

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

$$A(x) = \sum$$

Can just keep track of coefficients

Degree = k means

Examples

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

Has degree 3

Has degree bound

Has coefficients

()

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

Has coefficients

()

Easy to Add Polynomials

$A(x)$

(a_0, a_1, \dots, a_n)

$B(x)$

(b_0, b_1, \dots, b_n)

$A(x) + B(x)$

(, , ...,)

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

$(1, 0, 1, 1)$

Multiplication is More Complicated

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

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

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

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

More Generally

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

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

Then

$$c_j = \sum a_k b_{j-k}$$

Note, for $k > n$

Example

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

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

$$c_0 = (-1)(1) =$$

$$c_1 = (-1)(0) + (-2)(1) =$$

$$c_2 = (-1)(1) + (-2)(0) + (0)(1) =$$

$$c_3 = (-1)(1) + (-2)(1) + (0)(0) + (1)(1) =$$

$$c_4 = (-2)(1) + (0)(1) + (1)(0) =$$

$$c_5 = (0)(1) + (1)(1) =$$

$$c_6 = (1)(1) =$$

Point-Value Representation

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

$$A(x)$$

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

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

$$x_i \quad (0, 1, 2, 3)$$

$$A(x_i) \quad (, , ,)$$

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

Interpolating Back to Coefficients

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

Lagrange's formula

$$A(x) = \sum Y_k \frac{\prod (x - x_j)}{\prod (x_k - x_j)}$$

Example

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

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

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

$$5 \cdot \frac{(x-0)(x-1)(x-3)}{(2-0)(2-1)(2-3)}$$

$$22 \cdot \frac{(x-0)(x-1)(x-2)}{(3-0)(3-1)(3-2)}$$

Addition

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

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

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

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

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

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

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

$$\{(0, \quad), (1, \quad), (2, \quad), (3, \quad)\}$$

Multiplication

Same works for multiplication, kind of

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

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

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

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

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

$$\{(0, \quad), (1, \quad), (2, \quad), (3, \quad), (-1, \quad), (-2, \quad), (-3, \quad)\}$$

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)

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

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

↓

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

Lecture Notes 6 David Maier **14**

Why Bother

Have we gained anything?

Evaluation and interpolation are $O(n^2)$
in general

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

Roots of Unity

Use n^{th} roots of 1 (unity)

Any ω such that

What are the 4th roots of unity?

1, -1,

What are the 8th roots of unity?

All of the above work, but there are 4 more!

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

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

Check that it's a root

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

Principal Root

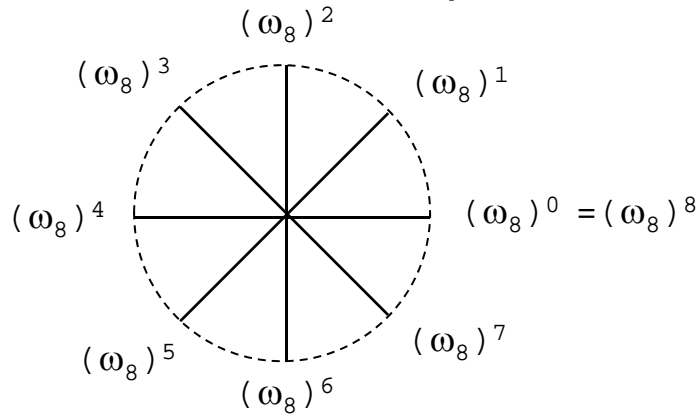
The *principal* n^{th} root of unity is

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

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

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

Picture of 8th Roots in Complex Plane



These roots act like the integers mod 8 under +

$$(\omega_8)^j (\omega_8)^k = (\omega_8)^{j+k} =$$

Cancellation Lemma

An example

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

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

In general

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

More generally

$$\omega_n^k = (\omega_n)^k$$

Special case

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

Squares of 2^rth roots

ω_{2r}^k and $(\omega_{2r})^{k+r}$

have the same square

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

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

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:

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

Actually

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

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

$$Y_k = A(\omega_n^k) =$$

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 $A(x)$

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

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

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

$$A(x) =$$

Consider

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

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

What is

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

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 $A.1(y)$

$$x_0, x_1, x_2, \dots, x_{n-1}$$

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

Evaluating at n^{th} Roots

If the x_i 's are the n^{th} roots of unity,
where $n = 2r$

So

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

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

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**

Time Complexity

Recursive FFT

```

FFT(a0) =
FFT(a0, a1, ..., an-1)
Let ωn be principal nth root of unity
w ← 1
a.0 = (a0, a2, a4, ..., an-2)
a.1 = (a1, a3, a5, ..., an-1)
y.0 =
y.1 =
for k ← 1 to (n/2)-1
    Yk ← Y.0k +
    Yk+(n/2) ← Y.0k -
    w ← w·ωn
return( )
    
```

Are the Values Right?

Note

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

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

So

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

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

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

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

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

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