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 $C(x) = A(x) \cdot B(x) = c_0 + c_1x + c_2 + x^2 + \dots + c_{2d}x^{2d}$ where

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

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,

$$A_e(x) = 3 + 6x + x^2$$
$$A_o(x) = 4 + 2x + 10x^2$$

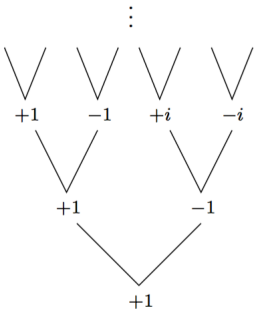
If we use positive-negative pairs x_i,

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

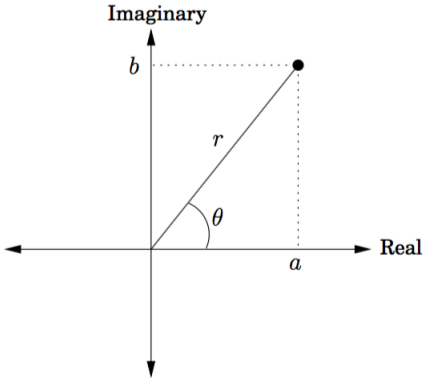
After the first level, we have to make x_0 and x_1, x_2 and $x_3, \dots$ positive negative pairs as well. If we can do this until $n = 1$, at each level we make two recursive calls to evaluate a problem that is half the size. Thus we have a recurrence

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 $+1$. Simiarily, 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).

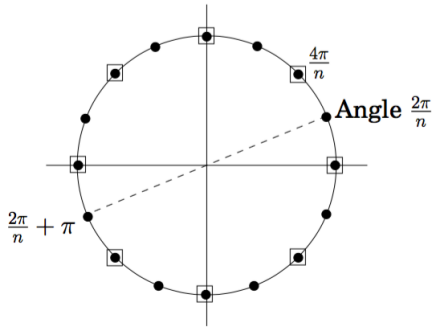
Polar coordinates: rewrite as $z = r(\cos\theta + i\sin\theta) = re^{i\theta}$, **denoted** (r, θ).

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

Examples:

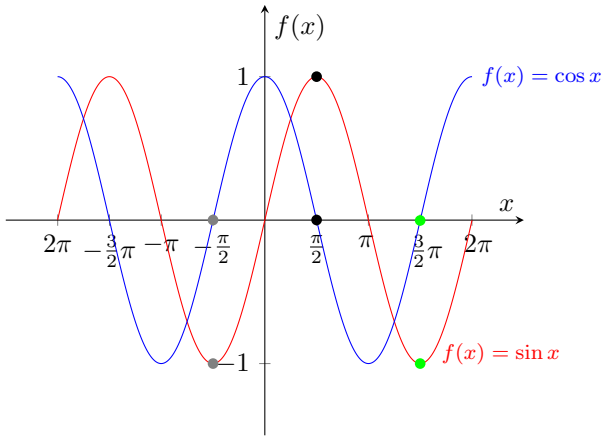
Number	-1	i	$5 + 5i$
Polar coords	$(1, \pi)$	$(1, \pi/2)$	$(5\sqrt{2}, \pi/4)$

If we use nth roots of unity, such that n is a power of two, we can keep squaring pairs at each level.
The nth roots of unity are complex numbers $1, \omega, \omega^2, \ldots, \omega^{n-1}$, 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 us $(n/2)$nd roots of unity.



These n roots are solutions to the equation $z^n = 1$. Solutions are $z = re^{ie}$ for some multiple of $2\pi/n$.
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 π will negate the number. Picking a point on the x axis, we can see that negating the points is the same as adding π on the sine and cosine curves.



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

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

Interpolation

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

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

Let's call the middle matrix $M_n(\omega)$. In this special ordering, we have a Vandermonde matrix. If $\omega^0, \omega^1, \ldots, \omega^{n-1}$ 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 $M_n(\omega)M_n(\omega^{-1})$.

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

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

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

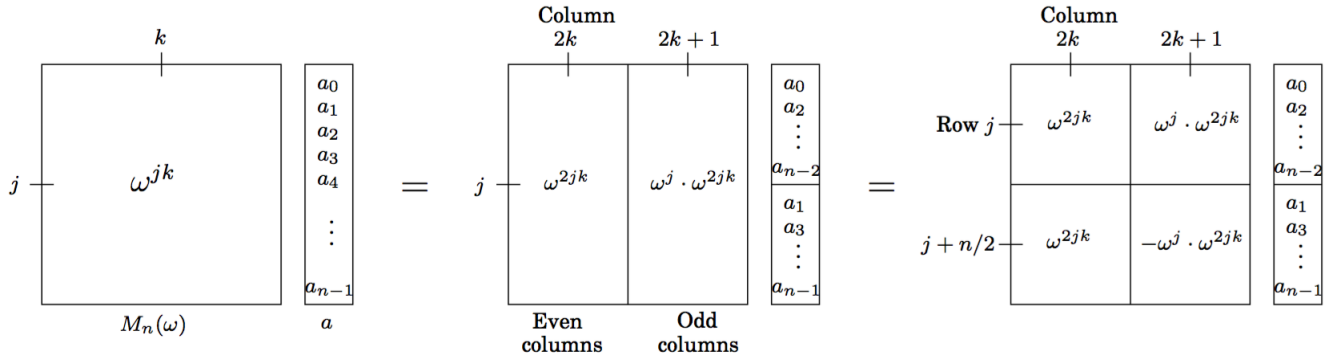
This becomes a geometric series with $r = \omega^{j-k}$. When $j = k$, $Z = n$, which is the term for the entries on the diagonal of the matrix.
When $j \neq k$

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

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



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

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, $0 \le k \le n/2$.

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

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

Now, lets split the matrix up and bottom. Row index is now $0 \le j \le n/2$. 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 ω^{2jk}, such that $0 \le j \le n/2$ and $0 \le k \le n/2$, we have a $n/2$ x $n/2$ matrix.

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

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

[1]

[1] Diagrams from Course Textbook, Algorithms by Dasgupta, Papadimitriou, and Vazirani