COL 351:
Analysis and Design of Algorithms

Lecture 26

Polynomial Multiplication

Given: Two polynomials $A(x) = a_0 + a_1x + \cdots + a_nx^n$ and $B(x) = b_0 + b_1x + \cdots + b_nx^n$, with degree less than equal to 'n' and integer coefficients.

Find: Product $A(x) \cdot B(x)$ = $c_0 + c_1x + c_2x^2 + \cdots + c_{2n}x^{2n}$ (Say, $C(x)$)

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

Example:

If $A(x) = 1 + x + x^2$ and

$B(x) = 1 + 2x + x^3$. Then,

$C(x) = 1 + 3x + 3x^2 + 3x^3 + x^4 + x^5$

Trivial: $O(n^2)$

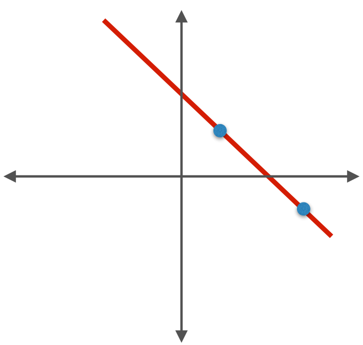
GOAL : $O(n \log n)$

Representation of a polynomial

- An alternate way to represent polynomial $A(x) = a_0 + a_1x + \cdots + a_nx^n$.

$n = 1$

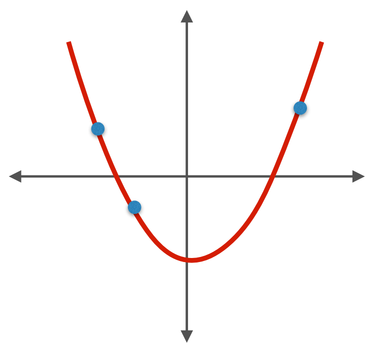
$$A(x) = a_0 + a_1x$$



Evaluation at 2 point suffices

$n = 2$

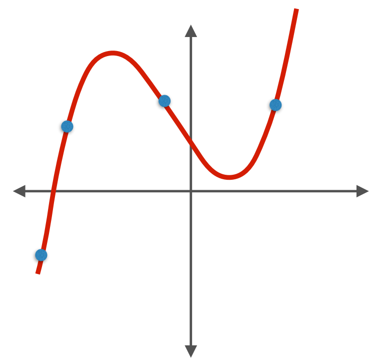
$$A(x) = a_0 + a_1x + a_2x^2$$



Evaluation at 3 point suffices

$n = 3$

$$A(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$



Evaluation at 4 point suffices

Representation of a polynomial

- An alternate way to represent polynomial $A(x) = a_0 + a_1 x + \cdots + a_n x^n$.

> **Lemma**: Given $n+1$ pairs $(x_0, y_0),\ (x_1, y_1),\ \ldots,\ (x_n, y_n)$, there exists a unique polynomial (say P) with degree at most n such that $y_i = P(x_i)$, for $i = 0,1,\ldots,n$.

Proof:
(Hint: A polynomial can be represented as product of monomials in Complex numbers)

1. Suppose $P_1,\ P_2$ have same evaluations on $x_0, x_1, \ldots, x_n$.
2. Define $Q := P_1 - P_2$.
3. On the $(n+1)$ points Q will evaluate to 0, but Q is not identically 0.
4. This is not possible as $deg(Q) \leqslant n$.

Why are we looking at alternate representation?

- Answer: Efficient way to compute product.
  Take a set $S = \{x_0, x_1, x_2, \ldots, x_{2n}\}$

$|S| = 1 + 2n$

$A(x)$ and $B(x)$

$(deg \leqslant n)$

evaluate at $(2n+1)$ points

STEP 1

$A(x_0) \quad B(x_0)$

$A(x_1) \quad B(x_1)$

$\vdots \quad \vdots$

$A(x_{2n}) \quad B(x_{2n})$

Evaluate A, B at $(2n+1)$ points

Point wise product

STEP 2

$A(x_0) \times B(x_0)$

$A(x_1) \times B(x_1)$

$\vdots$

$A(x_{2n}) \times B(x_{2n})$

Do pairwise-product on $(2n+1)$ points

STEP 3

Find $C(x)$

$(deg \leqslant 2n)$

Find C given the evaluations

Step 1: Pointwise evaluation

Given: Polynomial 'A' of degree $\leqslant n$, find its evaluation on a set $S = \{x_0, x_1, \ldots, x_n\}$.

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \cdots + a_n x^n$$

$$= \left(a_0 + a_2 x^2 + a_4 x^4 + \cdots\right) + x\left(a_1 + a_3 x^2 + a_5 x^4 + \cdots\right)$$

$$= A_{even}\left(x^2\right) + x \cdot A_{odd}\left(x^2\right)$$

Assume $N = (n+1)$ is a power of 2

$$|S| \leqslant N$$
$$deg < N$$

Problem of size N

Remark 1: Degree of polynomials $A_{even}, A_{odd} \leqslant (n-1)/2 < N/2$.

Remark 2: If $|S^2| \leqslant N/2$, then we get two subproblems of size $N/2$.

$S^i = \{x^i \mid x \in S\}$

Can we say $T(N) = 2T(N/2) + O(N)$?

Only if..

$$|S| = N$$

$$|S^2| = N/2$$

$$|S^4| = N/4$$

$$|S^N| = 1$$

$\Rightarrow$ Set S should be N roots of $x^N = 1$

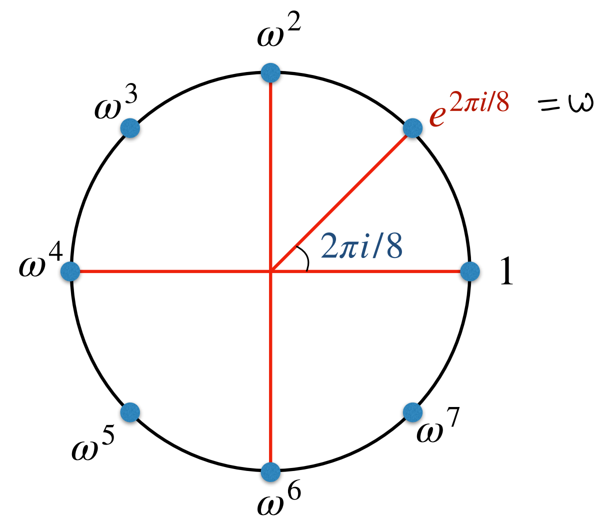
$$S^i = \{x^i \mid x \in S\}$$

N-th Roots of Unity

$N = 8$

$$S = \{e^{\frac{2\pi i}{N}} \ \mid i \in [1, N]\}$$

$$S = \{1, \omega, \omega^2, \omega^3, \ \ldots, \omega^8\}$$



What is:

$S = \{1, \omega, \omega^2, \ \ldots, \omega^7\}$

$S^2 = \{1, \omega^2, \omega^4, \omega^6\} = \{1, i, -1, -i\}$

$S^4 = \{1, \ {}^4\} = \{1, -1\}$

$S^8 = \{1\}$

$$\omega = e^{2\pi i/8}$$

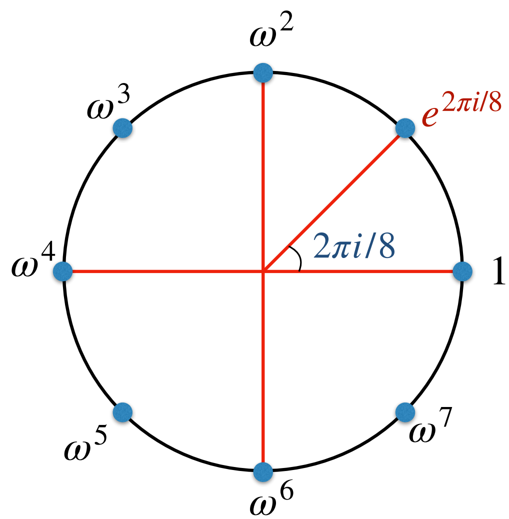
$$= \cos\left(\frac{2\pi}{8}\right) + i \sin\left(\frac{2\pi}{8}\right)$$

$$S^i = \{x^i \mid x \in S\}$$

How to generate all roots from a single root?

$N=8$

Primitive Root:
An N^{th} root of unity that can generate all other N^{th} roots.



N-th root of unity:

ω such that $\omega^N = 1$

N-th primitive root of unity:

ω such that

- $\omega^N = 1$, and
- $\omega^i \neq 1, \quad \text{for} \quad 0 < i < N$

Homework

Ques 1:

Suppose $\omega = e^{2\pi i/N}$, then list all i for which ω^i is an N^{th} primitive root of unity.

Ques 2:

If ω is N^{th} root of unity other than 1, then show that $1 + \omega + \cdots + \omega^{N-1} = 0$.

Ques 3:

If ω is N^{th} primitive root of unity and $i \in [1, N-1]$, then show that

$$1 + \omega^i + \cdots + \omega^{i(N-1)} = 0.$$