Multiplying Polynomials:

Monday 10/20/14

Example: 2 polynomials of degree $d=2$:

$$A(x) = 1 + 2x + 3x^2 = a_0 + a_1 x + a_2 x^2$$
$$B(x) = 2 - x + 4x^2 = b_0 + b_1 x + b_2 x^2$$

Goal: compute their product:

$$C(x) = A(x)B(x) = (1+2x+3x^2)(2-x+4x^2)$$
$$= 2 + 3x + 8x^2 + 5x^3 + 12x^4$$
$$= c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4$$

$c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$, $c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$ ($a_0 b_3$ and $a_3 b_0$ are 0)
$= a_1 b_2 + a_2 b_1$

$c_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = a_2 b_2$

In general: Given the coefficients $a = (a_0, a_1, a_2, \ldots, a_d)$ & $b = (b_0, b_1, \ldots, b_d)$ for polynomials $A(x) = \sum_{i=0}^{d} a_i x^i$ & $B(x) = \sum_{i=0}^{d} b_i x^i$,

Compute the coefficients $c = (c_0, c_1, \ldots, c_{2d})$ for the polynomial $C(x) = \sum_{i=0}^{2d} c_i x^i = A(x)B(x)$

where

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$
$$= \sum_{i=0}^{k} a_i b_{k-i}$$
$$= \sum_{i=\max\{0,k-d\}}^{\min\{k,d\}} a_i b_{k-i}$$

Vector $C = a * b$ is called the convolution of vectors a & b.

Naive approach: $O(k)$ time for c_k, $O(\ell^2)$ total time

Using FFT: $O(\ell \log \ell)$ total time.

Sample application: Pattern matching

Given binary strings $S = s_0 s_1 \cdots s_{n-1}$ (string) & $P = p_0 p_1 \cdots p_{m-1}$ (pattern)

where $n \geq m$.

Does P appear in S?

In other words, is there a position k where:

$$s_k s_{k+1} \cdots s_{k+m-1} = p_0 p_1 \cdots p_{m-1}?$$

Example: $S = aababbabba$ $P = abba$

Idea: map $a \to -1$ & $b \to +1$

So $S = -1, -1, 1, -1, 1, 1, -1, 1, 1, -1$ & $P = -1, 1, 1, -1$

Consider 2 strings of length m, say $p = abba$ & $q = aaba$

So $p = (-1, 1, 1, -1)$ & $q = (-1, -1, 1, -1)$

Note $p \cdot q = 1 - 1 + 1 + 1 = 2$ ← dot product

in general:

if $p = q$ then $p \cdot q = m$

if $p \neq q$ then $p \cdot q < m$.

To check if $s_k \cdots s_{k+m-1} = p_0 \cdots p_{m-1}$

we want to check if $s_k p_0 + s_{k+1} p_1 + \cdots + s_{k+m-1} p_{m-1} = m$

First try: let $a = (p_0, p_1, \ldots, p_{m-1})$ & $b = (s_0, s_1, \ldots, s_{n-1})$ in ± 1 format

What's c_k where $c = a * b$.

$$c_1 = p_0 s_0,\ c_1 = p_0 s_1 + p_1 s_0,\ \ldots;\ c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

$k = m-1$: $c_{m-1} = p_0 s_{m-1} + p_1 s_{m-2} + \cdots + p_{m-1} s_0$

looks like what we want but need to reverse p or s.

Attempt 2: let $a = (p_{m-1}, p_{m-2}, \ldots, p_0)$

& $b = (s_0, s_1, \ldots, s_{n-1})$

Compute $c = a * b$.

What is c_{k+m-1}?

$$c_{k+m-1} = p_{m-1}s_{k+m-1} + p_{m-2}s_{k+m-2} + \cdots + p_0 s_k$$

Thus to check if

$$s_k s_{k+1} \cdots s_{k+m-1} = p_0 \cdots p_{m-1}$$

we just check if $c_{k+m-1} = m$?

So just scan the vector c to check for any entries $= m$.

Back to multiplying Polynomials:

Two ways to represent a polynomial $A(x) = a_0 + a_1 x + \dots + a_d$

1) coefficients: $a_0, a_1, \dots, a_d$

or 2) values: $A(x_0), A(x_1), \dots, A(x_d)$

Lemma: A degree d polynomial is uniquely characterized by its values at any $d+1$ distinct points

example: a line has $d=1$ & is defined by any 2 points.

We assume input/output is in coefficients representation, but the values representation is useful for multiplying polynomials:

Given $A(x_0), \dots, A(x_{2d})$ & $B(x_0), \dots, B(x_{2d})$

then $C(x_i) = A(x_i) B(x_i)$ for $i = 0, 1, \dots, 2d$

& this defines $C(x)$.

Need to convert between coefficients $\longleftrightarrow$ values

FFT: does so for carefully chosen set of points.

Consider Poly $A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$
where n is a power of 2

We are given $a = (a_0, a_1, \ldots, a_{n-1})$
We want to output $A(x_1), A(x_2), \ldots, A(x_{2n})$
for $2n$ points that we choose

How should we choose these points?

Key idea: Suppose we have n points $x_1, \ldots, x_n$
& the other n are opposites: $x_{n+1} = -x_1, \ldots, x_{2n} = -x_n$
So the $2n$ points are $\pm x_1, \ldots, \pm x_n$

Note $A(x_i)$ & $A(-x_i)$ are the same for the even terms
& opposite for odd terms.

So split $A(x)$ into even & odd terms.

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

$a_{even} = (a_0, a_2, \ldots, a_{n-2})$

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

$a_{odd} = (a_1, a_3, a_5, \ldots, a_{n-1})$

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

Hence, $A(x_i) = A_{even}(x_i^2) + x_i A_{odd}(x_i^2)$

& $A(x_{n+i}) = A(-x_i) = A_{even}(x_i^2) - x_i A_{odd}(x_i^2)$

So given $A_{even}(y_1), \ldots, A_{even}(y_n)$

& $A_{odd}(y_1), \ldots, A_{odd}(y_n)$

for $y_1 = x_1^2, \ldots, y_n = x_n^2$

then we get in $O(n)$ time

$A(x_1), \ldots, A(x_n), \underbrace{A(x_{n+1})}_{A(-x_1)}, \ldots, \underbrace{A(x_{2n})}_{A(-x_n)}$

Note, $A_{even}(y)$ & $A_{odd}(y)$ are of degree $\frac{n-2}{2} = \frac{n}{2} - 1$ whereas $A(x)$ had degree $n-1$.

So to solve the problem of evaluating $A(x)$ of degree $n-1$ at $2n$ points

→ need $A_{even}(y)$ & $A_{odd}(y)$ of degree $\frac{n}{2} - 1$ at n p

⇒ Divide & conquer!

$T(n) = 2T\left(\frac{n}{2}\right) + O(n) = O(n \log n)$

But what about the next round?

Need that $x_1^2, x_2^2, \ldots, x_n^2$ are $\pm$ pairs so:

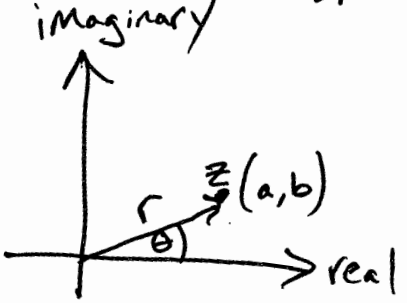
$$x_1^2 = -x_{\frac{n}{2}+1}^2$$
$$x_2^2 = -x_{\frac{n}{2}+2}^2$$
$$\vdots$$
$$x_{\frac{n}{2}}^2 = -x_n^2$$

But x_1^2 and $x_{\frac{n}{2}+1}^2$ are both ≥ 0 so impossible!

unless we use complex numbers.

Complex numbers:

$a+bi$ represented as (a,b) in the complex plane or (r,θ) in polar coordinates



for Polar (r,θ):

$$z = r(\cos\theta + i\sin\theta) = re^{i\theta}$$

this is Euler's formula
(prove using Taylor expansions)

Polar is convenient:

Multiplying: $(r_1, \theta_1) \times (r_2, \theta_2) = (r_1 r_2, \theta_1 + \theta_2)$

So if $r=1$, for $z=(1,\theta)$

then $z^n = (1, n\theta)$

And since $-1 = (1, \pi)$

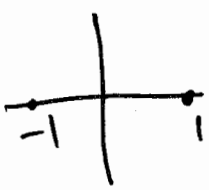
then if $z=(r,\theta)$ then $-z = (r, \theta+\pi)$

n^{th} complex roots of unity are solutions to $z^n = 1$.

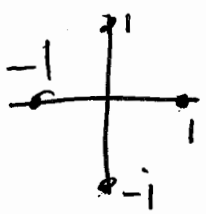
they are $z=(1,\theta)$ where $z^n = (1, 2\pi)$

Hence, they have $\theta = \frac{2\pi}{n} j$ for $j = 0, 1, \ldots, n-1$.

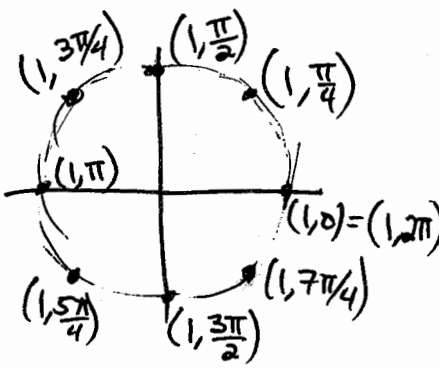
$n=2$:



$n=4$:



$n=8$:



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

The n^{th} roots are $\omega_{0,n}, \omega_{1,n}, \ldots, \omega_{n-1,n}$

For even n: $\omega_{i,n} = -\omega_{\frac{n}{2}+i,n}$

For n which is a power of 2:

$$(\omega_{j,n})^2 = \left(1, \frac{2\pi j}{n}\right) \times \left(1, \frac{2\pi j}{n}\right) = \left(1, \frac{2\pi j}{n/2}\right) = \omega_{j,n/2}$$

$$\& \quad (\omega_{\frac{n}{2}+j,n})^2 = (-\omega_{j,n})^2 = \omega_{j,n/2}$$

So for $X_0 = \omega_{0,n}, X_1 = \omega_{1,n}, \ldots, X_{n-1} = \omega_{n-1,n}$

then $Y_0 = X_0^2 = X_{\frac{n}{2}}^2 = \omega_{0,\frac{n}{2}}$

$\vdots$

$$Y_{\frac{n}{2}-1} = X_{\frac{n}{2}-1}^2 = X_{n-1}^2 = \omega_{\frac{n}{2}-1,\frac{n}{2}}$$

the squares of the n^{th} roots are the $\frac{n}{2}^{\text{th}}$ roots and they have the $\pm$ property.

FFT$(A, 2n)$:

input: coefficients $a_0, \ldots, a_{n-1}$ for Polynomial $A(x)$ of degree where n is a power of 2

output: $A(\omega_{0,2n}), A(\omega_{1,2n}), \ldots, A(\omega_{2n-1,2n})$ = Value of $A(x)$ at $2n$th roots of unity.

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

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

Call FFT(A_{even}, n) to get $A_{even}(\omega_{j,n})$ for $j=0,\ldots,n-1$
Call FFT(A_{odd}, n) to get $A_{odd}(\omega_{j,n})$ for $j=0,\ldots,n-1$

For $j=0 \to n-1$

$$A(\omega_{j,2n}) = A_{even}(\omega_{j,n}) + \omega_{j,2n} A_{odd}(\omega_{j,n})$$
$$A(\omega_{n+j,2n}) = A_{even}(\omega_{j,n}) - \omega_{j,2n} A_{odd}(\omega_{j,n})$$

Return $(A(\omega_{0,2n}), A(\omega_{1,2n}), \ldots, A(\omega_{2n-1,2n}))$

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

To multiply polynomials $A(x)$ & $B(x)$ of degree $\leq n-1$

- Run FFT to get both at $2n^{\text{th}}$ roots of unity
- Compute $C(\omega_{j,2n}) = A(\omega_{j,2n})B(\omega_{j,2n})$ for $j = 0 \to 2n-1$
- Then do "inverse" FFT to convert from values to coefficients of $C(x)$.