Today.

...Complex numbers, polynomials today. FFT.

Multiplying polynomials.

$(1+2x+3x^2)(4+3x+2x^2)$

Coefficient of x^4 in result?

(A) 6

(B) 5

(A) 6 of course!

Coeefficient of x^2 in result?

Uh oh...

Multiplying polynomials.

$(1+2x+3x^2)(4+3x+2x^2)$

x^0	$((1)(4))$	$=4$
x^1	$((1)(3)+(2)(4))$	$=11$
x^2	$((1)(2)+(2)(3)+(3)(4)))$	$=20$
x^3	$((2)(2)+(3)(3))$	$=13$
x^4	$((3)(2))$	$=6$

$4+11x+20x^2+13x^3+6x^4$

Given:

$a_0+a_1x+\cdots a_dx^d$ In example: $a_0=1, a_1=2, a_2=3$

$b_0+b_1x+\cdots b_dx^d$ In example: $b_0=4, b_1=3, b_2=2$

Product: $c_0+c_1x+\cdots c_{2d}x^{2d}$

$$c_k = \sum_{0\le i\le k} a_i * b_{k-i}.$$

E.g.: $c_2 = a_2b_0+a_1b_1+a_0b_2$.

Multiplying polynomials.

Multiply: $(1+2x+3x^2)(4+3x+2x^2)$

Given:

$a_0+a_1x+\cdots a_dx^d$ In example: $a_0=1, a_1=2, a_2=3$

$b_0+b_1x+\cdots b_dx^d$ In example: $b_0=4, b_1=3, b_2=2$

Product: $c_0+c_1x+\cdots c_{2d}x^{2d}$

$$c_k = \sum_{0\le i\le k} a_i * b_{k-i}.$$

E.g.: $c_2 = a_2b_0+a_1b_1+a_0b_2$.

Runtime?

(A) $O(d)$

(B) $O(d\log d)$

(C) $O(n^2)$

(D) $O(d^2)$

Time: $O(k)$ multiplications for each k up to $k=2d$.

$\implies O(d^2)$.

or (D) ..will use n as parameter shortly. so (C) also.

Hmmm...

$O(d^2)$ time!

Quadratic Time!

Can we do better?

Yes? No?

How?

Use different representation.

Another representation.

Represent a line?

Slope and intercept! a_0, a_1

How many points determine a line? 2

Represent line as two points on line instead of coefficients!

How many points determine a parabola (a quadratic polynomial)? 3

How many points determine a a degree d polynomial?

$d+1$

How to find points on function?

plug in x-values...and evaluate.

How to find “line” from points?

Solve two variable system of equations!

How to find polynomial from points?

Solve $d+1$ variable system of equations!

Point-value representation.

$A(x_0), \cdots, A(x_{2d})$
$B(x_0), \cdots, B(x_{2d})$

Product: $C(x_0), \cdots, C(x_{2d})$

$$C(x_i) = A(x_i)B(x_i)$$

$O(d)$ multiplications!

Given: $a_0, \ldots, a_d$ and $b_0, \ldots, b_d$.
Evaluate: $A(x), B(x)$ on $2d+1$ points: $x_0, \cdots, x_{2d}$.
Recall(from CS70): unique representation of polynomial.

Multiply: $A(x)B(x)$ on points to get points for $C(x)$.

Interpolate: find $c_0 + c_1 x + c_2 x^2 + \cdots c_{2d} x^{2d}$.

Interpolation

Points: $(x_0, y_0), \ldots (x_d, y_d)$.

Lagrange:

$\Delta_i(x) = \Pi_{i \neq j} \frac{x - x_j}{x_i - x_j}$

$P(x) = \sum_i y_i \Delta_i(x)$.

Correctness: $\Delta_i(x_j) = 0$ for $x_i \neq x_j$ and $\Delta_i(x_i) = 1$. Thus, $P(x_i) = y_i$.

Linear system:

$c_0 + c_1 x_0 + c_2 x_0^2 \cdots c_d x_0^d = y_0$.
$c_0 + c_1 x_1 + c_2 x_1^2 \cdots c_d x_1^d = y_1$.
$\vdots$
$c_0 + c_1 x_d + c_2 x_d^2 \cdots c_d x_d^d = y_d$.

Has solution? Lagrange.
Unique?
At most d roots in any degree d polynomial.
Not unique $\implies P(x)$ and $Q(x)$ where $P(x_i) = Q(x_i)$.
$P(x) - Q(x)$ has $d+1$ roots. Contradicts not unique.

What is it good for?

What is the point-value representation good for (from CS70)?

Error tolerance.

Any d points suffices.

"Encode" polynomial with $d+k$ point values.
Can lose *any* k points and reconstruct.

The original "message/file/polynomial" is recoverable.

Polynomial Evaluation.

Evaluate $A(x) = a_0 + a_1 x + \cdots a_{n-1} x^{n-1}$ on n points: $x_0, \cdots, x_{n-1}$.

On one point at at a time:

Example: $4 + 3x + 5x^2 + 4x^3$ on 2.

Horners Rule: $4 + x(3 + x(5 + 4x))$

$5 + 4x = 13$, then $3 + 2(13) = 29$, then $4 + 2(29) = 62$.

In general: $a_0 + x(a_1 + x(a_2 + x(...)))$.

n multiplications/additions to evaluate one point.

Evaluate on n points . We get $O(n^2)$ time.

Could have just multiplied polynomials!

Evaluation of polynomials: Recursive.

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

where

Even coefficient polynomial.
$A_e(x) = a_0 + a_2 x + a_4 x^2 \ldots$.

Odd coefficient polynomial.
$A_o(x) = a_1 + a_3 x + a_5 x^2 \ldots$.

Example:

$A(x) = 4 + 12x + 20x^2 + 13x^3 + 6x^4 + 7x^5$
$= (4 + 20x^2 + 6x^4) + (12x + 13x^3 + 7x^5)$
$= (4 + 20x^2 + 6x^4) + x(12 + 13x^2 + 7x^4)$

$A_e(x) = 4 + 20x + 6x^2$
$A_o(x) = 12 + 13x + 7x^2$
$A(x) = A_e(x^2) + xA_o(x^2)$

Plug in x^2 into A_e and A_o use results to find $A(x)$.

Recursive Evaluation.

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

where

Even coefficient polynomial.
$A_e(x) = a_0 + a_2 x + a_4 x^2 \ldots$.

Odd coefficient polynomial.
$A_o(x) = a_1 + a_3 x + a_5 x^2 \ldots$.

Evaluate recursively:
For a point x:

Compute $A_e(x^2)$ and $A_o(x^2)$.

$T(n) = 2T(n/2) + 1 = O(n)$.

$O(n)$ for 1 point!

n points – $O(n^2)$ time to evaluate on n points.

No better than polynomial multiplication! Bummer.

Recursive on more than one point.

$A(x) = A_e(x^2) + x(A_o(x^2))$
Reuse computations.

n points: $\pm x_0, \pm x_1, \ldots, \pm x_{(n-1)/2}$.
Also $n = d+1$: number of coefficients.

Two points: $+x_0$ and $-x_0$ One square: $(+x_0)^2 = (-x_0)^2 = x_0^2$.

$A(x_0) = A_e(x_0^2) + x_0 A_o(x_0^2)$

$A(-x_0) = A_e((-x_0)^2) + (-x_0)A_o((-x_0)^2)$
$A(-x_0) = A_e(x_0^2) - x_0 A_o(x_0^2)$

From $A_e(x_0^2)$ and $A_o(x_0^2)$ compute both $A(-x_0)$ and $A(x_0)$?

From $A_e(x_i^2)$ and $A_o(x_i^2)$ compute both $A(-x_i)$ and $A(x_i)$?

Evaluate n coefficient polynomial on n points by

Evaluating 2 $\frac{n}{2}$ coefficient polynomials on $\frac{n}{2}$ points.

$T(n,n) = 2T(\frac{n}{2}, \frac{n}{2}) + O(n) = O(n \log n)$!!!!

From $O(n^2)$ to $O(n \log n)$!!!

Explore recursion.

Recursive Condition:
n points: $\frac{n}{2}$ pairs of distinct numbers with common squares.
E.g., $\pm x_0$ both have x_0^2 as square,
$\pm x_1$ both have x_1^2 as square.
.....

Next step:
$\frac{n}{2}$ points: squares should only be $n/4$ distinct numbers

But all our $\frac{n}{2}$ points are squares ...and positive!

Need the $\frac{n}{2}$ points to come in Positive/Negatives pairs!
How can squares be negative?

Complex numbers!

Pairs with common squares.

Want n numbers:
$x_0, \ldots, x_{n-1}$ where
$|\{x_0^2, \ldots, x_{n-1}^2\}| = \frac{n}{2}$,
and
$|\{x_0^4, \ldots, x_{n-1}^4\}| = \frac{n}{4}$,
...and ...
$\{x_0^{\log n}, \ldots, x_{n-1}^{\log n}\}| = 1$.

Each recursive level evaluates:
polynomials of half the degree on half as many points.
n represents both degree and number of points.

In reverse: start with a number 1
Take square roots: 1, -1.
Take square roots: 1,-1, i, $-i$.
Uh oh.

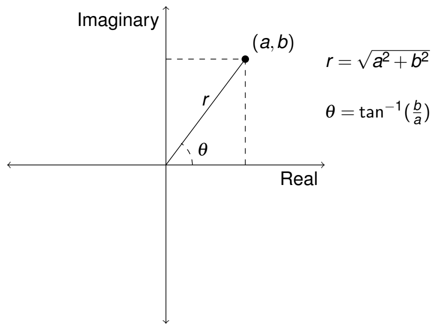
Actually: ± 1, $\pm i$, $\pm \frac{1}{\sqrt{2}}(1+i)$, $\pm \frac{1}{\sqrt{2}}(-1+i)$,

Complex numbers!

Uh oh? Can we get a pattern?

Complex plane

$z = a + bi$

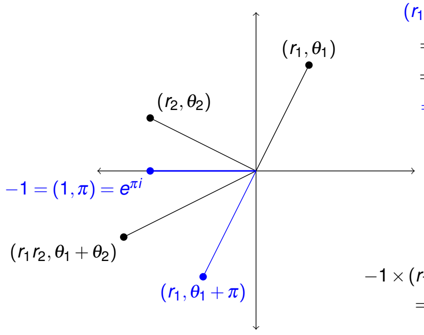


$r = \sqrt{a^2+b^2}$

$\theta = \tan^{-1}(\frac{b}{a})$

Polar coordinate: $r(\cos\theta + i \sin\theta) = re^{i\theta}$ or (r, θ)

Multiplying Complex Numbers



$(r_1, \theta_1) \times (r_2, \theta_2)$
$= r_1 e^{i\theta_1} \times r_2 e^{i\theta_2}$
$= (r_1 r_2) e^{i(\theta_1 + \theta_2)}$
$= (r_1 r_2, \theta_1 + \theta_2)$

$-1 \times (r_1, \theta_1) = (r_1, \theta_1 + \pi)$
$= r_1 e^{r_1(\theta_1 + \pi)i}$

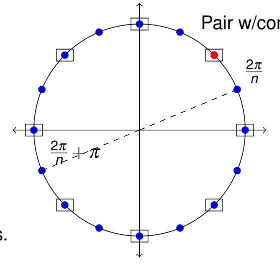
The nth complex roots of unity.

$(e^{\frac{2i\pi}{n} + \pi})^2 = (e^{\frac{2i\pi}{n}})^2 e^{2\pi} = (e^{\frac{2i\pi}{n}})^2$

Solutions to $z^n = 1$

$(1, \frac{2\pi}{n})^n = (1, \frac{2\pi}{n} \times n) = (1, 2\pi) = 1!$ $(1, \frac{2k\pi}{n})^n = (1, 2k\pi) = 1!$
$(1, \theta + \pi)^2 = (1, 2\theta + 2\pi) = (1, 2\theta) = (1, \theta)^2$.

Pair w/common square!



Squares: $\frac{n}{2}$th roots.

Quiz

Which are the same as 1?

(A) $(1)^2$
(B) $(-1)^2$
(C) -1
(D) $e^{2\pi i}$
(E) $(e^{\pi i})^2$

Which are the same as -1?

(A) $(-1)^2$
(B) $(e^{3\pi i/2})^2$
(C) $(e^{\pi i/2})^2$
(D) $(e^{\pi i})^2$

Note: $e^{\pi i} = -1$. (B) $(e^{3\pi i/2})^2 = e^{3\pi i} = e^{\pi i}$ (D) $(e^{\pi i/2})^2 = e^{\pi i}$.

Which are 4th roots of unity? (Hint: take the 4th power.)

(A) $e^{\pi i/2}$
(B) $e^{\pi i}$
(C) $e^{\pi i/3}$
(D) $e^{3\pi i/2}$

(A), (B) and (D).

The FFT!

Defn: $\omega = (1, \frac{2\pi}{n}) = e^{\frac{2\pi i}{n}}$, nth root of unity.
Pairs: ω^i and $\omega^{i+\frac{n}{2}} = \omega^i \omega^{\frac{n}{2}} = -\omega^i$. Common square!
Common Squares: are $\frac{n}{2}$ root of unity.

Fast Fourier Transform:
Evaluate $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_{n-1} x^{n-1}$
on points $\omega^0, \omega, \omega^2, \ldots, \omega^{n-1}$.

Procedure:
Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity:
$\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $j \leq \frac{n}{2}$.

$A(\omega^j) = A_e(\omega^{2j}) + \omega^j A_o(\omega^{2j})$
$A(\omega^{j+\frac{n}{2}}) = A_e(\omega^{2j}) - \omega^j A_o(\omega^{2j})$

Runtime Recurrence:
A_e and A_o are degree $\frac{n}{2}$, $\frac{n}{2}$ points in recursion.
$T(n) = 2T(\frac{n}{2}) + O(n) = O(n \log n)$!

Quiz 2: review

What is ω_n^n? 1

What is $(\omega_n)^{a+n}$? ω_n^a.

What is $(\omega_n^{a+n/2})^2$? ω_n^{2a}

Consider n points: $S_n = \{\omega_n, (\omega_n)^2, \ldots, \omega_n^n\}$.

How many points in the set: $\{(\omega_n)^2, (\omega_n)^4, \ldots, \omega_n^{2n}\}$?

$n/2$ points!!!

FFT: Evaluate degree n polynomial on n points
by evaluating two degree $n/2$ polynomials on $n/2$ points!

Summary.

Polynomial Multiplication: $O(n^2)$.

In Point form: $O(n)$.

Polynomial Evaluation: $O(n^2)$.

Polynomial: $A(x) = A_e(x^2) + x A_o(x^2)$
Evaluate on n points recursively.
$T(n,n) = 2T(n/2,n) + O(n) = O(n^2)$.
The number of leaves is n.
and the work on each leaf is $O(n)$.

Consider n points: $S_n = \{\omega_n, (\omega_n)^2, \ldots, \omega_n^n\}$.

Set of squares: $S_{n/2} = \{\omega_n^2), \omega_n)^4, \ldots, (\omega_n)^n, (\omega_n)^{n+2}, \ldots (\omega_n)^{2n}\}$.
Set of squares: $S_{n/2} = \{\omega_n^2), \omega_n)^4, \ldots, (\omega_n)^n\}$.
Only $n/2$ values here.

Evaluate $A(x) = A_e(x^2) + x A_o(x^2)$.
Only need to evaluate A_e and A_o on $n/2$ points.
$T(n,n) = 2T(n/2, n/2) + O(n)$.
Or $T(n) = 2(n/2) + O(n) = O(n \log n)$