

Fourier Transform

Time domain \rightarrow frequency domain

Express a periodic function as a sum of sine and cosine functions

We will use a discrete version of it for fast multiplication of polynomials

First, some examination of polynomials

Polynomial as List of Coefficients

Polynomial with $n+1$ terms

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

Write as a summation

$$A(x) = \sum_{j=0}^n a_j x^j$$

Can just keep track of coefficients

$$(a_0, a_1, \dots, a_n)$$

Degree = k means a_k is the highest non-zero coefficient

Examples

$$x^3 - 2x - 1$$

Has degree 3

Has degree bound value > degree 4, 5, 17, ...

Has coefficients

$$(-1, -2, 0, 1)$$

$$x^3 + x^2 + 1$$

Has coefficients

$$(1, 0, 1, 1)$$

Easy to Add Polynomials

$A(x)$

$$(a_0, a_1, \dots, a_n)$$

$B(x)$

$$(b_0, b_1, \dots, b_n)$$

$A(x) + B(x)$

$$(a_0 + b_0, a_1 + b_1, \dots, a_n + b_n)$$

$$(-1, -2, 0, 1)$$

$$(1, 0, 1, 1)$$

$$\hline (0, -2, 1, 2)$$

$$2x^3 + x^2 - 2x$$

Multiplication is More Complicated

$$\begin{array}{r} x^3 - 2x - 1 \\ x^3 + x^2 + 1 \end{array}$$

Consider x^3 term in the result. Want to multiply all terms whose exponents sum to 3.

$$(x^3)(1) + (-2x)(x^2) + (-1)(x^3)$$

$$x^3 - 2x^3 - x^3 = -2x^3$$

More Generally

Suppose $A(x) \cdot B(x)$ has coefficients

$$(c_0, c_1, \dots, c_{2n})$$

Then

$$c_j = \sum_{k=0}^j a_k b_{j-k}$$

if $k > n$
 $a_k = 0$
 $b_k = 0$

Note, for $k > n$

Example

$$\begin{aligned} & \downarrow \\ & (-1, -2, 0, 1) \\ & (1, 0, 1, 1) \\ c_0 &= (-1)(1) = -1 \\ c_1 &= (-1)(0) + (-2)(1) = -2 \\ c_2 &= (-1)(1) + (-2)(0) + (0)(1) = -1 \\ c_3 &= (-1)(1) + (-2)(1) + (0)(0) + \\ & \quad (1)(1) = -2 \\ c_4 &= (-2)(1) + (0)(1) + (1)(0) = -2 \\ c_5 &= (0)(1) + (1)(1) = 1 \\ c_6 &= (1)(1) = 1 \\ & (-1, -2, -1, -2, -2, 1, 1) \\ & x^6 + x^5 - 2x^4 - 2x^3 - x^2 - 2x - 1 \end{aligned}$$

Point-Value Representation

A polynomial of degree n is uniquely determined by its value at $n+1$ distinct points *Fundamental Theorem of Algebra*

$$A(x) \{ (x_0, A(x_0)), (x_1, A(x_1)), \dots, (x_n, A(x_n)) \}$$

Example $A(x) = x^3 - 2x + 1$

$$\begin{aligned} x_i & (0, 1, 2, 3) \\ A(x_i) & (1, 0, 5, 22) \end{aligned}$$

$$\{(0, 1), (1, 0), (2, 5), (3, 22)\}$$

Algorithm Design & Analysis

Interpolating Back to Coefficients $A(x_i)$

Can go from point-value set $\{(x_i, y_i)\}$
back to coefficients

Lagrange's formula

$$A(x) = \sum_{k=0}^n y_k \left\{ \frac{\prod_{j \neq k} (x - x_j)}{\prod_{j \neq k} (x_k - x_j)} \right\}$$

formal variable $\left\{ \begin{array}{l} \text{polynomial} \\ \text{for } x = x_1, x_2, \dots, x_{k-1}, x_{k+1}, \dots, x_n \end{array} \right\}$
 $\left. \begin{array}{l} \text{polynomial} \\ \text{number} \end{array} \right\} = 1 \text{ if } x = x_k$

Lecture Notes 6 David Maier **9**

Algorithm Design & Analysis

Example

$\{(0, 1), (1, 0), (2, 5), (3, 22)\}$

$$1 \cdot \frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)} = 1 \cdot \frac{x^3 - 6x^2 + 11x - 6}{-6}$$

$$0 \cdot \frac{(x-0)(x-2)(x-3)}{(1-0)(1-2)(1-3)}$$

$$5 \cdot \frac{(x-0)(x-1)(x-3)}{(2-0)(2-1)(2-3)} = \frac{x^3}{-6} + 0 + \frac{5x^3}{-2} + \frac{22x^3}{6}$$

$$22 \cdot \frac{(x-0)(x-1)(x-2)}{(3-0)(3-1)(3-2)} = \frac{-1 + 0 - 15 + 22}{6} x^3 = \frac{6}{6} x^3 = x^3$$

Lecture Notes 6 David Maier **10**

Addition

Adding polynomials in point-value form is $O(n)$ (if x 's are the same)

$(x_i, A(x_i))$
 $(x_i, B(x_i))$

} use same x_0, x_1, \dots, x_n

$(x_i, A(x_i) + B(x_i))$

$x^3 + x^2 + 1$

$\{ (0, 1), (1, 3), (2, 13), (3, 37) \}$
 $\{ (0, 1), (1, 0), (2, 5), (3, 22) \}$

$\{ (0, 2), (1, 3), (2, 18), (3, 59) \}$

Multiplication

Same works for multiplication, kind of

$(x_i, A(x_i))$
 $(x_i, B(x_i))$

$A * B(x_i)$

$(x_i, A(x_i) \cdot B(x_i))$

Problem: $A(x)B(x)$ has degree $2n$, but this only gives $n+1$ coefficients. We need $2n+1$ coefficients

Need to start with more evaluation points

Algorithm Design & Analysis

Need 7 Coefficients Here

$$\{(0, 1), (1, 3), (2, 13), (3, 37), (-1, 2), (-2, -3), (-3, -20)\}$$

$$\{(0, 1), (1, 0), (2, 5), (3, 22), (-1, 1), (-2, -3), (-3, -17)\}$$

Result

$$\{(0, 1), (1, 0), (2, 65), (3, 814), (-1, 2), (-2, 9), (-3, 340)\}$$

Usually use $2n+2$ coefficients

Lecture Notes 6 David Maier **13**

Algorithm Design & Analysis

One Way to Multiply $A(n), B(n)$ of Degree n

Given as coefficient lists

(a_0, \dots, a_n)
 (b_0, \dots, b_n)

coefficient form

$O(n^2)$ evaluation

(c_0, \dots, c_{2n})

coefficient form

$O(n^2)$ interpolate

$((x_0, A(x_0)), \dots, (x_{2n}, A(x_{2n})))$
 $((x_0, B(x_0)), \dots, (x_{2n}, B(x_{2n})))$

$O(n \log n)$ FFT + inverse

$O(n)$ pairwise multiply

$((x_0, A(x_0) \cdot B(x_0)), \dots, (x_{2n}, A(x_{2n}) \cdot B(x_{2n})))$

point-value

point-value

Lecture Notes 6 David Maier **14**

Algorithm Design & Analysis

Why Bother

Have we gained anything?
 Evaluation and interpolation are $O(n^2)$
 in general

$O(n^2)$ over all

However, if we correctly pick the x_i ,
 we can do both in $O(n \log(n))$, giving
 $O(n \log(n))$ over all.

Lecture Notes 6 David Maier **15**

Algorithm Design & Analysis

Roots of Unity

Use n^{th} roots of 1 (unity)
 Any ω such that

$\omega^n = 1$

What are the 4th roots of unity?
 1, -1, i , $-i$ *$\sqrt{-1} = i$*

What are the 8th roots of unity?
 All of the above work, but there are 4 more!

if multiply any 2 by each other you get another one.

$\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)^2 = \frac{1}{2} + \frac{2i}{2} + \frac{i^2}{2} = i$

$\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}, -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}, \frac{-1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$

Lecture Notes 6 David Maier **16**

Pattern for Roots of Unity

There are n n^{th} roots of unity

$$e^{k/n(2\pi i)}, k = 0, \dots, n-1$$

Note that

$$e^{ui} = \cos(u) + i \cdot \sin(u)$$

Here u represents an angle in radians

So

$$e^{k/n(2\pi i)} = \cos\left(\frac{k}{n} 2\pi\right) + i \cdot \sin\left(\frac{k}{n} 2\pi\right)$$

Check that it's a root

$$(e^{k/n(2\pi i)})^n = e^{k(2\pi i)} = \cos(k \cdot 2\pi) + i \sin(k \cdot 2\pi) = 1$$

Principal Root

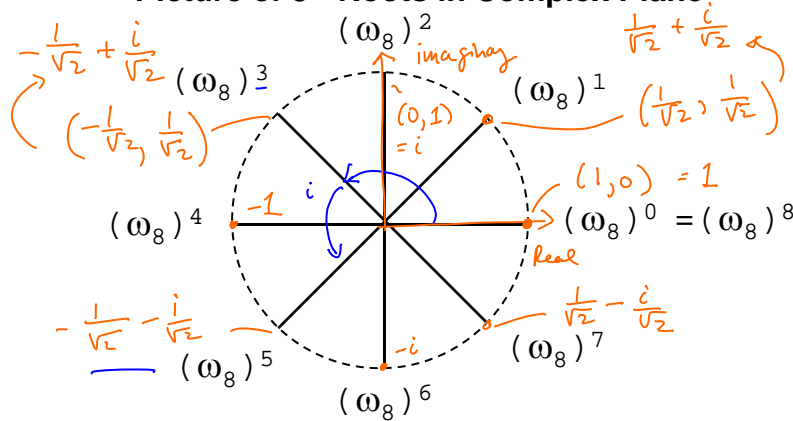
The *principal* n^{th} root of unity is

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

Get all of them by taking power $k = 0, \dots, n-1$

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

Picture of 8th Roots in Complex Plane



These roots act like the integers mod 8 under +

$$(\omega_8)^j (\omega_8)^k = (\omega_8)^{j+k} = (\omega_8)^r \quad r = (j+k) \bmod 8$$

$$(\omega_8)^3 \cdot (\omega_8)^2 = (\omega_8)^5 \quad (\omega_8)^7 \cdot (\omega_8)^6 = (\omega_8)^{13} = (\omega_8)^5$$

Cancellation Lemma

An example

$$(\omega_{24})^6 = \omega_4$$

$$(e^{1/24(2\pi i)})^6 = e^{6/24(2\pi i)} = e^{1/4(2\pi i)} = \omega_4$$

In general

$$\omega_n = (\omega_{dn})^d$$

More generally

$$\omega_n^k = (\omega_{dn})^{dk}$$

Special case

$$\omega_{2r}^r = \omega_2 = -1$$

Squares of 2rth roots

ω_{2r}^k and $(\omega_{2r})^{k+r}$

have the same square

$$(\omega_{2r}^k)^2 = (\omega_{2r}^{2k}) = (\omega_r)^k$$

$$(\omega_{2r}^{k+r})^2 = \omega_{2r}^{2k} \cdot \omega_{2r}^{2r} = (\omega_{2r})^{2k} = (\omega_r)^k$$

which is an rth root of unity

$$\{(\omega_{2r}^0)^2, (\omega_{2r}^1)^2, (\omega_{2r}^2)^2, \dots, (\omega_{2r}^{2r-1})^2\}$$

$$= \{\omega_r^0, \omega_r^1, \omega_r^2, \dots, \omega_r^{r-1}\}$$

Exercise:

$$\omega_{2r}^k = -(\omega_{2r})^{k+r}$$

Summing Up nth Roots

Exercise:

$$\omega_{2r}^k = -(\omega_{2r})^{k+r}$$

So:

$$\omega_{2r}^0 + \omega_{2r}^1 + \omega_{2r}^2 + \dots + \omega_{2r}^{2r-1} = 0$$

Actually

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

$$\sum_{j=0}^{n-1} (\omega_n^k)^j = 0$$

$$\sum_{j=0}^{n-1} a^j = \frac{a^n - 1}{a - 1}$$

k is not divisible by n

$$\frac{(\omega_n^k)^n - 1}{\omega_n^k - 1} = \frac{1 - 1}{1 - 1} = 0$$

Discrete Fourier Transform (DFT)

For a polynomial $A(x)$ of degree bound n
 Point-value representation at the n^{th}
 roots of unity

$$\{(\omega_n^0, A(\omega_n^0)), (\omega_n^1, A(\omega_n^1)), (\omega_n^2, A(\omega_n^2)), \dots, (\omega_n^{n-1}, A(\omega_n^{n-1}))\}$$

If $A(x)$ has coefficients $(a_0, a_1, \dots, a_{n-1})$

$$Y_k = A(\omega_n^k) = \sum_{j=0}^{n-1} a_j (\omega_n^k)^j$$

DFT of $(a_0, a_1, \dots, a_{n-1})$ is
 $(Y_0, Y_1, \dots, Y_{n-1})$

Fast Fourier Transform

Reuse work when n is a power of 2

Split up $A(x)$

$$6 + 3x + 5x^2 - 2x^3 + x^4 - 8x^5 + x^6 + 3x^7$$

$$B.0(x) = 6 + 5x^2 + x^4 + x^6$$

$$B.1(x) = 3x - 2x^3 - 8x^5 + 3x^7 = x(3 - 2x^2 - 8x^4 + 3x^6)$$

$$A(x) = B.0(x) + B.1(x)$$

Consider $let y = x^2$

$$A.0(y) = 6 + 5y + y^2 + y^3$$

$$A.1(y) = 3 - 2y - 8y^2 + 3y^3 =$$

What is

$$A.0(x^2) + x \cdot A.1(x^2)$$

Algorithm Design & Analysis

How to Evaluate A(x)

Can evaluate A(x) at n points
 $x_0, x_1, x_2, \dots, x_{n-1}$

By evaluating A.0(y) and A.1(y)
 $x_0^2, x_1^2, x_2^2, \dots, x_{n-1}^2$

What is the degree of A.0(y) and A.1(y)?

$\frac{n-1}{2}$

 at $\frac{n-1}{2}$ points

Plus a little bit $O(n)$ of work to combine results

Lecture Notes 6 David Maier **25**

Algorithm Design & Analysis

Evaluating at nth Roots

If the x_i 's are the nth roots of unity, where $n = 2r$

So

$x_j = \omega_n^j = \omega_{2r}^j$
 $(x_j)^2 = (\omega_n^j)^2 = \omega_{2r}^{2j} = \omega_r^j$

← one of the rth roots of unity

Instead of 2r points, we only have r points to evaluate

Evaluating one polynomial of degree 2r-1 at 2r points =

Evaluating two polynomials of degree r-1 at r points **plus**

$O(r)$ work to combine results.

Time Complexity: $O(n \lg n)$

Lecture Notes 6 David Maier **26**

Recursive FFT

(a_0, \dots, a_{n-1})
 n is a power of 2

Basis

$$\text{FFT}(a_0) = a_0$$

Recursive step

$$\text{FFT}(a_0, a_1, \dots, a_{n-1})$$

Let w_n be principal n^{th} root of unity

$$w \leftarrow 1$$

$$a.0 = (a_0, a_2, a_4, \dots, a_{n-2})$$

$$a.1 = (a_1, a_3, a_5, \dots, a_{n-1})$$

$$y.0 = \text{FFT}(a.0) = (y.0_0, y.0_1, \dots)$$

$$y.1 = \text{FFT}(a.1) = (y.1_0, y.1_1, y.1_2, \dots)$$

for $k \leftarrow 1$ to $(n/2)-1$

$$Y_k \leftarrow Y.0_k + w(y.1_k)$$

$$Y_{k+(n/2)} \leftarrow Y.0_k - w(y.1_k)$$

$$w \leftarrow w \cdot w_n$$

return $(y_0, y_1, \dots, y_{n-1})$

Are the Values Right?

Note

$$Y.0_k = A.0(\omega_{n/2}^k) = A.0(\omega_n^{2k})$$

$$Y.1_k = A.1(\omega_{n/2}^k) = A.1(\omega_n^{2k})$$

So

$$Y_k = Y.0_k + \omega_n^k \cdot Y.1_k$$

$$= A.0(\omega_n^{2k}) + \omega_n^k \cdot A.1(\omega_n^{2k}) = A(\omega_n^k)$$

$$Y_{k+(n/2)} = Y.0_k - \omega_n^k \cdot Y.1_k$$

$$= Y.0_k + \omega_n^{k+(n/2)} \cdot Y.1_k$$

$$= A.0(\omega_n^{2k}) + \omega_n^{k+(n/2)} \cdot A.1(\omega_n^{2k}) =$$

$$A.0(\omega_n^{2k+n}) + \omega_n^{k+(n/2)} \cdot A.1(\omega_n^{2k+n}) = A(\omega_n^{k+n/2})$$

$$\left. \begin{aligned} \omega_n^{k+n/2} &= -\omega_n^k \\ \omega_n^{2k+n} &= \omega_n^{2k} \end{aligned} \right\}$$

Inverse DFT (Interpolation)

DFT⁻¹

- Reverse y_i 's and a_j 's
- Change $\omega_n \rightarrow \omega_n^{-1}$
- Divide resulting coefficients by n