

---

# CSS.201.1 ALGORITHMS

*Instructor: Umang Bhaskar*

*TIFR 2024, Aug-Dec*

---

SCRIBE: SOHAM CHATTERJEE

SOHAMCHATTERJEE999@GMAIL.COM

WEBSITE: SOHAMCH08.GITHUB.IO

# CONTENTS

<b>CHAPTER 1</b>	<b>FINDING CLOSEST PAIR OF POINTS</b>	<b>PAGE 3</b>
1.1	Naive Algorithm	3
1.2	Divide and Conquer Algorithm	3
1.2.1	Divide	3
1.2.2	Conquer	4
1.2.3	Combine	4
1.2.4	Pseudocode and Time Complexity	5
1.3	Improved Algorithm for $O(n \log n)$ Runtime	6
1.4	Removing the Assumption	7
<b>CHAPTER 2</b>	<b>MEDIAN FINDING IN LINEAR TIME</b>	<b>PAGE 8</b>
2.1	Naive Algorithm	8
2.2	Linear Time Algorithm	8
2.2.1	Solve RANK-FIND using APPROXIMATE-SPLIT	8
2.2.2	Solve APPROXIMATE-SPLIT using RANK-FIND	9
2.2.3	Pseudocode and Time Complexity	10
<b>CHAPTER 3</b>	<b>POLYNOMIAL MULTIPLICATION</b>	<b>PAGE 11</b>
3.1	Naive Algorithm	11
3.2	Strassen-Schönhage Algorithm	11
3.2.1	Finding Evaluations of Multiplied Polynomial	12
3.2.2	Evaluation of a Polynomial at Points	12
3.2.3	Interpolation from Evaluations at Roots of Unity	13
<b>CHAPTER 4</b>	<b>LONGEST INCREASING SUBSEQUENCE</b>	<b>PAGE 14</b>
<b>CHAPTER 5</b>	<b>BIBLIOGRAPHY</b>	<b>PAGE 15</b>

# Finding Closest Pair of Points

FIND-CLOSEST( $S$ )

**Input:** Set  $S = \{(x_i, y_i) \mid x_i, y_i \in \mathbb{R}, \forall i \in [n]\}$ . We denote  $P_i = (x_i, y_i)$ .

**Question:** Given a set of points find the closest pair of points in  $\mathbb{R}^2$  find  $P_i, P_j$  that are at minimum  $l_2$  distance i.e. minimize  $\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$ .

## 1.1 Naive Algorithm

Now the naive algorithm for this will be checking all pairs of points and take their distance and output the minimum one. There are total  $\binom{n}{2}$  possible choices of pairs of points. And calculating the distance of each pair takes  $O(1)$  time. So it will take  $O(n^2)$  times to find the closest pair of points.

**Idea:**  $\forall P_i, P_j \in S$  find distance  $d(P_i, P_j)$  and return the minimum. Time taken is  $O(n^2)$ .

## 1.2 Divide and Conquer Algorithm

Below we will show a Divide and Conquer algorithm which gives a much faster algorithm. We will follow the algorithm from [CTL<sup>+</sup>, Section 33.4]

### Definition 1.2.1: Divide and Conquer

- Divide: Divide the problem into two parts (roughly equal)
- Conquer: Solve each part individually recursively. If the subproblem sizes are small enough, however, just solve the subproblems in a straightforward manner.
- Combine: Combine the solutions to the subproblems into the solution.

### 1.2.1 Divide

So to divide the problem into two roughly equal parts we need to divide the points into two equal sets. That we can do by sorting the points by their  $x$ -coordinate. Suppose  $S^x$  denote we get the new sorted array of points. And similarly we obtain  $S^y$  which denotes the array of points after sorting  $S$  by their  $y$ -coordinate.

**Algorithm 1:** Step 1 (Divide)

---

```

1 Function Divide:
2   Sort  $S$  by  $x$ -coordinate and  $y$ -coordinate
3    $S^x \leftarrow S$  sorted by  $x$ -coordinate
4    $S^y \leftarrow S$  sorted by  $y$ -coordinate
5    $\bar{x} \leftarrow \lfloor \frac{n}{2} \rfloor$  highest  $x$ -coordinate
6    $\bar{y} \leftarrow \lfloor \frac{n}{2} \rfloor$  highest  $y$ -coordinate
7    $S^L \leftarrow \{P_i \mid x_i < \bar{x}, \forall i \in [n]\}$ 
8    $S^R \leftarrow \{P_i \mid x_i \geq \bar{x}, \forall i \in [n]\}$ 

```

---

**1.2.2 Conquer**

Now we will recursively get pair of closest points in  $S_L$  and  $S_R$ . Suppose the  $(P_1^L, P_2^L)$  are the closest pair of points in  $S^L$  and  $(P_1^R, P_2^R)$  are the closest pair of points in  $S^R$ .

**Algorithm 2:** Step 1 (Solve Subproblems)

---

```

1 Function Conquer:
2   Solve for  $S_L, S^R$ .
3    $(P_1^L, P_2^L)$  are closest pair of points in  $S_L$ .
4    $(P_1^R, P_2^R)$  are closest pair of points in  $S_R$ .
5    $\delta^L = d(P_1^L, P_2^L), \delta^R = d(P_1^R, P_2^R)$ 
6    $\delta_{min} \leftarrow \min\{\delta^L, \delta^R\}$ 

```

---

**1.2.3 Combine**

Now we want to combine these two solutions.

**Question 1.1:** We are not done

Is there a pair of points  $P_i, P_j \in S$  such that  $d(P_i, P_j) < \delta_{min}$

If Yes:

- One of them must be in  $S_L$  and the other is in  $S_R$ .
- $x$ -coordinate  $\in [\bar{x} - \delta_{min}, \bar{x} + \delta_{min}]$ .
- $|y_i - y_j| \leq \delta_{min}$

So we take the strip of radius  $\delta_{min}$  around  $\bar{x}$ . Define  $T = \{P_i \in S \mid |x_i - \bar{x}| \leq \delta_{min}\}$



We now sort all the points in the  $T$  by their decreasing  $y$ -coordinate. Let  $T_y$  be the array of points. For each  $P_i \in T_y$  define the region

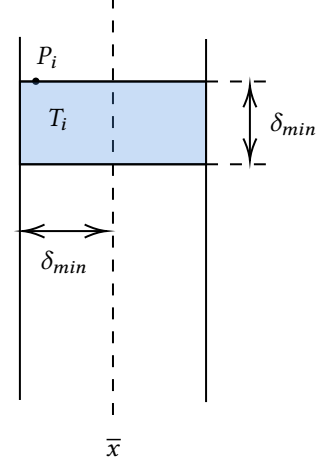
$$T_i = \{P_j \in T_y \mid 0 \leq y_j - y_i \leq \delta_{min}, j > i\}$$

**Lemma 1.2.1**

Number of points (other than  $P_i$ ) that lie inside the box is at most 8

**Proof:** Suppose there are more than 8 points that lie inside the box apart from  $P_i$ . The box has a left square part and a right square part. So one of the squares contains at least 5 points. WLOG suppose the left square has at least 5 points. Divide each square into 4 parts by a middle vertical and a middle horizontal line. Now since there are 5 points there is one part which contains 2 points but that is not possible as those two points are in  $S_L$  and their distance will be less than  $\delta_{min}$  which is not possible. Hence contradiction. Therefore there are at most 8 points inside the box. ■

Hence by the above lemma for each  $P_i \in T_y$  there are at most 8 points in  $T_i$ . So for each  $P_j \in T_i$  we find the  $d(P_i, P_j)$  and if it is less than  $\delta_{min}$  we update the points and the distance

**1.2.4 Pseudocode and Time Complexity**

**Assumption.** We will assume for now that for all  $P_i, P_j \in S$  we have  $x_i \neq x_j$  and  $y_i \neq y_j$ . Later we will modify the pseudocode to remove this assumption

**Algorithm 3: FIND-CLOSEST(S)**


---

**Input:** Set of  $n$  points,  $S = \{(x_i, y_i) \mid x_i, y_i \in \mathbb{R}, \forall i \in [n]\}$ . We denote  $P_i = (x_i, y_i)$ .  
**Output:** Closest pair of points,  $(P_i, P_j, \delta)$  where  $\delta = d(P_i, P_j)$

---

```

1 begin
2   if  $|S| \leq 10$  then
3     Solve by Brute Force (Consider every pair of points)
4    $S^x \leftarrow S$  sorted by  $x$ -coordinate,    $S^y \leftarrow S$  sorted by  $y$ -coordinate
5    $\bar{x} \leftarrow \lfloor \frac{n}{2} \rfloor$  highest  $x$ -coordinate,    $\bar{y} \leftarrow \lfloor \frac{n}{2} \rfloor$  highest  $y$ -coordinate
6    $S^L \leftarrow \{P_i \mid x_i < \bar{x}, \forall i \in [n]\}$ ,    $S^R \leftarrow \{P_i \mid x_i \geq \bar{x}, \forall i \in [n]\}$ 
7    $(P_1^L, P_2^L, \delta^L) \leftarrow \text{FIND-CLOSEST}(S^L)$ ,    $(P_1^R, P_2^R, \delta^R) \leftarrow \text{FIND-CLOSEST}(S^R)$ 
8    $\delta_{min} \leftarrow \min\{\delta^L, \delta^R\}$ 
9   if  $\delta_{min} < \delta^L$  then
10      $P_1 \leftarrow P_1^R, P_2 \leftarrow P_2^R$ 
11   else
12      $P_1 \leftarrow P_1^L, P_2 \leftarrow P_2^L$ 
13    $T \leftarrow \{P_i \mid |x_i - \bar{x}| \leq \delta_{min}\}$ 
14    $T_y \leftarrow T$  sorted by decreasing  $y$ -coordinate
15   for  $P \in T_y$  do
16      $U \leftarrow$  Next 8 points
17     for  $\hat{P} \in U$  do
18       if  $d(P, \hat{P}) < \delta_{min}$  then
19          $\delta_{min} \leftarrow d(P, \hat{P})$ 
20          $(P_1, P_2) \leftarrow (P, \hat{P})$ 
21 return  $(P_1, P_2, \delta_{min})$ 

```

---

Notice we used the assumption in the line 5 for finding the medians. So the line 4 takes  $O(n \log n)$  times. Lines 5,6 takes  $O(n)$  time. Since  $\bar{x}$  is the median, we have  $|S^L| = \lfloor \frac{n}{2} \rfloor$  and  $|S^R| = \lceil \frac{n}{2} \rceil$ . Hence  $\text{FIND-CLOSEST}(S^L)$  and  $\text{FIND-CLOSEST}(S^R)$  takes  $T(\frac{n}{2})$  time. Now lines 8 – 12 takes constant time. Line 13 takes  $O(n)$  time. And line 14 takes  $O(n \log n)$  time. Since  $U$  has 8 points i.e. constant number of points the lines 16 – 20 takes constant time for each  $P \in T_y$ . Hence the for loop at

line 15 takes  $O(n)$  time. Hence total time taken

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

### 1.3 Improved Algorithm for $O(n \log n)$ Runtime

Notice once we sort the points by  $x$ -coordinate and  $y$ -coordinate we don't need to sort the points anymore. We can just pass the sorted array of points into the arguments for solving the smaller problems. There is another time where we need to sort which is in line 14 of the above algorithm. This we can get actually from  $S^y$  without sorting just checking one by one backwards direction if the  $x$ -coordinate of the points satisfy  $|x_i - \bar{x}| \leq \delta_{min}$ . So

$$T_y = \text{REVERSE}(\{P_i \in S^y \mid |x_i - \bar{x}| \leq \delta_{min}\})$$

So we form a new algorithm which takes the input  $S^x$  and  $S^y$  and then finds the closest pair of points. Then we will use that subroutine to find closest pair of points in any given set of points.

---

**Algorithm 4:** FIND-CLOSEST-SORTED( $S^x, S^y$ )

---

**Input:** Set of  $n$  points,  $S = \{(x_i, y_i) \mid x_i, y_i \in \mathbb{R}, \forall i \in [n]\}$ .

$S^x$  and  $S^y$  are the sorted array of points with respect to  $x$ -coordinate and  $y$ -coordinate respectively

**Output:** Closest pair of points,  $(P_i, P_j, \delta)$  where  $\delta = d(P_i, P_j)$

```

1 begin
2   if  $|S| \leq 10$  then
3     Solve by Brute Force
4    $\bar{x} \leftarrow \lfloor \frac{n}{2} \rfloor$  highest  $x$ -coordinate
5    $\bar{y} \leftarrow \lfloor \frac{n}{2} \rfloor$  highest  $y$ -coordinate
6    $S^L \leftarrow \{P_i \in S^x \mid x_i < \bar{x}, \forall i \in [n]\}$ 
7    $S_y^L \leftarrow \{P_i \in S^y \mid x_i < \bar{x}\}$ 
8    $S^R \leftarrow \{P_i \in S^x \mid x_i \geq \bar{x}, \forall i \in [n]\}$ 
9    $S_y^R \leftarrow \{P_i \in S^y \mid x_i \geq \bar{x}\}$ 
10   $(P_1^L, P_2^L, \delta^L) \leftarrow \text{FIND-CLOSEST-SORTED}(S^L, S_y^L)$ 
11   $(P_1^R, P_2^R, \delta^R) \leftarrow \text{FIND-CLOSEST-SORTED}(S^R, S_y^R)$ 
12   $\delta_{min} \leftarrow \min\{\delta^L, \delta^R\}$ 
13  if  $\delta_{min} < \delta^L$  then
14     $P_1 \leftarrow P_1^R, P_2 \leftarrow P_2^R$ 
15  else
16     $P_1 \leftarrow P_1^L, P_2 \leftarrow P_2^L$ 
17   $T \leftarrow \{P_i \mid |x_i - \bar{x}| \leq \delta_{min}\}$ 
18   $T_y \leftarrow \text{REVERSE}(\{P_i \in S^y \mid |x_i - \bar{x}| \leq \delta_{min}\})$ 
19  for  $P \in T_y$  do
20     $U \leftarrow$  Next 8 points
21    for  $\hat{P} \in U$  do
22      if  $d(P, \hat{P}) < \delta_{min}$  then
23         $\delta_{min} \leftarrow d(P, \hat{P})$ 
24         $(P_1, P_2) \leftarrow (P, \hat{P})$ 
25  return  $(P_1, P_2, \delta_{min})$ 

```

---



---

**Algorithm 5:** FIND-CLOSEST( $S$ )

---

**Input:** Set of  $n$  points,

$S = \{(x_i, y_i) \mid x_i, y_i \in \mathbb{R}, \forall i \in [n]\}$ .

We denote  $P_i = (x_i, y_i)$ .

**Output:** Closest pair of points,  $(P_i, P_j, \delta)$  where  $\delta = d(P_i, P_j)$

```

1 begin
2   if  $|S| \leq 10$  then
3     Solve by Brute Force
4    $S^x \leftarrow S$  sorted by  $x$ -coordinate
5    $S^y \leftarrow S$  sorted by  $y$ -coordinate
6   return FIND-CLOSEST-SORTED( $S^x, S^y$ )

```

---

This algorithm only sorts one time. So time complexity for FIND-CLOSEST-SORTED( $S^x, S^y$ ) is

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

and therefore times complexity for FIND-CLOSEST( $S$ ) is  $O(n \log n)$ .

## 1.4 Removing the Assumption

For this there nothing much to do. For finding the median  $\bar{x}$  if we have more than one points with same  $x$ -coordinate which appears as the  $\lfloor \frac{n}{2} \rfloor$  highest  $x$ -coordinate we sort only those points with respect to their  $y$ -coordinate update the  $S^x$  like that and then take  $\lfloor \frac{n}{2} \rfloor$  highest point in  $S^x$ . We do the same for  $S^y$  and update accordingly. All this we do so that  $S^L$  and  $S^R$  has the size  $\frac{n}{2}$ .

# Median Finding in Linear Time

MEDIAN-FIND( $S$ )

**Input:** Set  $S$  of  $n$  distinct integers

**Question:** Find the  $\lfloor \frac{n}{2} \rfloor^{th}$  smallest integer in  $S$

## 2.1 Naive Algorithm

The naive algorithm for this will be to sort the array in  $O(n \log n)$  time then return the  $\lfloor \frac{n}{2} \rfloor^{th}$  element. This will take  $O(n \log n)$  time. But in the next section we will show a linear time algorithm.

## 2.2 Linear Time Algorithm

In this section we will show an algorithm to find the median of a given set of distinct integers in  $O(n)$  time complexity. We will follow [CTL<sup>+</sup>, Section 9.3]. Consider the following two problems:

RANK-FIND ( $S, k$ )

**Input:** Set  $S$  of  $n$  distinct integers and an integer  $k \leq n$

**Question:** Find the  $k^{th}$  smallest integer in  $S$

APPROXIMATE-SPLIT( $S$ )

**Input:** Set  $S$  of  $n$  distinct integers

**Question:** Given  $S$ , return an integer  $z \in S$  such that  $z$  where  $rank(z) \in [\frac{n}{4}, \frac{3n}{4}]$

### 2.2.1 Solve RANK-FIND using APPROXIMATE-SPLIT

---

**Algorithm 6:** RANK-FIND( $S, k$ )

---

**Input:** Set  $S$  of  $n$  distinct integer and  $k \in [n]$   
**Output:**  $k^{th}$  smallest integer in  $S$

```

1 begin
2   if  $|S| \leq 100$  then
3     Sort  $S$ , return  $k^{th}$  smallest element in  $S$ 
4    $z \leftarrow$  APPROXIMATE-SPLIT( $S$ )      ( $z$  is the  $r^{th}$  smallest element for some  $r \in [\frac{n}{4}, \frac{3n}{4}]$ )
5    $S_L \leftarrow \{x \in S \mid x \leq z\}$ ,  $S_R \leftarrow \{x \in S \mid x > z\}$ 
6   if  $k \leq |S_L|$  then
7     return RANK-FIND( $S_L, k$ )
8   return RANK-FIND( $S_R, k - |S_L|$ )

```

---



Certainly if we can solve RANK-FIND( $S, k$ ) for all  $k \in [n]$  we can also solve MEDIAN-FIND. We will try to use both the problems and recurse to solve RANK-FIND in linear time.

In the above algorithm  $\text{rank}(z) \in [\frac{n}{4}, \frac{3n}{4}]$ . So  $\frac{n}{4} \leq |S_L|, |S_R| \leq \frac{3n}{4}$ . For now suppose RANK-FIND( $S, k$ ) takes  $T_{RF}(n)$  time and APPROXIMATE-SPLIT( $S$ ) takes  $T_{AS}(n)$  time. Then the time taken by the algorithm is

$$T_{RF}(n) \leq O(n) + T_{AS}(n) + T_{RF}\left(\frac{3n}{4}\right)$$

### 2.2.2 Solve APPROXIMATE-SPLIT using RANK-FIND

We first divide  $S$  into groups of 5 elements. So take  $t = \lceil \frac{n}{5} \rceil$ . Now we sort each group. Since each group have constant size this can be done in  $O(n)$  time. So now consider the scenario:



After sorting each of the groups we take the medians of each group. Let  $z$  be the median of the medians. We claim that  $\text{rank}(z) \in [\frac{n}{4}, \frac{3n}{4}]$ .

---

#### Algorithm 7: APPROXIMATE-SPLIT( $S$ )

---

**Input:** Set  $S$  of  $n$  distinct integers  
**Output:** An integer  $z \in S$  such that  $\text{rank}(z) \in [\frac{n}{4}, \frac{3n}{4}]$

```

1 begin
2   if  $|S| \leq 100$  then
3     Sort, return Exact median
4    $t \leftarrow \lceil \frac{n}{5} \rceil$ 
5    $S_i \leftarrow i^{\text{th}}$  block of 5 elements in  $S$  for  $i \in [t-1]$ 
6    $S_t \leftarrow$  Whatever is left in  $S$ 
7   for  $i \in [t]$  do
8     Sort  $S_i$ , Let  $h_i$  be the median of  $S_i$ 
9    $T \leftarrow \{h_i \mid i \in [t]\}$ 
10  return RANK-FIND( $T, \lfloor \frac{t}{2} \rfloor$ )

```

---

So in the picture among elements in upper left the highest element is  $z$  and among the elements in lower right the lowest element is  $z$ . We will show that the number of elements smaller than  $z$  is between  $\frac{n}{4}$  and  $\frac{3n}{4}$ . Lets call the set of elements in upper left box is  $S_u$  and the set of elements in lower right box is  $S_d$ .

**Lemma 2.2.1**

$$|S_u|, |S_d| \geq \frac{n}{4}$$

**Proof:**  $|S_u| \geq 3 \times \lfloor \frac{t}{2} \rfloor$ . For  $n \geq 100$ ,  $3 \lfloor \frac{t}{2} \rfloor > \frac{n}{4}$ . Hence  $|S_u| \geq \frac{n}{4}$ . Now similarly  $|S_d| \geq 3 \lfloor \frac{t}{2} - 1 \rfloor \geq \frac{n}{4}$ . ■

**Lemma 2.2.2**

Number of elements in  $S$  smaller than  $z$  lies between  $\frac{n}{4}$  and  $\frac{3n}{4}$ .

**Proof:** Now number of elements in  $S$  smaller than  $z \geq |S_u| \geq \frac{n}{4}$ . The number of elements greater than  $z \geq |S_d| \geq \frac{n}{4}$ . So number of elements in  $S$  smaller than  $z \leq n - \text{number of elements greater than } z \leq n - \frac{n}{4} = \frac{3n}{4}$ . ■

Hence the APPROXIMATE-SPLIT( $S$ ) takes time

$$T_{AS}(n) = O(n) + T_{RF}\left(\frac{n}{5}\right)$$

**2.2.3 Pseudocode and Time Complexity**

Hence using APPROXIMATE-SPLIT the final algorithm for RANK-FIND is the following:

**Algorithm 8: RANK-FIND( $S, k$ )**


---

**Input:** Set  $S$  of  $n$  distinct integer and  $k \in [n]$   
**Output:**  $k^{th}$  smallest integer in  $S$

---

```

1 begin
2   if  $|S| \leq 100$  then
3      $\lfloor$  Sort  $S$ , return  $k^{th}$  smallest element in  $S$ 
4    $t \leftarrow \lceil \frac{n}{5} \rceil$ 
5    $S_i \leftarrow i^{th}$  block of 5 elements in  $S$  for  $i \in [t-1]$ 
6    $S_t \leftarrow$  Whatever is left in  $S$ 
7   for  $i \in [t]$  do
8      $\lfloor$  Sort  $S_i$ , Let  $h_i$  be the median of  $S_i$ 
9    $T \leftarrow \{h_i \mid i \in [t]\}$ 
10   $z \leftarrow \text{RANK-FIND}(T, \lfloor \frac{t}{2} \rfloor)$ 
11   $S_L \leftarrow \{x \in S \mid x \leq z\}$ ,  $S_R \leftarrow \{x \in S \mid x > z\}$ 
12  if  $k \leq |S_L|$  then
13     $\lfloor$  return  $\text{RANK-FIND}(S_L, k)$ 
14  return  $\text{RANK-FIND}(S_R, k - |S_L|)$ 

```

---

Replacing  $T_{AS}(n)$  in the time complexity equation of  $T_{RF}(n)$  we get the equation:

$$T_{RF}(n) \leq O(n) + T_{RF}\left(\frac{n}{5}\right) + T_{RF}\left(\frac{3n}{4}\right)$$

Let  $T_{RF}(n) \leq kn + T_{RF}\left(\frac{n}{5}\right) + T_{RF}\left(\frac{3n}{4}\right)$ . We claim that  $T_{RF}(n) \leq cn$  for some  $c \in \mathbb{N}$  for all  $n \geq n_0$  where  $n_0 \in \mathbb{N}$ . By induction we have

$$T_{RF}(n) \leq kn + \frac{cn}{5} + \frac{3cn}{4} = \left(k + \frac{19c}{20}\right)n$$

To have  $k + \frac{19c}{20} \leq c$  we have to have  $k + \frac{19c}{20} \leq c \iff c \geq 20k$ . So take  $c \geq 20k$  and our claim follows. Hence  $T_{RF}(n) = O(n)$ . Since we can find any  $k^{th}$  smallest number in a given set of distinct integers in linear time we can also find the median in linear time.

# Polynomial Multiplication

## POLYNOMIAL MULTIPLICATION

**Input:** Given 2 univariate polynomials of degree  $n - 1$  by 2 arrays of their coefficients  $(a_0, \dots, a_{n-1})$  and  $(b_0, \dots, b_{n-1})$  such that  $A(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  and  $B(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$  respectively

**Question:** Given 2 polynomials of degree  $n - 1$  find their product polynomial  $C(x) = A(x)B(x)$  of degree  $2n - 2$  by returning the array of their coefficients.

### 3.1 Naive Algorithm

We can do this naively by calculating each coefficient of  $C$  in  $O(n)$  time since for any  $i \in \{0, \dots, 2n - 2\}$

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

Since there are  $2n - 1 = O(n)$  total coefficient of  $C$  it takes total  $O(n^2)$  time. In the following section we will do this in  $O(n \log n)$  time.

### 3.2 Strassen-Schönhage Algorithm

Before diving into the algorithm first let's consider how many ways we can represent a polynomial. Often changing the representation helps solving the problem in less time.

- **Coefficients:** We can represent a polynomial by giving the array of all its coefficient.
- **Point-Value Pairs:** We can evaluate the polynomial in distinct  $n$  points and give all the point-value pairs. This also uniquely represents a polynomial since there is exactly one polynomial of degree  $n - 1$  which passes through all these points.

#### Theorem 3.2.1

Given  $n$  distinct points  $(x_0, y_0), \dots, (x_{n-1}, y_{n-1})$  in  $\mathbb{R}^2$  there is an unique  $(n - 1)$ -degree polynomial  $P(x)$  such that  $P(x_i) = y_i$  for all  $i \in \llbracket n - 1 \rrbracket$

Since we want to find the polynomial  $C(x) = A(x)B(x)$  and  $C(x)$  has degree  $2n - 2$ , we will evaluate the polynomials  $A(x)$  and  $B(x)$  in  $2n - 1$  distinct points. So we will have the algorithm like this:



### 3.2.1 Finding Evaluations of Multiplied Polynomial

Suppose we were given  $A(x)$  and  $B(x)$  evaluated at  $2n-1$  distinct points  $x_0, \dots, x_{2n-2}$ . Then we can get  $C(x)$  evaluated at  $x_0, \dots, x_{2n-2}$  by

$$C(x_i) = A(x_i)B(x_i) \quad \forall i \in \llbracket 2n-2 \rrbracket$$

Since there are  $O(n)$  many points and for each point it takes constant time to multiply we can find evaluations of  $C$  at  $x_0, \dots, x_{2n-2}$  in  $O(n)$  time.

### 3.2.2 Evaluation of a Polynomial at Points

#### Question 3.1

Suppose there is only one point,  $x_0$ . Can we evaluate a  $n-1$  degree polynomial  $A(x) = \sum_{i=0}^{n-1} a_i x^i$  at  $x_0$  efficiently?

We can rewrite  $A(x)$  as

$$A(x) = a_0 + x(a_1 + x(a_2 + x(a_3 + \dots (a_{n-1} + x(a_n)) \dots)))$$

In this represent it is clear that we have to do  $n$  additions and  $n$  multiplications to find  $A(x_0)$ . Hence we can evaluate a  $n-1$  degree polynomial at a point in  $O(n)$  time

But we have  $O(n)$  points. And if each point takes  $O(n)$  time to find the evaluation of the polynomial then again it will take total  $O(n^2)$  time. We are back to square one. So instead we will evaluate the polynomial in some special points and we will evaluate in all of them in  $O(n \log n)$  time. So now the problem we will discuss now is to find some special  $n$  points where we can evaluate a  $n-1$ -degree polynomial in  $O(n \log n)$  time.

**Idea:** Evaluate at roots of unity and use Fast Fourier Transform

Assume  $n$  is a power of 2. We have the polynomial  $A(x) = \sum_{i=0}^{n-1} a_i x^i$ . So now consider the following two polynomials

$$A^0(x) = a_0 + a_2x + a_4x^2 + \dots + a_{n-2}x^{\frac{n}{2}-1} \quad A^1(x) = a_1 + a_3x + a_5x^2 + \dots + a_{n-1}x^{\frac{n}{2}-1}$$

Certainly we have

$$A(x) = A^0(x^2) + xA^1(x^2)$$

Hence we can get  $A(1)$  and  $A(-1)$  by

$$A(1) = A^0(1) + A^1(1) \quad A(-1) = A^0(1) - A^1(1)$$

Hence like this by evaluating two  $\frac{n}{2} - 1$  degree polynomials at one point we get evaluation of  $A$  at two points. More generally for any  $y \geq 0$  we have

$$A(\sqrt{y}) = A^0(y) + \sqrt{y}A^1(y) \quad A(-\sqrt{y}) = A^0(y) - \sqrt{y}A^1(y)$$

So by recursing like this evaluating at 1, -1 we can get evaluations of  $A$  at  $n^{th}$  roots of unity.

Let

$$\omega_n^k = n^{th} \text{ root of unity for } k \in \llbracket n-1 \rrbracket = e^{i\frac{k}{n}2\pi} = \cos\left(\frac{k}{n}2\pi\right) + i \sin\left(\frac{k}{n}2\pi\right)$$

Hence we have

$$\begin{aligned} A\left(\omega_n^k\right) &= A^0\left(\omega_n^{2k}\right) + \omega_n^k A^1\left(\omega_n^{2k}\right) = A^0\left(\omega_{\frac{n}{2}}^k\right) + \omega_n^k A^1\left(\omega_{\frac{n}{2}}^k\right) \\ A\left(-\omega_n^k\right) &= A\left(\omega_n^{\frac{n}{2}+k}\right) = A^0\left(\omega_n^{2k}\right) - \omega_n^k A^1\left(\omega_n^{2k}\right) = A^0\left(\omega_{\frac{n}{2}}^k\right) - \omega_n^k A^1\left(\omega_{\frac{n}{2}}^k\right) \end{aligned}$$

. Hence now we will solve the following problem:

RECURSIVE-DFT

**Input:**  $(a_0, \dots, a_{n-1})$  representing  $(n-1)$ -degree polynomial  $A(x) = \sum_{i=0}^{n-1} a_i x^i$

**Question:** Find the evaluations of the polynomial  $A(x)$  in all  $n^{th}$  roots of unity

Since  $A^0$  and  $A^1$  have degree  $\frac{n}{2} - 1$  we can use recursion. Hence the algorithm is

---

**Algorithm 9:** RECURSIVE-DFT( $A$ )

---

**Input:**  $A = (a_0, \dots, a_{n-1})$  such that  $A(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$

**Output:**  $A(x)$  evaluated at  $n^{th}$  roots of unity  $\omega_n^k$  for all  $k \in \llbracket n-1 \rrbracket$

```

1 begin
2   if  $n == 1$  then
3     return  $A[0]$ 
4    $A^0 \leftarrow (A[0], A[2], \dots, A[n-2])$ 
5    $A^1 \leftarrow (A[1], A[3], \dots, A[n-1])$ 
6    $Y^0 \leftarrow \text{RECURSIVE-DFT}(A^0)$ 
7    $Y^1 \leftarrow \text{RECURSIVE-DFT}(A^1)$ 
8   for  $k = 0$  to  $\frac{n}{2} - 1$  do
9      $Y[k] \leftarrow Y^0[k] + \omega_n^k Y^1[k]$  //  $A(\omega_n^k) = A^0(\omega_{\frac{n}{2}}^k) + \omega_n^k A^1(\omega_{\frac{n}{2}}^k)$ 
10
11      $Y[k + \frac{n}{2}] \leftarrow Y^0[k] - \omega_n^{\frac{n}{2}+k} Y^1[k]$  //  $A(-\omega_n^k) = A^0(\omega_{\frac{n}{2}}^k) - \omega_n^k A^1(\omega_{\frac{n}{2}}^k)$ 
12
13   return  $Y$ 
```

---

**Algorithm Time Complexity:**  $T(n) = 2T\left(\frac{n}{2}\right) + O(n) = O(n \log n)$ .

Therefore we can evaluate a  $n-1$  degree polynomial in all the  $n^{th}$  roots of unity in  $O(n \log n)$  time. Hence with this algorithm we will get evaluations of the polynomial  $C(x) = A(x)B(x)$  in all the  $2n^{th}$  roots of unity. Now we need to interpolate the polynomial  $C(x)$  from its evaluations. We will describe the process in the next subsection.

### 3.2.3 Interpolation from Evaluations at Roots of Unity

In this section

# Longest Increasing Subsequence

LONGEST INCREASING SUBSEQUENCE

**Input:** Sequence of distinct integers  $A = (a_1, \dots, a_n)$

**Question:** Given an array of distinct integers find the longest increasing subsequence i.e. return maximum size set  $S \subseteq [n]$  such that  $\forall i, j \in S, i < j \implies a_i < a_j$

# CHAPTER 5

## Bibliography

[CTL<sup>+</sup>] Thomas H. Cormen, H. Thomas, Leiserson, E. Charles, Ronald L. Rivest, L. Ronald, Stein, and Clifford. *Introduction to Algorithms*. Brand: PHI Learning.