

# CS 170 Spring 2017 — Discussion 3

Raymond Chan

## Fast Fourier Transform

### Polynomial Multiplication

Given two polynomials  $A(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$  and  $B(x) = b_0 + b_1x + b_2x^2 + \dots + b_dx^d$ , we want  $C(x) = A(x) \cdot B(x) = c_0 + c_1x + c_2x^2 + \dots + c_{2d}x^{2d}$  where

$$c_k = a_0b_k + a_1b_{k-1} \dots a_kb_0 = \sum_{i=0}^k a_ib_{k-i}$$

This is really slow because we have to evaluate every pairwise coefficients between  $A(x)$  and  $B(x)$  to compute  $C(x)$ , which is  $O(d^2)$ .

Since any polynomial with degree  $d$  can be determined by  $d + 1$  points, we can use these values to represent our polynomials. Now  $C(x_i) = A(x_i) \cdot B(x_i)$ . The step would take only  $O(d)$ . Below we have another method for polynomial multiplication.

- **Selection**

Pick points  $x_0, x_1, \dots, x_{n-1}$ ,  $n \geq 2d + 1$ .

- **Evaluation**

Compute  $A(x_0), A(x_1), \dots, A(x_{n-1}), B(x_0), B(x_1), \dots, B(x_{n-1})$ .

- **Multiplication**

Compute  $C(x_k) = A(x_k) \cdot B(x_k)$ ,  $k = 0, 1, \dots, n - 1$ .

- **Interpolation**

Recover  $C(x) = c_0 + c_1x + c_2x^2 + \dots + c_{2d}x^{2d}$  from  $C(x_k)$ ,  $k = 0, 1, \dots, n - 1$ .

Selection and Multiplication takes  $O(n)$  time. We need to do evaluation and interpolation in sub- $O(n^2)$  time.

## Evaluation Divide and Conquer

Suppose we pick plus-minus pairs of  $x$  such that we have  $\pm x_0, \pm x_1, \dots, \pm x_{n/2-1}$ , squaring the plus-minus pairs gives us the same value.  $x_0^2, x_1^2, \dots, x_{n/2-1}^2$ .  
Looking at an example,

$$A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 = (3 + 6x^2 + x^4) + x(4 + 2x^2 + 10x^4)$$

In the RHS, we have  $A_e(x) = 3 + 6x + x^2$  and LHS  $A_o(x) = 4 + 2x + 10x^2$ .  $A_e(\cdot)$  contains the even degree coefficients and  $A_o(\cdot)$  contains the odd degree coefficients. In general terms,

$$A(x) = A_e(x^2) + xA_o(x^2)$$

In our example,

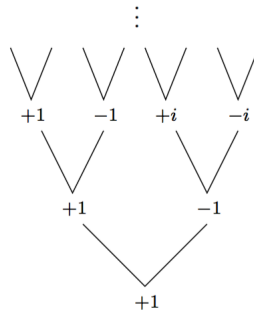
$$\begin{aligned} A_e(x) &= 3 + 6x + x^2 \\ A_o(x) &= 4 + 2x + 10x^2 \end{aligned}$$

If we use positive-negative pairs  $x_i$ ,

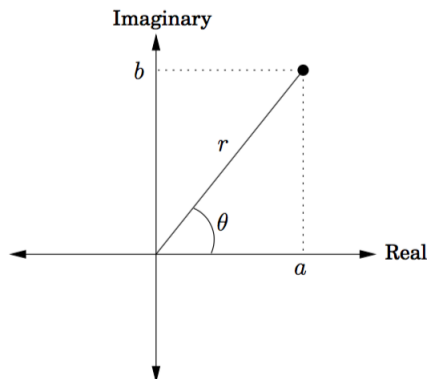
$$\begin{aligned} A(x_i) &= A_e(x^2) + xA_o(x^2) \\ A(-x_i) &= A_e(x^2) - xA_o(x^2) \end{aligned}$$

After the first level, we have to make  $x_0$  and  $x_1, x_2$  and  $x_3, \dots$  positive negative pairs as well. If we can do this until  $n = 1$ , at each level we make two recursive calls to evaluate a problem that is half the size. Thus we have a recurrence relation  $T(n) = 2T(n/2) + O(n)$  and runtime  $O(n \log n)$ .

Back to finding values of  $x$  that we can keep finding pairs such that there will be positive-negative pairs after squaring them. This can be achieved using complex numbers.



Squaring  $+1$  and  $-1$  gives us  $+1$ . Similarly, squaring  $+i$  and  $-i$  gives us  $-1$ . Now at this level, squaring  $+1$  and  $-1$  gives us  $+1$ .



### The complex plane

$z = a + bi$  is plotted at position  $(a, b)$ .

**Polar coordinates:** rewrite as  $z = r(\cos \theta + i \sin \theta) = re^{i\theta}$ , denoted  $(r, \theta)$ .

- **length**  $r = \sqrt{a^2 + b^2}$ .
- **angle**  $\theta \in [0, 2\pi)$ :  $\cos \theta = a/r, \sin \theta = b/r$ .
- $\theta$  can always be reduced modulo  $2\pi$ .

Number	$-1$	$i$	$5 + 5i$
Polar coords	$(1, \pi)$	$(1, \pi/2)$	$(5\sqrt{2}, \pi/4)$

Suppose we multiply complex numbers in polar coordinate form  $(r_1, \theta_1) \cdot (r_2, \theta_2)$ .

$$\begin{aligned}(r_1, \theta_1) \cdot (r_2, \theta_2) &= r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2} \\ &= r_1 r_2 e^{i(\theta_1 + \theta_2)} \\ &= (r_1 r_2, \theta_1 + \theta_2)\end{aligned}$$

If we were to move along the unit circle by  $90^\circ$ ,

$$\begin{aligned}(r, \theta) \cdot (1, \pi) &= (r, \theta + \pi) \\ &= r e^{i(\theta + \pi)}\end{aligned}$$

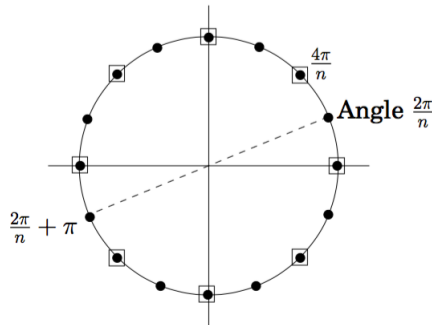
The  $n$ th roots of unity are all solutions to  $z^n = 1$ .

$$\begin{aligned}(1, 0) &= 1 \\ (1, \frac{2\pi}{n})^n &= (1, \frac{2\pi}{n} \cdot n) = (1, 2\pi) = 1 \\ (1, \frac{4\pi}{n})^n &= (1, 4\pi) = 1 \\ (1, \frac{2k\pi}{n})^n &= (1, 2k\pi) = 1\end{aligned}$$

Also, notice that,

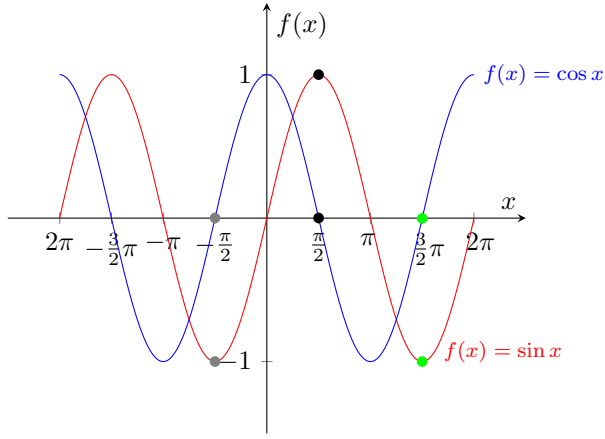
$$\begin{aligned}(1, 0) &= 1 \\ (1, \frac{2\pi}{n})^n &= (1, 2\pi) = 1 \\ (1, \frac{3\pi}{n})^n &= (1, 3\pi) = -1 \\ (1, \frac{4\pi}{n})^n &= (1, 4\pi) = 1 \\ (1, \frac{5\pi}{n})^n &= (1, 5\pi) = -1\end{aligned}$$

For any point on a unit circle, adding  $\pi$  degrees will negate the value.



In the unit circle, the numbers are plus-minus paired.  $-\cos \theta - i \sin \theta = \cos(\theta + \pi) + i \sin(\theta + \pi)$ . The squares will be the  $(n/2)$ nd roots of unity, which is the immediate left with a box around the point.

Now let us see why adding  $\pi$  will negate the number. Picking a point on the  $x$  axis, we can see that negating the points is the same as adding  $\pi$  on the sine and cosine curves.



The  $n$ th roots of unity are complex numbers  $1, \omega, \omega^2, \dots, \omega^{n-1}$ , where  $\omega = e^{2\pi i/n}$ . When  $n$  is even, these roots are plus-minus pairs,  $\omega^{n/2+j} = -\omega^j$ . Squaring them produces the  $(n/2)$ nd roots of unity. These  $n$  roots are solutions to the equation  $z^n = 1$ . Solutions are  $z = re^{ie}$  for some multiple of  $2\pi/n$ .

Below we have fast Fourier transform.  $A$  has polynomial of degree  $\leq n - 1$ .

```

procedure FFT( $A, \omega$ )
  if  $\omega = 1$  then return  $A(1)$ 
  Split  $A(\omega)$  into  $A_e(\omega^2) + A_o(\omega^2)$ 
  FFT( $A_e, \omega^2$ )
  FFT( $A_o, \omega^2$ )
  for  $j = 0, \dots, n - 1$  do
     $A(\omega^j) = A_e(\omega^{2j}) + \omega^j A_o(\omega^{2j})$ 
  return  $A(\omega^0), \dots, A(\omega^{n-1})$ 

```

The calls to  $A_e(\cdot)$  and  $A_o(\cdot)$  are evaluating polynomials with degrees at least half of the degree of  $A(\omega)$  because we are passing in squared  $\omega$  values as the input. We have a recurrence relation of  $T(n) = 2T(n/2) + O(n) = O(n \log n)$ .

When performing FFT evaluation, we need to pick  $n$  values such that  $n \geq d + 1$  and is a power of two. This will ensure the squaring of values gives us the proper divide and conquer all the way to the base case. Now in the polynomial multiplication problem, if we have  $A(x)$  and  $B(x)$  with degrees  $d_a$  and  $d_b$  respectively,  $C(x)$  will have degree  $d_a + d_b$ . This means we need to pick  $n \geq d_a + d_b + 1$  in order to uniquely define  $C(x)$  in value representation.

## Evaluation FFT Example

Let's use our example from earlier.

$$A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 = (3 + 6x^2 + x^4) + x(4 + 2x^2 + 10x^4)$$

- **Level 1**

We see that  $A(x)$  has degree 5, so we need the smallest power of two  $\geq 6$ .

Thus we have  $n = 8$  and  $\omega = e^{2\pi i/8} = e^{\pi i/4} = \cos(\pi/4) + i\sin(\pi/4)$ . Below are the 8 roots of unity in positive negative pairs.

$$\begin{aligned}\omega^0 &= 1 \\ \omega^4 &= e^{\pi i} = \cos(\pi) + i\sin(\pi) = -1 \\ \omega^1 &= e^{\pi i/4} = \cos(\pi/4) + i\sin(\pi/4) = \frac{1+i}{\sqrt{2}} \\ \omega^5 &= e^{5\pi i/4} = \cos(5\pi/4) + i\sin(5\pi/4) = -\frac{1+i}{\sqrt{2}} \\ \omega^2 &= e^{\pi i/2} = \cos(\pi/2) + i\sin(\pi/2) = i \\ \omega^6 &= e^{3\pi i/2} = \cos(3\pi/2) + i\sin(3\pi/2) = -i \\ \omega^3 &= e^{3\pi i/4} = \cos(3\pi/4) + i\sin(3\pi/4) = -\frac{1-i}{\sqrt{2}} \\ \omega^7 &= e^{7\pi i/4} = \cos(7\pi/4) + i\sin(7\pi/4) = \frac{1-i}{\sqrt{2}}\end{aligned}$$

Next we split  $A(x)$  into two recursive polynomials.

$$\begin{aligned}A(x) &= A_e(x^2) + xA_o(x^2) \\ A_e(x) &= B(x) = 3 + 6x + x^2 \\ A_o(x) &= C(x) = 4 + 2x + 10x^2\end{aligned}$$

Substituting the roots of unity,

$$\begin{aligned}A(\omega^0) &= B(1^2) + C(1^2) = B(1) + C(1) \\ A(\omega^4) &= B((-1)^2) - C((-1)^2) = B(1) - C(1) \\ A(\omega^2) &= B(i^2) + iC(i^2) = B(-1) + iC(-1) \\ A(\omega^6) &= B((-i)^2) + iC((-i)^2) = B(-1) - iC(-1) \\ A(\omega^1) &= B\left(\left(\frac{1+i}{\sqrt{2}}\right)^2\right) + \frac{1+i}{\sqrt{2}}C\left(\left(\frac{1+i}{\sqrt{2}}\right)\right) = B(i) + \frac{1+i}{\sqrt{2}}C(i) \\ A(\omega^5) &= B\left(\left(-\frac{1+i}{\sqrt{2}}\right)^2\right) - \frac{1+i}{\sqrt{2}}C\left(\left(-\frac{1+i}{\sqrt{2}}\right)\right) = B(i) - \frac{1+i}{\sqrt{2}}C(i) \\ A(\omega^3) &= B\left(\left(-\frac{1-i}{\sqrt{2}}\right)^2\right) - \frac{1-i}{\sqrt{2}}C\left(\left(-\frac{1-i}{\sqrt{2}}\right)\right) = B(-i) - \frac{1-i}{\sqrt{2}}C(-i) \\ A(\omega^7) &= B\left(\left(\frac{1-i}{\sqrt{2}}\right)^2\right) + \frac{1-i}{\sqrt{2}}C\left(\left(\frac{1-i}{\sqrt{2}}\right)\right) = B(-i) + \frac{1-i}{\sqrt{2}}C(-i)\end{aligned}$$

**After the recursive call**

$$\begin{aligned}
A(\omega^0) &= B(1) + C(1) = 10 + 16 = 26 \\
A(\omega^4) &= B(1) - C(1) = 10 - 16 = -6 \\
A(\omega^2) &= B(-1) + iC(-1) = -2 + 12i \\
A(\omega^6) &= B(-1) - iC(-1) = -2 - 12i \\
A(\omega^1) &= B(i) + \frac{1+i}{\sqrt{2}}C(i) = 2 + 6i + \left(\frac{1+i}{\sqrt{2}}\right)(-6 + 2i) = 2 + 6i - (4 + 2i)\sqrt{2} \\
A(\omega^5) &= B(i) - \frac{1+i}{\sqrt{2}}C(i) = 2 + 6i - \left(\frac{1+i}{\sqrt{2}}\right)(-6 + 2i) = 2 + 6i + (4 + 2i)\sqrt{2} \\
A(\omega^3) &= B(-i) - \frac{1-i}{\sqrt{2}}C(-i) = 2 - 6i + \left(\frac{1-i}{\sqrt{2}}\right)(-6 - 2i) = (2 - 6i) - (4 - 2i)\sqrt{2} \\
A(\omega^7) &= B(-i) + \frac{1-i}{\sqrt{2}}C(-i) = 2 - 6i - \left(\frac{1-i}{\sqrt{2}}\right)(-6 - 2i) = (2 - 6i) + (4 - 2i)\sqrt{2}
\end{aligned}$$

Thus we have the points that we need.

• **Level 2**

Both  $B(x)$  and  $C(x)$  have degree 2 polynomial. Thus we end up with the 4 roots of unity via the recursive call,  $\omega = e^{2\pi i/4}$ ,

$$\begin{aligned}
\omega^0 &= 1 \\
\omega^2 &= e^{\pi i} = \cos(\pi) + i\sin(\pi) = -1 \\
\omega^1 &= e^{\pi i/2} = \cos(\pi/2) + i\sin(\pi/2) = i \\
\omega^3 &= e^{3\pi i/2} = \cos(3\pi/2) + i\sin(3\pi/2) = -i
\end{aligned}$$

Again we split both  $B(x)$  and  $C(x)$  into two halves,

$$\begin{aligned}
B(x) &= 3 + 6x + x^2 = B_e(x^2) + xB_o(x^2) \\
B_e(x) &= D(x) = 3 + x \\
B_o(x) &= E(x) = 6
\end{aligned}$$

$$\begin{aligned}
C(x) &= 4 + 2x + 10x^2 = C_e(x) + xC_o(x^2) \\
C_e(x) &= F(x) = 4 + 10x \\
C_o(x) &= G(x) = 2
\end{aligned}$$

Substituting the 4 roots of unity,

$$\begin{aligned}
B(\omega^0) &= D(1^2) + E(1^2) = D(1) + E(1) \\
B(\omega^2) &= D((-1)^2) - E((-1)^2) = D(1) - E(1) \\
B(\omega^1) &= D(i^2) + iE(i^2) = D(-1) + iE(-1) \\
B(\omega^3) &= D((-i)^2) - iE((-i)^2) = D(-1) - iE(-1) \\
C(\omega^0) &= F(1) + G(1) \\
C(\omega^2) &= F(1) - G(1) \\
C(\omega^1) &= F(-1) + iG(-1) \\
C(\omega^3) &= F(-1) - iG(-1)
\end{aligned}$$

After the recursive call

$$\begin{aligned}
B(\omega^0) &= D(1) + E(1) = 4 + 6 = 10 \\
B(\omega^2) &= D(1) - E(1) = 4 - 6 = -2 \\
B(\omega^1) &= D(-1) + iE(-1) = 2 + 6i \\
B(\omega^3) &= D(-1) - iE(-1) = 2 - 6i \\
C(\omega^0) &= F(1) + G(1) = 14 + 2 = 16 \\
C(\omega^2) &= F(1) - G(1) = 14 - 2 = 12 \\
C(\omega^1) &= F(-1) + iG(-1) = -6 + 2i \\
C(\omega^3) &= F(-1) - iG(-1) = -6 - 2i
\end{aligned}$$

• **Level 3**

Now we are left with 2 roots of unity for functions  $D(x), E(x), F(x), G(x)$ . At this point, we can just do arithmetic. However, I will show how the algorithm continues until the next level, which is the base case.

Again we split the 4 functions into halves,

$$\begin{aligned}
D(x) &= 3 + x = D_e(x^2) + xD_o(x^2) \\
D_e(x) &= 3 \\
D_o(x) &= 1 \\
E(x) &= 6 = E_e(x^2) + xE_o(x^2) \\
E_e(x) &= 6 \\
E_o(x) &= 0 \\
F(x) &= 4 + 10x = F_e(x^2) + xF_o(x^2) \\
F_e(x) &= 4 \\
F_o(x) &= 10 \\
G(x) &= 2 = G_e(x^2) + xG_o(x^2) \\
G_e(x) &= 2 \\
G_o(x) &= 0
\end{aligned}$$

We have 2 roots of unity,

$$\begin{aligned}
D(\omega^0) &= D_e(1^2) + D_o(1^2) = D_e(1) + D_o(1) \\
D(\omega^1) &= D_e((-1)^2) + D_o((-1)^2) = D_e(1) - D_o(1) \\
E(\omega^0) &= E_e(1) + E_o(1) \\
E(\omega^1) &= E_e(1) - E_o(1) \\
F(\omega^0) &= F_e(1) + F_o(1) \\
F(\omega^1) &= F_e(1) - F_o(1) \\
G(\omega^0) &= G_e(1) + G_o(1) \\
G(\omega^1) &= G_e(1) - G_o(1)
\end{aligned}$$

After the recursive calls

$$\begin{aligned}
D(\omega^0) &= D(1) = 3 + 1 = 4 \\
D(\omega^1) &= D(-1) = 3 - 1 = 2 \\
E(\omega^0) &= E(1) = 3 + 0 = 6 \\
E(\omega^1) &= E(-1) = 3 - 0 = 6 \\
F(\omega^0) &= F(1) = 4 + 10 = 14 \\
F(\omega^1) &= F(-1) = 4 - 10 = -6 \\
G(\omega^0) &= G(1) = 2 + 0 = 2 \\
G(\omega^1) &= G(-1) = 2 - 0 = 2
\end{aligned}$$

- **Level 4 - Base Case**

At  $\omega = 1$ , we just return our functions with 1 passed in. Now we can propagate upwards.

$$\begin{aligned}
D_e(1) &= 3, D_o(1) = 1 \\
E_e(1) &= 6, E_o(1) = 0 \\
F_e(1) &= 4, F_o(1) = 10 \\
G_e(1) &= 2, G_o(1) = 0
\end{aligned}$$



## Interpolation

After obtaining values, we need to get it back to coefficients. Let's take a look at the following matrix.

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

Let's call the middle matrix  $M_n(\omega)$ . In this special ordering, we have a Vandermonde matrix. If  $\omega^0, \omega^1, \dots, \omega^{n-1}$  are distinct,  $M_n(\omega)$  is invertible. Thus we can obtain the coefficients using

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

We need to find  $(M_n(\omega))^{-1}$  such that  $M_n(\omega)(M_n(\omega))^{-1} = I_n$ .

Lets try  $M_n(\omega)M_n(\omega^{-1})$ .

$$Z = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \dots & \omega^{-(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \dots & \omega^{-(n-1)(n-1)} \end{bmatrix}$$

For (row, column)  $(j, k)$ , we have

$$\begin{aligned} Z_{(j,k)} &= \sum_{m=0}^{n-1} \omega^{m(j-1)} \omega^{-m(k-1)} \\ &= \sum_{m=0}^{n-1} \omega^{m(j-k)} \\ &= \sum_{m=1}^n \omega^{(m-1)(j-k)} \end{aligned}$$

This becomes a geometric series with  $r = \omega^{j-k}$ . When  $j = k$ ,  $Z = n$ , which is the term for the entries on the diagonal of the matrix.

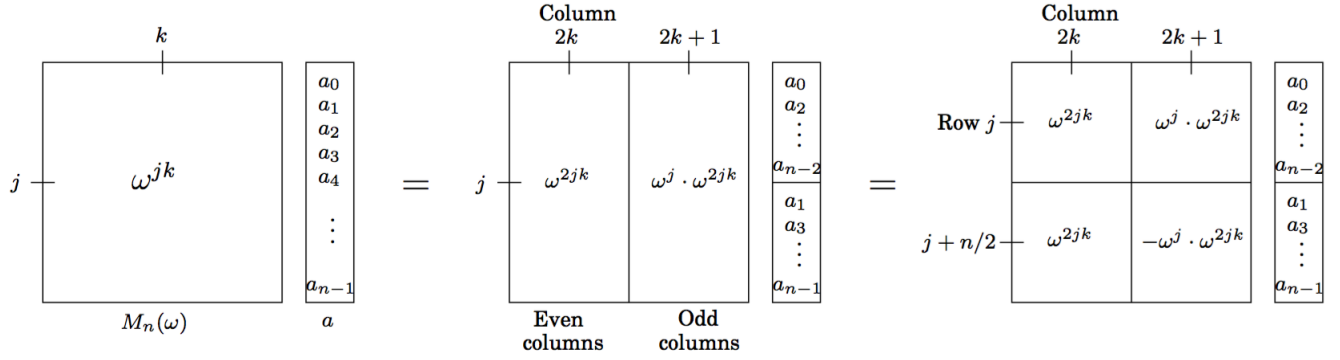
When  $j \neq k$

$$\begin{aligned} \sum_{m=1}^n \omega^{(m-1)(j-k)} &= \frac{1 - (\omega^{(j-k)})^n}{1 - \omega^{(j-k)}} \\ &= \frac{1 - \omega^{n(j-k)}}{1 - \omega^{(j-k)}} \\ \omega &= e^{2\pi i/n} \\ Z_{(j,k)} &= \frac{1 - e^{2(j-k)\pi i}}{1 - e^{2(j-k)\pi i/n}} \\ e^{2(j-k)\pi i} &= \cos(2(j-k)\pi) + i \sin(2(j-k)\pi) \\ &= 1 + i0 \\ &= 1 \\ \frac{1 - e^{2(j-k)\pi i}}{1 - e^{2(j-k)\pi i/n}} &= \frac{0}{1 - e^{2(j-k)\pi i/n}} \\ \therefore Z_{(j,k)} &= 0, j \neq k \end{aligned}$$

Thus

$$\begin{aligned}M_n(\omega)M_n(\omega^{-1}) &= nI_n \\M_n(\omega)\frac{1}{n}M_n(\omega^{-1}) &= I_n \\ \therefore M_n(\omega)^{-1} &= \frac{1}{n}M_n(\omega^{-1})\end{aligned}$$

## Matrix Form FFT



$$M_n(\omega) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(n-1)} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix} = [\omega^{jk}]$$

First, let's split the matrix where the even index columns  $2k$  are on the left side and the odd index columns  $(2k+1)$  are on the right side,  $0 \leq k \leq n/2$ .

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^2 & \dots & \omega^1 & \omega^3 & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{2(n-1)} & \dots & \omega^{(n-1)} & \omega^{3(n-1)} & \dots \end{bmatrix} = [\omega^{-2jk} \quad \omega^{-j-2jk}] = [\omega^{-2jk} \quad \omega^{-j} \cdot \omega^{-2jk}]$$

Since the column range  $k$  has decreased by a half, each element  $\omega^{jk}$  increases to  $\omega^{2jk}$ . For each  $k$ , the difference between the even column and the odd column is by a multiplicative factor of  $\omega^j$ . Thus we multiply the even column elements by  $\omega^j$  to obtain the odd column elements.

Now, let's split the matrix up and bottom. Row index is now  $0 \leq j \leq n/2$ . Upper portion row indices are  $j$ . Lower portion row indices are  $j + n/2$ .

By decreasing the domain of  $j$  by a half, the difference between the lower right half and the upper right half is  $j = n/2$ . Thus the difference is a multiplicative factor of  $\omega^{n/2}$ , which is  $-1$  as shown below.

$$\begin{aligned} \omega^n &= (e^{2\pi i/n})^n \\ &= e^{2\pi i} \\ &= \cos 2\pi + i \sin 2\pi \\ &= 1 \\ \omega^{kn} &= e^{2k\pi i} \\ &= \cos 2k\pi + i \sin 2k\pi \\ &= 1 \\ \omega^{n/2} &= (e^{2\pi i/n})^{n/2} \\ &= e^{\pi i} \\ &= \cos \pi + i \sin \pi \\ &= -1 \\ \omega^{kn/2} &= e^{k\pi i} \\ &= \cos k\pi + i \sin k\pi \\ &= -1 \end{aligned}$$

Take  $j = 1$  for example, we set the LHS as  $-1 \cdot$  upper right elements, and set RHS as lower right elements.

$$\begin{aligned} -1(\omega \cdot \omega^{2k}) &= \omega^{(1+n/2)} \cdot \omega^{2(1+n/2)k} \\ -1(\omega \cdot \omega^{2k}) &= \omega^{1+n/2} \cdot \omega^{(2+n)k} \\ -1(\omega \cdot \omega^{2k}) &= \omega \cdot \omega^{n/2} \cdot \omega^{2k} \cdot \omega^{kn} \\ -1(\omega \cdot \omega^{2k}) &= -1 \cdot \omega \cdot \omega^{2k} \end{aligned}$$

Thus to obtain the lower right half elements, we multiply the upper right half elements by  $\omega^{n/2} = -1$ .

Similarly, we can see that the multiplicative difference of the upper left elements and the lower left elements is only 1. Using the  $j = 1$  example.

$$\begin{aligned} \omega^{2j_u k} &= \omega^{2k} \\ \omega^{2j_l k} &= \omega^{2(1+n/2)k} \\ &= \omega^{(n+2)k} \\ &= \omega^{kn} \cdot \omega^{2k} \\ &= 1 \cdot \omega^{2k} \\ &= \omega^{2j_u k} \end{aligned}$$

With the multiplicative factor between the upper left and lower left being 1, we can leave as is.

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^2 & \dots & \omega & \omega^3 & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{2(n-1)} & \dots & \omega^{(n-1)} & \omega^{3(n-1)} & \dots \end{bmatrix} = \begin{bmatrix} \omega^{2jk} & \omega^j \cdot \omega^{2jk} \\ \omega^{2jk} & -\omega^j \cdot \omega^{2jk} \end{bmatrix}$$

With all four corners sharing elements  $\omega^{2jk}$ , such that  $0 \leq j \leq n/2$  and  $0 \leq k \leq n/2$ , we have a  $n/2 \times n/2$  matrix.

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{(n-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^n & \omega^{2n} & \dots & \omega^{(n-2)(n-2)} \end{bmatrix} = M_{n/2}(\omega)$$

$$\therefore M_n(\omega) = \begin{bmatrix} M_{n/2}(\omega) & \omega^j M_{n/2}(\omega) \\ M_{n/2}(\omega) & -\omega^j M_{n/2}(\omega) \end{bmatrix}$$

---

<sup>1</sup>Diagrams from Course Textbook, Algorithms by Dasgupta, Papadimitriou, and Vazirani