a_{j+\frac{n}{2}}\right)$

$\vec{D} = (D_0, \ldots, D_{\frac{n}{2}-1})$

Even locations of $\vec{b}$ can be obtained by $DFT_{\frac{n}{2}}(\vec{C})$

and Odd locations from $DFT_{\frac{n}{2}}(\vec{D})$.

$$
\begin{tikzcd}
 & \boxed{DFT_{\frac{n}{2}}(\vec{C})} \arrow[r] & C_j = a_j + a_{j+\frac{n}{2}} \\
\underline{DFT_n(\vec{a})} \arrow[ur] \arrow[dr] & & \\
 & \boxed{DFT_{\frac{n}{2}}(\vec{D})} \arrow[r] & D_j = (a_j - a_{j+\frac{n}{2}})\,\omega^j .
\end{tikzcd}
$$

Both $\vec{C}$ and $\vec{D}$ depend on $\vec{a}$.

$$T(n) = 2 \cdot T\left(\frac{n}{2}\right) + O(n) .$$

$$= O(n \log n) .$$

Rewriting Polynomial mult:

Convolution of two vectors $\vec{a}$ and $\vec{b}$ (denoted by $\vec{a} * \vec{b}$)

$i \in [0, 2n-2]$; $\quad (a * b)_i = \sum_{\substack{j+k=i \\ 0 \le j,k \le n-1}} a_j \cdot b_k$

Convolution gives coefs of the product of the polys whose coefs are $\vec{a}$ and $\vec{b}$.

$$\left(\sum_{j=0}^{n-1} a_j x^j\right)\left(\sum_{k=0}^{n-1} b_k x^k\right) = \sum_i \Big(\underbrace{\sum_{j+k=i} a_j b_k}\Big) \cdot x^i$$

Convolution

$$a * b = \mathrm{InvDFT}_{2n}\left(\mathrm{DFT}_{2n}(\vec{a}') \odot \mathrm{DFT}_{2n}(\vec{b}')\right)$$

point wise mult.

$$\vec{a}' = (\underbrace{a_0, \ldots, a_{n-1}, 0, \ldots, 0}_{2n})$$

$$\vec{b}' = (\underbrace{b_0, \ldots, b_{n-1}, 0, \ldots, 0}_{2n}).$$

$$(a_1, \ldots, a_n) \odot (b_1, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

Using DFT: Integer mult is in $O(n \log n)$ if R is "nice".

Else

$O(n \log n \log\log n)$

Schonhage-Strassen integer mult.

$O(n \log n) \cdot 2^{O(\log^* n)}$

[Furer 2008]

[De - Kurur - Saha - Saptarishi] STOC 2008