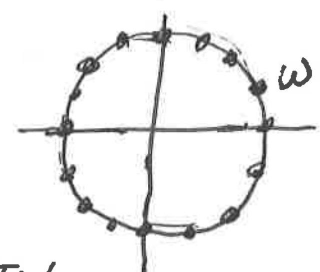
Wednesday 10/22/14 ①

Recap of last lecture:

FFT: Given the coefficients $a = (a_0, a_1, \ldots, a_{n-1})$
for a polynomial $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$
of degree $\leq n-1$ where n is a power of 2,
outputs $A(x)$ evaluated at n points which are
the n^{th} roots of unity

What are the n^{th} roots of unity?
Take the unit circle in the complex plane &
take 1 and the $n-1$ evenly spaced points.

For example, for $n=16$:



Let $\omega = \left(1, \frac{2\pi}{n}\right) = e^{2\pi i/n}$

Then, the n^{th} roots are $1, \omega, \omega^2, \ldots, \omega^{n-1}$

Note: $\omega^j = \left(1, \frac{2\pi j}{n}\right) = e^{2\pi i j/n}$

Key properties:

1) the 1^{st} $\frac{n}{2}$ of the n^{th} roots = − the last $\frac{n}{2}$ of the n^{th} roots

$$\omega^j = -\omega^{\frac{n}{2}+j}$$

$$\omega^j = \left(1, \frac{2\pi j}{n}\right) = (-1)(-1)\left(1, \frac{2\pi j}{n}\right) = -(1, \pi)\left(1, \frac{2\pi j}{n}\right) = -\left(1, \frac{2\pi j}{n} + \pi\right) = -\omega^{\frac{n}{2}+j}$$

2) Square of the n^{th} roots are the $\frac{n}{2}^{nd}$ roots:

Let $\omega_n = (1, \frac{2\pi}{n}) = e^{2\pi i/n}$

So the n^{th} roots are $1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}$

$$(\omega_n^j)^2 = (1, \tfrac{2\pi j}{n}) \times (1, \tfrac{2\pi j}{n}) = (1, \tfrac{2\pi j}{n/2}) = \omega_{n/2}^j$$

and $(\omega_n^{\frac{n}{2}+j})^2 = (-\omega_n^j)^2 = \omega_{\frac{n}{2}}^j$

Key idea for the divide and conquer approach:

Let $A_{even}(y) = a_0 + a_2 y + a_4 y^2 + \cdots + a_{n-2} y^{\frac{n-2}{2}}$

& $A_{odd}(y) = a_1 + a_3 y + a_5 y^2 + \cdots + a_{n-1} y^{n-2/2}$

Note that $A(x) = A_{even}(x^2) + x A_{odd}(x^2)$

& deg of $A(x)$ is $\leq n-1$

whereas degree of $A_{even}(y)$ and $A_{odd}(y)$ is $\leq \frac{n}{2} - 1 = \frac{n-2}{2}$

To evaluate $A(\omega_n^j) = A_{even}(\omega_{\frac{n}{2}}^j) + \omega_n^j A_{odd}(\omega_{\frac{n}{2}}^j)$

& $A(\omega_n^{\frac{n}{2}+j}) = A_{even}(\omega_{\frac{n}{2}}^j) + \omega_n^{\frac{n}{2}+j} A_{odd}(\omega_{\frac{n}{2}}^j)$

Thus, to evaluate $A(x)$ at the n^{th} roots we need A_{even} & A_{odd} at the $\frac{n}{2}^{th}$ roots (so 2 subproblems of half the size)

FFT algorithm:

Let $\omega = \omega_n = e^{2\pi i/n}$

FFT(a, ω):

input: vector $a = (a_0, a_1, \dots, a_{n-1})$ which are coefficients for polynomial $A(x)$ of degree $\le n-1$ where n is a power of 2 & ω is a n^{th} root of unity

output: $A(\omega^0), A(\omega), A(\omega^2), \dots, A(\omega^{n-1})$

if $n=1$, return $(A(1))$

Let $a_{even} = (a_0, a_2, \dots, a_{n-2})$ & $a_{odd} = (a_1, a_3, \dots, a_{n-1})$

$(s_0, s_1, \dots, s_{\frac{n}{2}-1}) = \text{FFT}(a_{even}, \omega^2)$

$(t_0, t_1, \dots, t_{\frac{n}{2}-1}) = \text{FFT}(a_{odd}, \omega^2)$

For $j = 0 \to \frac{n}{2} - 1$:

$$r_j = s_j + \omega^j t_j$$

$$r_{\frac{n}{2}+j} = s_j - \omega^j t_j$$

Return$(r_0, r_1, \dots, r_{n-1})$

Running time: $T(n) = 2T(\frac{n}{2}) + O(n) = O(n \log n)$

What about going from $A(\omega^0), A(\omega), A(\omega^2), \ldots, A(\omega^{n-1})$

& trying to get the coefficients $a = (a_0, a_1, \ldots, a_{n-1})$?

For points $x_0, x_1, \ldots, x_{n-1}$, notice that:

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ & & \vdots & & \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

for FFT we have:

$$\underbrace{\begin{bmatrix} A(1) \\ A(\omega) \\ A(\omega^2) \\ \vdots \\ A(\omega^{n-1}) \end{bmatrix}}_{A} = \underbrace{\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ & & \vdots & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix}}_{M_n(\omega)} \underbrace{\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}}_{a}$$

So: $A = M_n(\omega) a$

What's $M_n(\omega)^{-1}$?

Then
$$M_n(\omega)^{-1} A = a$$

Lemma: $M_n(\omega)^{-1} = \frac{1}{n} M_n(\omega^{-1})$

What's ω^{-1}? $\omega^{-1} = \omega^{n-1}$ because:

$\omega^{n-1} \times \omega = \omega^n = 1$ (since ω is a n^{th} root of unity)

So then computing $M_n(\omega)^{-1}A$ is just another FFT step.

Run $FFT(A, \omega^{n-1})$ & this gives $M_n(\omega^{-1})A = M_n(\omega)^{-1}A$

Just need to prove the lemma.

First a useful property of ω:

Note: $(\omega-1)(\omega^{n-1}+\omega^{n-2}+\dots+\omega+1) = \omega^n - 1$

since ω is a n^{th} root then $\omega^n = 1$ so $\omega^n - 1 = 0$

Hence, $(\omega-1)(\omega^{n-1}+\dots+1) = 0$

Since $\omega \neq 1$, then

$$\underline{\omega^{n-1}+\omega^{n-2}+\dots+\omega+1 = 0}$$

and for any $x \neq 1$ where x is a n^{th} root of unity: $\underline{x^{n-1}+x^{n-2}+\dots+x+1 = 0}$

To prove the lemma, we want to show that:

$$\frac{1}{n} M_n(\omega) M_n(\omega^{-1}) = I$$

I is the identity matrix $= \begin{bmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \end{bmatrix}$

1's on the diagonal
& 0's off the diagonal

Let's first take a diagonal entry:

take row k of $M_n(\omega) = (1 \ \omega^k \ \omega^{2k} \ \dots \ \omega^{(n-1)k})$

& take column k of $M_n(\omega^{-1}) = \begin{pmatrix} 1 \\ (\omega^{-1})^k \\ (\omega^{-1})^{2k} \\ \vdots \\ (\omega^{-1})^{(n-1)k} \end{pmatrix}$

the entry (k,k) of $\frac{1}{n} M_n(\omega) M_n(\omega^{-1}) =$

$$= \frac{1}{n}(1, \omega^k, \omega^{2k}, \dots, \omega^{(n-1)k}) \cdot (1, (\omega^{-1})^k, (\omega^{-1})^{2k}, \dots, (\omega^{-1})^{(n-1)k})$$

$$= \frac{1}{n}(1 + 1 + 1 + \dots + 1)$$

$$= 1$$

So the diagonals are correct.

For the off-diagonals, take row k of $M_n(\omega)$
& column j of $M_n(\omega^{-1})$
where $k \neq j$

then we have:

$$\frac{1}{n}\left(1, \omega^k, \omega^{2k}, \dots, \omega^{(n-1)k}\right) \cdot \left(1, (\omega^{-1})^j, (\omega^{-1})^{2j}, \dots, (\omega^{-1})^{(n-1)j}\right)$$

$$= \frac{1}{n}\left(\underbrace{1 + \omega^{k-j} + \left(\omega^{k-j}\right)^2 + \left(\omega^{k-j}\right)^3 + \dots + \left(\omega^{k-j}\right)^{n-1}}_{=0}\right)$$

$= 0$ because ω^{k-j} is a n^{th} root of unity.
as we showed before for $\omega \neq 1$.

So the off-diagonals are also correct. $\blacksquare$

Back to polynomial multiplication:

Given $a=(a_0,\ldots,a_{n-1})$ which are coefficients for polynomial $A(x)=\sum_{i=0}^{n-1} a_i x^i$

& $b=(b_0,\ldots,b_{n-1})$ which are coefficients for polynomial $B(x)=\sum_{i=0}^{n-1} b_i x^i$

We want to compute $c=(c_0,\ldots,c_{2n-2})$ which are coefficients for $C(x)=A(x)B(x)$

1. Run $FFT(a,\omega_{2n})$ & $FFT(b,\omega_{2n})$ where $\omega_{2n}=2n^{\text{th}}$ root of unity

This gives $A(1), A(\omega_{2n}), A(\omega_{2n}^2),\ldots, A(\omega_{2n}^{2n-1})$
& $B(1), B(\omega_{2n}), B(\omega_{2n}^2),\ldots, B(\omega_{2n}^{2n-1})$

2. For $j=0\to 2n-1$
$$C(\omega_{2n}^j)=A(\omega_{2n}^j)B(\omega_{2n}^j)$$

3. Run $FFT\left(\left(C(\omega_{2n}^0),\ldots,C(\omega_{2n}^{2n-1})\right),\omega_{2n}^{-1}\right)$ to get $n\cdot(c_0,c_1,\ldots,c_{2n-1})$