

CSCE 310H - Fall 2021

---

Computer Science III - honors

Dr. Chris Bourke

---

---

---



$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

A hand-drawn diagram illustrating the Euclidean distance formula. Two points are plotted on a grid. Point 1 is at coordinates  $(x_1, y_1)$  and Point 2 is at  $(x_2, y_2)$ . A vertical line segment connects the two points, and a horizontal line segment connects them. The length of this hypotenuse is labeled  $d$ , representing the distance between the two points.

Pairs = Combinations of size 2

given a set of  $n$  distinct elements,  
how many combinations (order does  
not matter)  
of  $k$  elements are there?

$n$  "choose"  $k$

$${n \choose k} = C(n, k) = {n \choose k} = {}_n C_k$$

$$\binom{n}{k} = \frac{n!}{(n-k)! k!}$$

ex:

$$\binom{n}{2} = \text{number of pairs}$$

$$= \frac{n!}{(n-2)! 2!}$$

$$= \frac{n(n-1)}{2}$$

$$\in O(n^2)$$

$$= \frac{n^2}{2} - \frac{n}{2}$$

Input: A set of points  $A = \{(x_1, y_1), \dots, (x_n, y_n)\}$

Output: 2 closest points in A

1  $\text{MinDist} \leftarrow \infty$

2 for each pair of points  $(x_a, y_a), (x_b, y_b)$  in A

3  $d \leftarrow \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$

4 if  $d < \text{MinDist}$

5      $\text{MinDist} \leftarrow d$

6      $(P_a, P_b) \leftarrow (P_1, P_2)$

7 Output  $(P_a, P_b)$

1) Input: A

2) Input size: n

3) Element Op:

comp,  $\sim n^4$

4)  $\binom{n}{2}$  5)  $O(n^2)$

~~for  $x$  in  $A$ :~~

$O$  loose

~~for  $y$  in  $A$ :~~

$n \in \Theta(n)$

$n \in O(n^2)$

$n \in O(2^n)$

for  $i = 0 \dots n-1$

  for  $j = i+1 \dots n$

$\dots$

$i$

$$\sum_{i=0}^{n-1} \sum_{j=i+1}^{n-1} 1 = \sum_{i=0}^{n-1} (n-i)$$

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}$$

Gauss's Formula

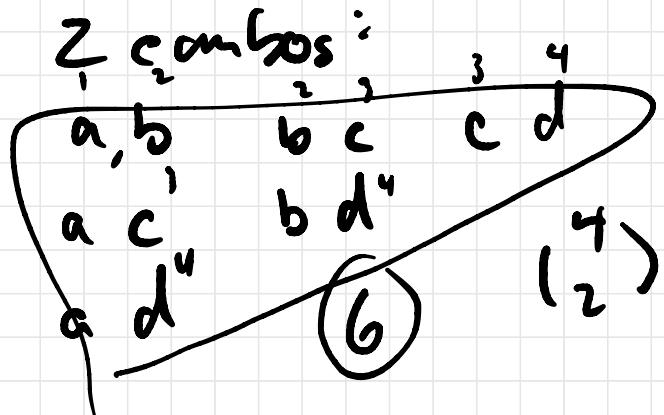
## $k$ -combinations

Given a set of  $n$  elements,  $\{1, 2, 3, \dots, n\}$

a  $k$ -combination is a subset of size  $k$

$\hookrightarrow$  unordered

ex)  $\{a, b, c d\}$



$$= \frac{4!}{(4-2)!(2!)} = \frac{4 \cdot 3}{2} = 6$$

3 - combos of a b c d ... n

for  $i = 1 \dots 2^{n-2}$   
for  $j = i+1 \dots 3^{n-1}$   
for  $k = j+1 \dots 4^n$

Want: generate all possible subsets..

- how many subsets are there of a set of size  $n$ ?

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n-1} + \binom{n}{n}$$

$$= 2^n$$

$$\mathcal{O}(2^n) \rightarrow \text{exp.}$$

$$S = \{a, b, c \dots n\}$$

$P(S)$  = Power Set

a, b, c

$\emptyset$

$\{a\}$

$\{b\}$

$\{c\}$

$\{a, b\}$

$\{a, c\}$

$\{b, c\}$

$\{a, b, c\}$

bit

000

100

010

001

110

101

011

111

000

001

010

011

100

101

110

111

0

1

2

3

4

...

?

1 if  $x \in \text{Subset}$

$0 \dots 2^n - 1$

0 if  $x$  is ~~not~~<sup>not</sup> in  
subset

$$\binom{n}{k} = \frac{n!}{(n-k)! k!}$$

$$\binom{n}{k} \in O(n^k)$$

$$\binom{n}{2} \in O(n^2)$$

$$\binom{n}{3} \in O(n^3)$$

$$\binom{n}{4} \in O(n^4)$$

$$\binom{n}{n/2}$$

$$\binom{n}{n}$$

$$\binom{4}{4}^1$$

$$\binom{4}{3}^4$$

$$\binom{4}{2}^6$$

↓

$$\binom{4}{1}^4$$

$$\binom{4}{0}^1$$

$$\binom{3}{0}^1$$

$$\binom{3}{1}^3$$

$$\binom{1}{1}^1$$

$$\binom{2}{0}^2$$

$$\binom{2}{0}^1$$

$$\binom{2}{1}^2$$

$$\binom{2}{2}^1$$

$$\binom{3}{2}^3$$

$$\binom{3}{3}^1$$

$$\binom{0}{0}^1$$

$$\binom{n}{n/2} = \frac{\frac{n!}{(n-n/2)!}}{n/2!} \in O(2^n)$$

$$\{2, 5, 6, 9, 10\}$$

$$2 \ 5 \ 7 \ 9 \ 10$$

$$\begin{array}{l} n = 10 \\ k = 5 \end{array}$$

## Algorithm 2: Next $k$ -Combination

INPUT : A set of  $n$  elements and an  $k$ -combination,  $a_1 \dots a_k$ .

OUTPUT : The next  $k$ -combination.

- 1  $i = k$
- 2 WHILE  $a_i = n - k + i$  DO
- 3     $i = i - 1$
- 4     $a_i = a_i + 1$
- 5 FOR  $j = (i + 1) \dots k$  DO
- 6     $a_j = a_i + j - i$

$$n = 5 \quad \{1, 2, 3, 4, 5\}$$

$$k = 3$$

Current:	$a_1$	$a_2$	$a_3$
	1	4	5
	↓	↓	↓
	2	3	4

2) replace  $a_1 \rightarrow a_1 + 1$

$$a_2 : a_1 + j - i$$

$$j \quad 2 + 2 - 1 = 3$$

$$a_3 : a_1 + j - i$$

$$j \quad 2 + 3 - 1 = 4$$

Next?

1) locate last  $a_i$  such that

$$a_i \neq n - k + i \quad a_3 = 5 \stackrel{?}{=} n - k + i \\ \stackrel{?}{=} 5 - 3 + 3 = 5$$

$$a_1 = 1 \stackrel{?}{=} 5 - 3 + 1 \\ \neq 3$$

$$a_2 = 4 \stackrel{?}{=} 5 - 3 + 1 \\ \stackrel{?}{=} 5 - 3 + 2 = 4$$

## Permutations

A permutation is an arrangement (order matters) of elements

abc      bac      cab  
acb      bca      cba

in general:  
 $n!$

$$n=3 \quad 6$$

$n=6$

1 2 3 4 5 6

1 2 3 4 6 5

1 2 3 5 4 6

perm      "next"      sorty

$$n = 6$$

$a_i, a_{i+1}$   
16 3 5 4 2  
 $\downarrow$   $a'$

$\downarrow$   
16 4 5 3 2  
 $\underbrace{\quad\quad\quad}_{\text{sort}}$   
 $\downarrow$   
16 4 2 3 5 ✓

- 1) find last pair that is in order
  - 2) find  $a'$ : smallest element  
larger than  $a_i$  to the right
- a) swap  $a_i, a'$
  - b) sort everything to the right of  $a'$

16 4 2 3 5  
  \u2193  
  Surp

16 4 2 5 3  
  \u2193  
  sort

:

6 5 4 3 2 1

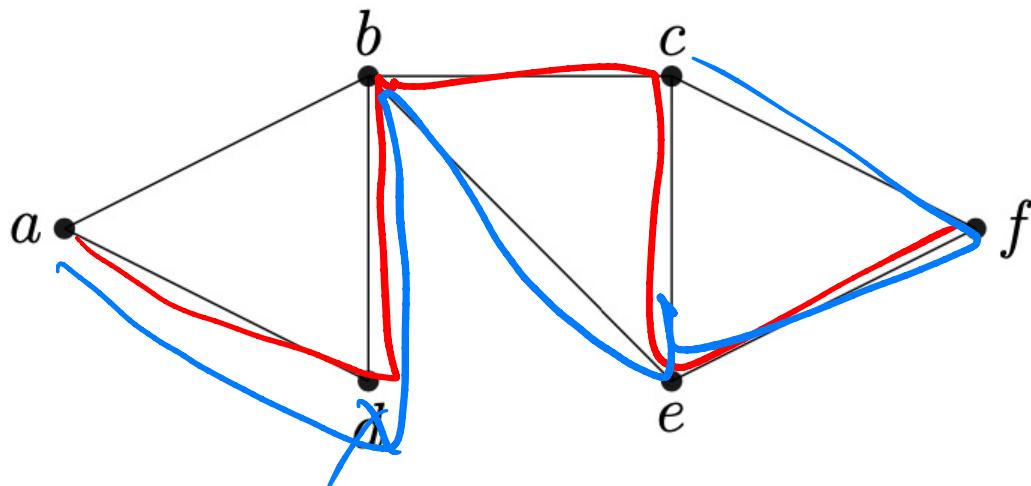
i) rightmost inward pair

$n!$  permutations

$$O(n!) = O(n^n)$$

$$0! = 1$$

, n



adbc<sub>e</sub>f  
adbefc

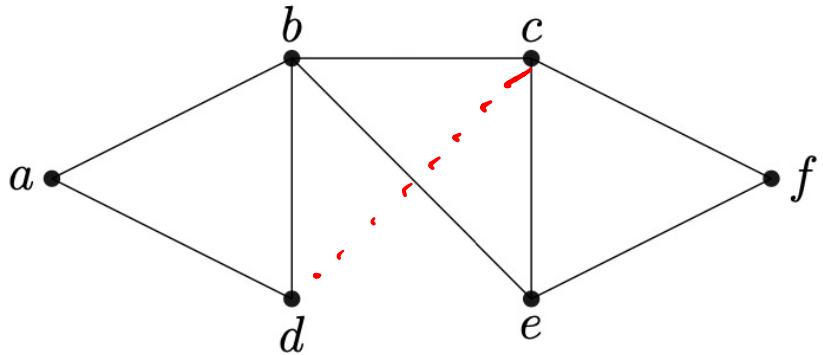
abcef<sub>d</sub>

for each permutation  $\pi$  of  $\{v_1 \dots v_n\}$ :

{     // Verify if it is a path:  
    isValid <- true  
    for  $i = 1 \dots n-1$  :  
        [     if  $(v_i, v_{i+1}) \notin E$   
            L isValid <- false  
            if isValid  
                [     output Yes  
            ]  
        ]  
    ]  
}  
}

$O(n!)$

Output No



$$n! = 6! = 720$$

↓

$$600$$

↓

$$480$$

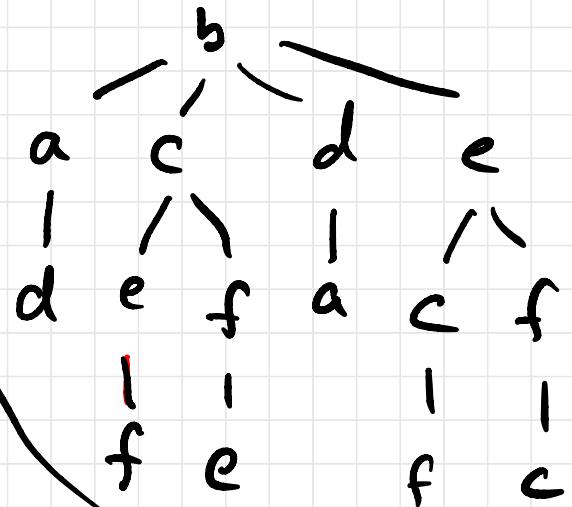
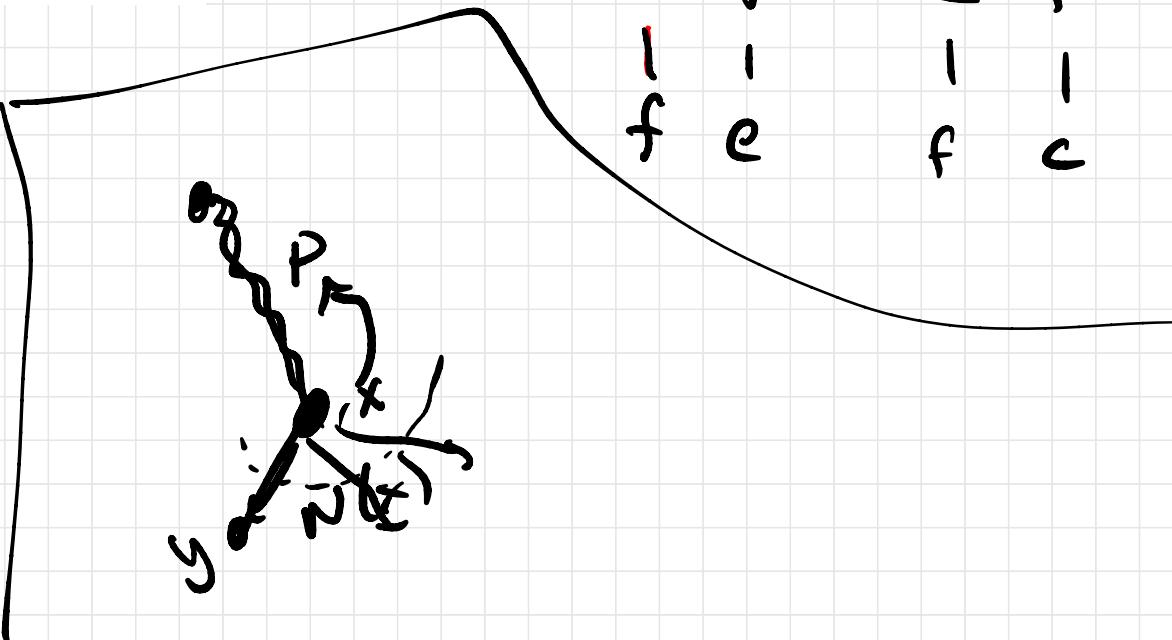
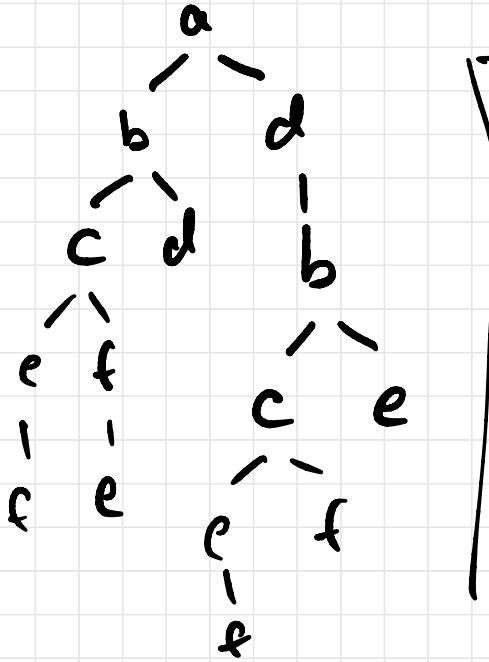
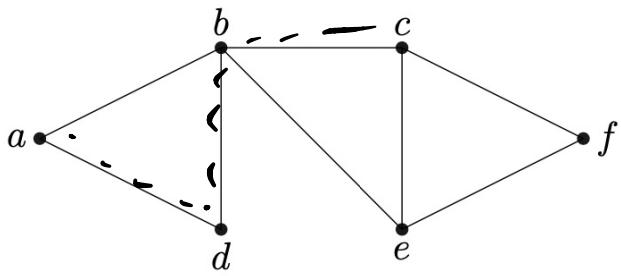
$\overset{x}{\circ}$   
dc

a, b, e, f

$$5! = 120$$

cd

$$5! = 120$$



## DFS Hamiltonian Walk - MAIN

Input: A graph  $G = (V, E)$

Output: true if  $G$  contains a Ham. path

for each  $v \in V$ :

path  $\leftarrow v$

if  $WALK(G, p)$ :

    Output true

Output false

$\text{WALK}(G, p)$ :

Input: A graph  $G = (V, E)$ , a path  $p$

Output true if  $G$  contains a Ham. path

if  $|p| = |V| - 1$

    └ output true

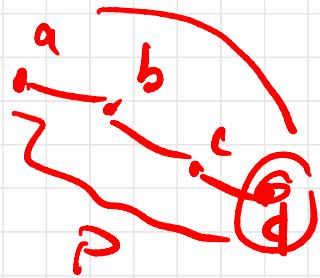
$x \leftarrow$  last vertex in  $p$

for  $y \in N(x)$

    | if  $y \notin p$

        └  $\text{WALK}(G, p + y)$

Output false

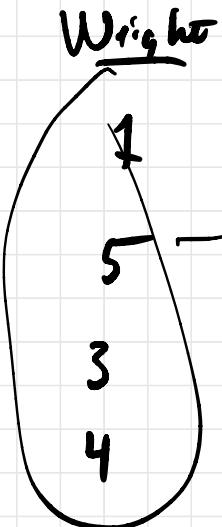


$N(x) =$  neighbourhood  
of  $x$

$|p| =$  length of the  
path  $p$

$|V|$  cardinality of  $V$

<u>Item</u>	<u>Value</u>
$a_1$	15
$a_2$	10
$a_3$	9
$a_4$	5

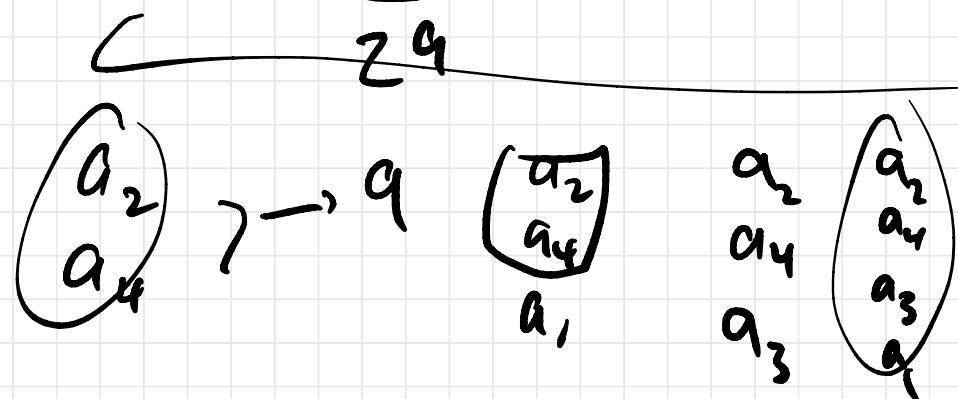


$W = 8$  max capacity

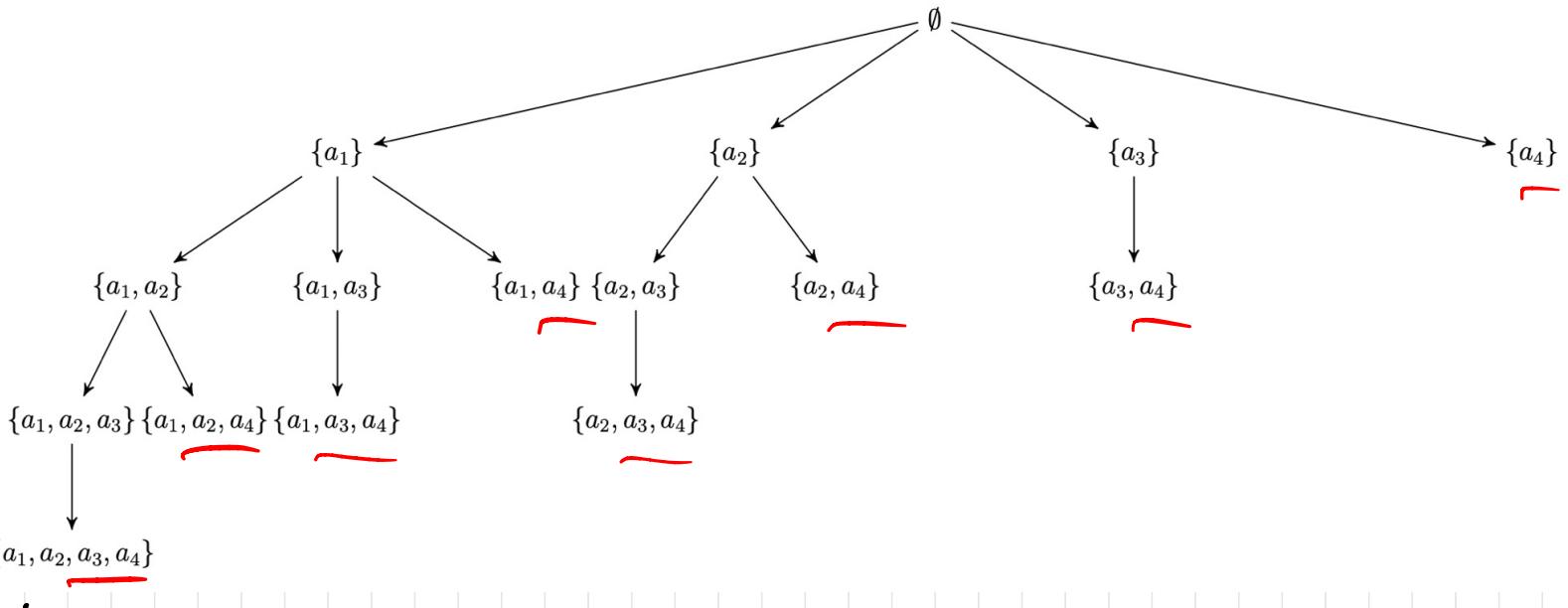
Knapsack

$a_1$	15	1	(7)
$a_3$	9	3	(4)
$a_4$	5	4	(0)

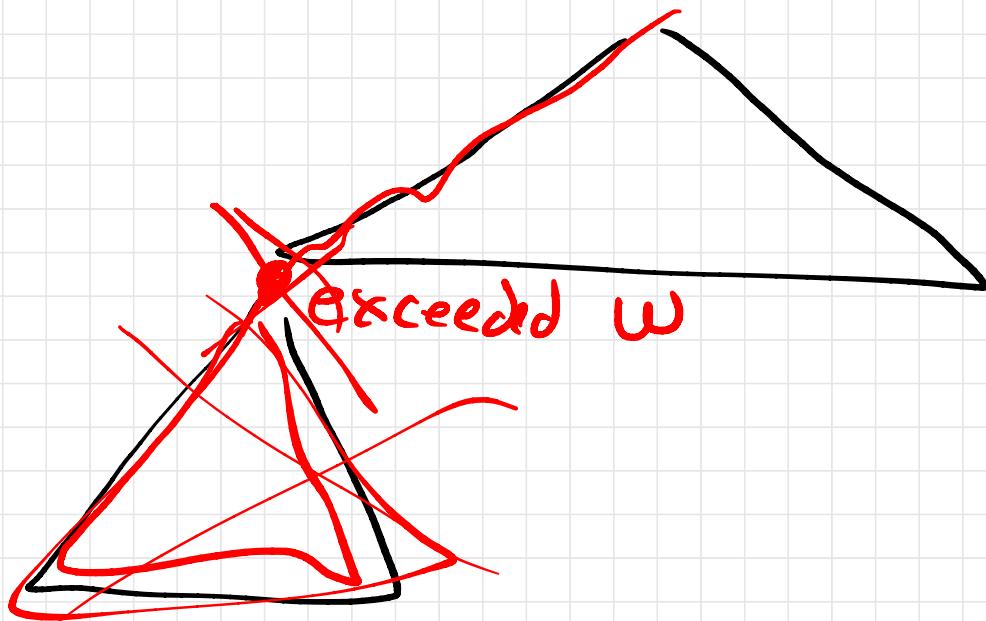
$$\begin{array}{r} a_1 \\ a_2 \\ \hline 15 \\ 10 \\ \hline 25 \end{array} \quad \begin{array}{r} 1 \\ 5 \\ \hline 6 \end{array}$$



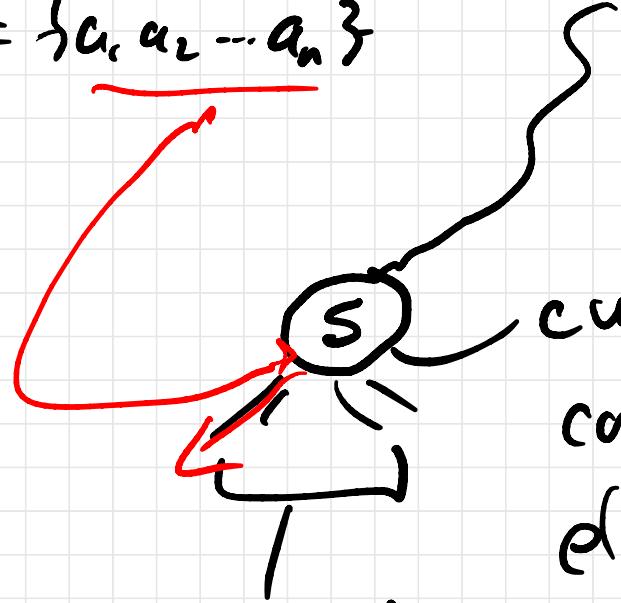
$n = 4$



$\{a_1, a_2, a_3, a_4\}$



$$A = \{a_1, a_2, \dots, a_n\}$$



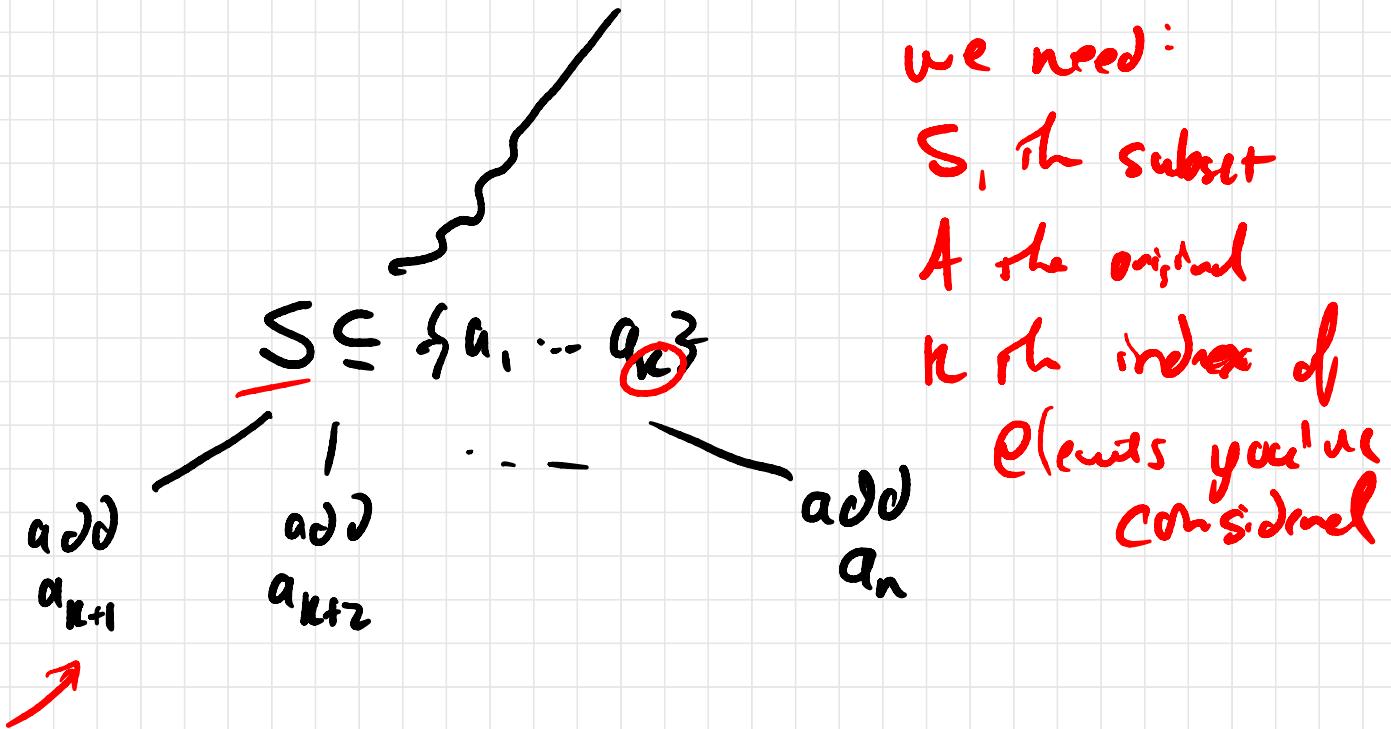
current subset

consisting of some

elements  $a_1, \dots, a_k$

consider

add  $a_{k+1}, a_{k+2}, a_{k+3}, \dots, a_n$



we need:  
 S, the subset  
 A the original  
 k the index of  
 Elements you're  
 considered

# KNAPSACK( $K, k, S$ )

Input: An instance of The 0-1 knapsack  $K = (A, \text{wt. val}, w)$

An index  $k$ , a partial solution  $S \subseteq A$  not consisting  
of elements indexed more than  $k$

Output: A feasible solution at least as good as  $S$

Sum of values  
of items in  $T$

if  $k = n$   
return  $S$

$S_{best} \leftarrow S$

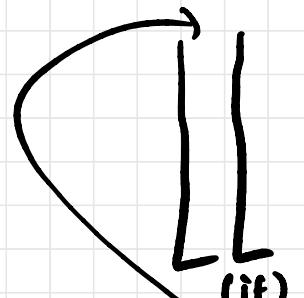
for  $j = k+1 \dots n$

$S' \leftarrow S \cup \{a_j\}$

if  $\text{wt}(S') \leq w$  //feasible

| :

sum of wt's of items in  $S'$

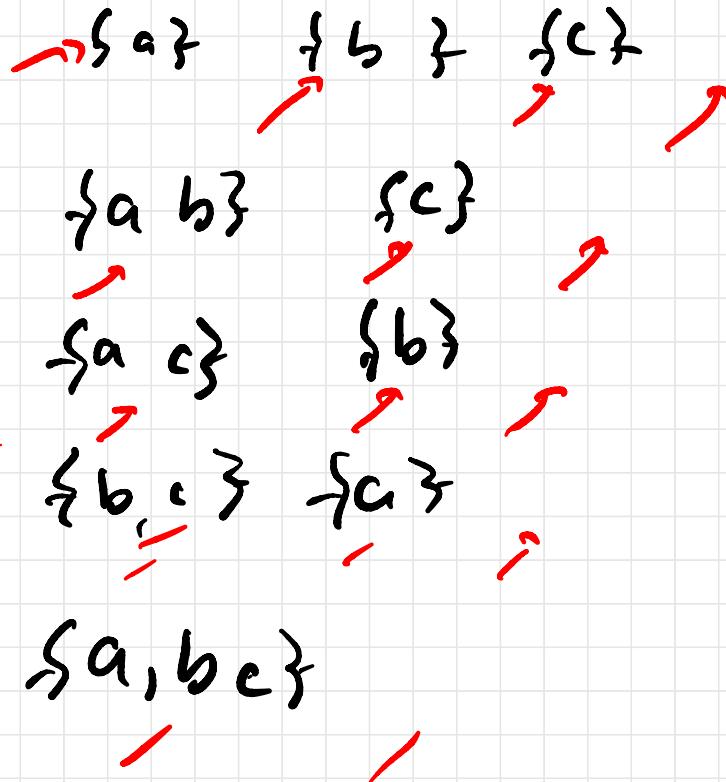


$T \leftarrow \text{KNAPSACK}(n, j, S')$   
if  $\text{Val}(T) > \text{val}(S_{best})$

$S_{best} \leftarrow T$

| — return  $S_{best}$

a b c d



## Generalize Permutations

Ex:  $P(4,2)$  permute 2 elements from a set of size 4

a b c d

a b      a c      a d      b c      b d      c d      (12)  
ba      ca      da      cb      db      dc

$$P(n, r) \quad P(n, n) = n!$$

$P(n, r) =$  1). choose  $r$  elements from  $n$  to arrange  
2) arrange them

$$= \binom{n}{r} \times \frac{r!}{r!}$$

$$= \frac{n!}{(n-r)! \cdot r!} \cdot \cancel{r!}$$

$$= \frac{n!}{(n-r)!}$$

how do you generate all possible permutations,  $P(n,r)$

for each  $r$ -combination  $C$ :

output each permutation of  $C$

Permutations with repetition:

- DNA: A G C T

- generate all DNA strings of length 3 trigrams

AAA  
AAG  
AAC  
AAT  
AGA  
:  
:  
TTT

64

$d_1, d_2, \dots, d_k$

# possible strings:  $4^k$

Symbols:  $s_1, s_2, s_3, \dots, s_n$

Given  $n$  symbols how many "strings" of length  $k$  are there?

$$\begin{aligned}n &= 2 \\s_1 &= 0 \\s_2 &= 1 \\2^k\end{aligned}$$

$$\underbrace{n \cdot n \cdot n \cdots n}_k = n^k$$

Base 2

0 0 0 0	0
0 0 0 1	1
0 0 1 0	2
0 0 1 1	3
0 1 0 0	4

Base 4

000	0 → A
001	1 → G
002	2 → C
003	3 → T
010	
011	
012	
013	
020	
.	
2	

$d \times 10^k$

$$1874 = 1 \cdot 10^3 + 8 \cdot 10^2 + 7 \cdot 10^1 + 4 \cdot 10^0$$

$$\begin{array}{cccccc} & & \downarrow & & & \\ \therefore & 2^3 & & 2^2 & & 2^1 & 2^0 \end{array}$$

SAT = Satisfiability

Given a predicate on  $n$  variables:

boolean variables =  $\begin{matrix} 0 \\ 1 \end{matrix}$

$P(x_1, x_2 \dots x_n)$

is there a truth setting  $\vec{x} = x_1 \dots x_n$

such that  $P(\vec{x}) = 1$

$\frac{1}{0}, \frac{1}{10}, \frac{0}{0} \neq$

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_3) \wedge (x_3 \vee \neg x_1) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3)$$

$x_1$	$x_2$	$x_3$	$P(\vec{x})$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

This is not satisfiable

$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee x_3)$$

$x_1$	$x_2$	$x_3$	$P(\vec{x})$
0	0	0	0
0	0	1	1

is satisfiable

If you have  $n$  variables, There are  $\underline{2^n}$   
possible truth assignments

$$\mathcal{O}(2^n)$$

Set Partitions : Given  $n$  elements,  $a_1, \dots, a_n$

How many ways are there to partition  
them into a set of subsets

a b

①  $\{a\}$   $\{b\}$

a b c

$\{a\}$   $\{b\}$   $\{c\}$

$\{a, c\}$   $\{b\}$

$\{a\}$ ,  $\{b\}$ ,  $\{c\}$  3

②  $\{a, b\}$

,

$\{a, b, c\}$  2

$\{a, b\}$   $\{c\}$  3

a b c d

$\{a\}$   $\{b\}$   $\{c\}$   $\{d\}$

$\{a\}$   $\{b\}$   $\{c\}$

$\{a\}$   $\{b, d\}$   $\{c\}$

$\{a\}$   $\{b\}$   $\{c, d\}$

$\{a, c\}$   $\{b\}$

$\{a, c\}$   $\{b, d\}$

$\{a, c\}$   $\{b\}$   $\{d\}$

4

3

2

5

15

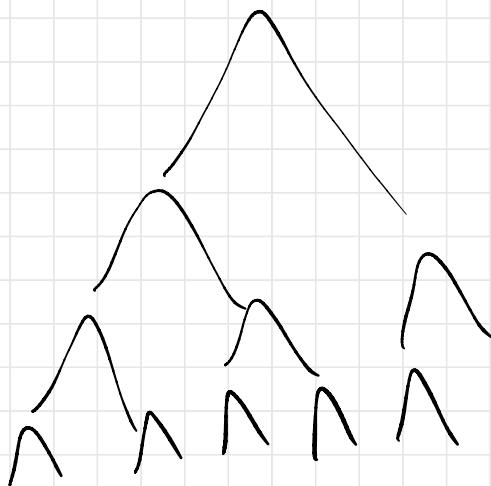
The number of set partitions of  $n+1$  elements is

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k$$

↑  
 $n+1$ th Bell Number

1	1	2	5	15	52	203	877
↑	↑	↑	↑			4140	—

$$\begin{array}{r} 8472 \\ + 1892 \\ \hline \end{array} \quad \begin{array}{r} 10364 \\ > \boxed{\phantom{000}} \\ \hline \end{array}$$
$$\begin{array}{r} 4771 \\ + 8948 \\ \hline \end{array} \quad \begin{array}{r} \boxed{\phantom{000}} \\ > \boxed{\phantom{000}} \\ \hline \end{array}$$



**Theorem 4** (Master Theorem). Let  $T(n)$  be a monotonically increasing function that satisfies

$$\begin{aligned} T(n) &= aT\left(\frac{n}{b}\right) + f(n) \\ T(1) &= c \end{aligned}$$

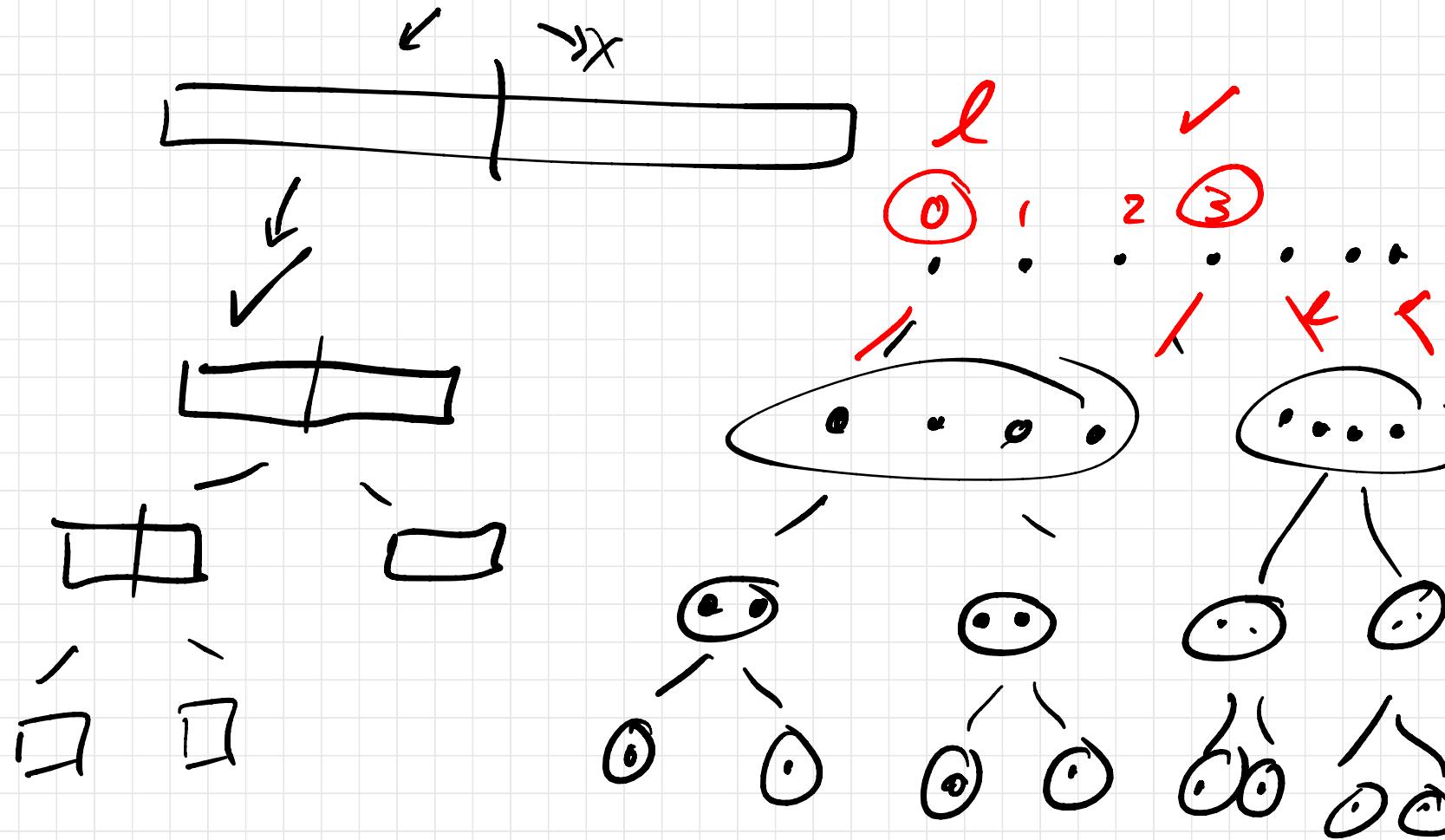
where  $a \geq 1, b \geq 2, c > 0$ . If  $f(n) \in \Theta(n^d)$  where  $d \geq 0$ , then

$$T(n) = \begin{cases} \Theta(n^d) & \text{if } a < b^d \\ \Theta(n^d \log n) & \text{if } a = b^d \\ \Theta(n^{\log_b a}) & \text{if } a > b^d \end{cases}$$

Doing  $a$  recursion calls

cutting the input size by a factor of  $b$

$f(n)$  is the non-recursive work.



A diagram on grid paper showing a vertical line segment from a point labeled  $l$  at the bottom to a point labeled  $r$  at the top. Below this line segment is the equation  $m = \frac{l+r}{2}$ .

$$l \downarrow \quad \int \quad \uparrow \downarrow \quad r$$
$$m = \frac{l+r}{2}$$

linear recursion search:

$$T(n) = \underbrace{\sum_{i=1}^a T\left(\frac{n}{2}\right)}_{\# \text{ of recursive calls}} + \underbrace{f(n)}_{\text{On } \underline{\Theta(1)}} \quad b=2$$

half as big       $f(n) \in O(1)$

$$T(1) = 1$$

$$O(1) = O(n^d)$$

$$a - b^d \geq 2^0$$

$$d = 0$$

$$\begin{aligned} T(n) &= O(n^{\log_2 2}) \\ &= O(n) \end{aligned}$$

Compute  $a^n \bmod m$

for "very large"  $n$

$$12^{26} \bmod 17$$

$n$  is 2000 digits

$$10 \bmod 3 = 1$$

$$10 \% 3$$

$\bmod$  = modulo  
= modulus

$$n = \overbrace{26}^2$$

$$n = \overbrace{26784 \dots 1872}^{100 \text{ digits}}$$

$\log_{10}(n)$  is the # of digits

↓

$\log_2(n)$  # of bits

$n$  is the input

$\log(n)$  is the input size

$$N = \log(n) \Rightarrow 2^N = n$$

$$O(n) = O(2^n)$$

$$a^{26} = \overbrace{a \cdot a}^1 \cdot a^8 \cdot a^2$$

$$a \cdot a \cdot a \cdot a$$

$$\begin{aligned} a \cdot a &= a^2 & 1 \text{ mult.} \\ a^2 \cdot a^2 &= a^4 & 1 \text{ mult.} \\ a^4 \cdot a^4 &= a^8 & 1 \\ a^8 \cdot a^8 &= \underline{\underline{a^{16}}} & 1 \\ && 2 \end{aligned}$$

6 multis

$O(\log_2(n)) \rightarrow$  ~~logarithmic?~~ linear

Nope

$n$  input

$N = \log_2(n)$  input size

$O(\log(n)) = O(N)$  linear

# Binary Exponentiation or Repeated Squaring

Input:  $a, n, m$ ;  $n = b_k b_{k-1} \dots b_0$

Output  $a^n \bmod m$

term =  $a$

if  $b_0 = 1$

L product =  $a$

else

L product = 1

for  $i = 1 \dots k$

| term =  $\text{term}^2 \bmod m$

↑  
higher order bits  
↓  
lowest order bit,

| if  $b_i = 1$   
| product = (product  $\cdot$  term)  
| mod m  
| output product



$$12^{26} \bmod 17$$

$$26 = 11010$$

$b_4 b_3 b_2 b_1 b_0$

$$12^{26} = 12^{2^4 \cdot b_4} \cdot 12^{2^3 \cdot b_3} \cdot 12^{2^2 \cdot b_2} \cdot 12^{2^1 \cdot b_1} \cdot 12^{2^0 \cdot b_0}$$

Diagram illustrating the modular exponentiation process:

- A blue curved arrow starts from the base  $12^{16} \cdot 12^8$  at the bottom left and points upwards to the first term  $12^{2^4 \cdot b_4}$ .
- Red curved arrows point from each term to its corresponding power of 12:
  - The first term is  $12^{2^4 \cdot b_4}$ .
  - The second term is  $12^{2^3 \cdot b_3}$ .
  - The third term is  $12^{2^2 \cdot b_2}$ .
  - The fourth term is  $12^{2^1 \cdot b_1}$ .
  - The fifth term is  $12^{2^0 \cdot b_0}$ .
- Labels "Square" and "Square it" are written next to the second and third terms respectively, indicating the steps of squaring the result.
- The final term  $12^{2^0 \cdot b_0}$  is circled in red.

$a \gg 1$  shifts bits of a left  
by 1  
(divides by 2)

$a \& 1$  → gives you jth leastorder bit

60  
八

$$2 \cdot 2 \cdot 3 \cdot 5$$

210  
一

$$2 \ 3 \ 5 \ 7$$

$$\underline{2}^2 \cdot \underline{3} \cdot \underline{5}$$

$$\underline{2} \cdot \underline{3} \cdot \underline{5} \cdot 7$$

$$2 \cdot 3 \cdot 5 = 30$$

$$2 \cdot 5 \cdot 7 \cdot 11$$

$$\begin{array}{r} 770 \\ - \\ 770 \end{array}$$

$$3 \cdot 13 \cdot 17$$

$$\begin{array}{r} 663 \\ - \\ 663 \end{array}$$

$$\underbrace{\gcd(770, 663)}_{=} = 1$$

$$\underline{1768}$$

$$\underline{184}$$

$$\begin{matrix} a \\ - \end{matrix} \quad \begin{matrix} b \\ - \end{matrix}$$

$$\underline{1768} = \underline{184} \cdot 9 + \underline{112}$$

gcd of  $(\underline{184}, \underline{1768})$

has to divide both

gcd must divide all 3

$$\text{gcd}(\underline{1768}, \underline{184}) = \text{gcd}(\underline{184}, \underline{112})$$

$$184 = \underline{112} \cdot 1 + 72$$

$$40 = 32 \cdot 1 + 8$$

$$32 = \boxed{8} \cdot 4 + 0$$

$$112 = 72 \cdot 1 + 40$$

$$72 = 40 \cdot 1 + 32$$

Euclid - simple

Input:  $a, b \in \mathbb{Z}^+$

Output:  $\text{gcd}(a, b)$

1 while  $b \neq 0$

2      $t \leftarrow b$

3      $b \leftarrow a \bmod t$      // remainder of  $a/t$

4      $a \leftarrow t$

5 output  $a$

1) Input: wLOG  $b > a$

2) Size:  $\log_2(b)$

3) Elem. op: line 3

Division

// % 4) how many times is

line 3  
executed?

• Worst case scenario :

maximize the # of iterations

what "choice" of  $b$  keeps :

$$\frac{x}{b}$$

"big"  $\Rightarrow$  make  $b$  as small  
as possible

$$\frac{b}{2} / \frac{b}{2} = 1$$

$n = \#$  of iterations

$$b \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} = 1$$

$$\frac{b}{2^n} = 1$$

$$b = 2^n$$
$$n = \log_2(b)$$

- # of iterations is at most  $\log_2(b)$
- input size is  $\log_2(b) = N$
- 5) Euclid is  $O(\log_2(b)) = O(N)$  (linear)

Input:  $a, b$

$$a_0 = a, b_0 = b$$

$$t_0 = 0, t = 1$$

$$s_0 = 1, s = 0$$

$$q = \lfloor \frac{a_0}{b_0} \rfloor$$

$$r = a_0 - q \cdot b_0$$

while  $r > 0$

$$\left\{ \begin{array}{l} \text{temp} = t_0 - q t \\ t_0 = t, t = \text{temp} \\ \text{temp} = s_0 - q s \\ s_0 = s, s = \text{temp} \\ \vdots \end{array} \right.$$

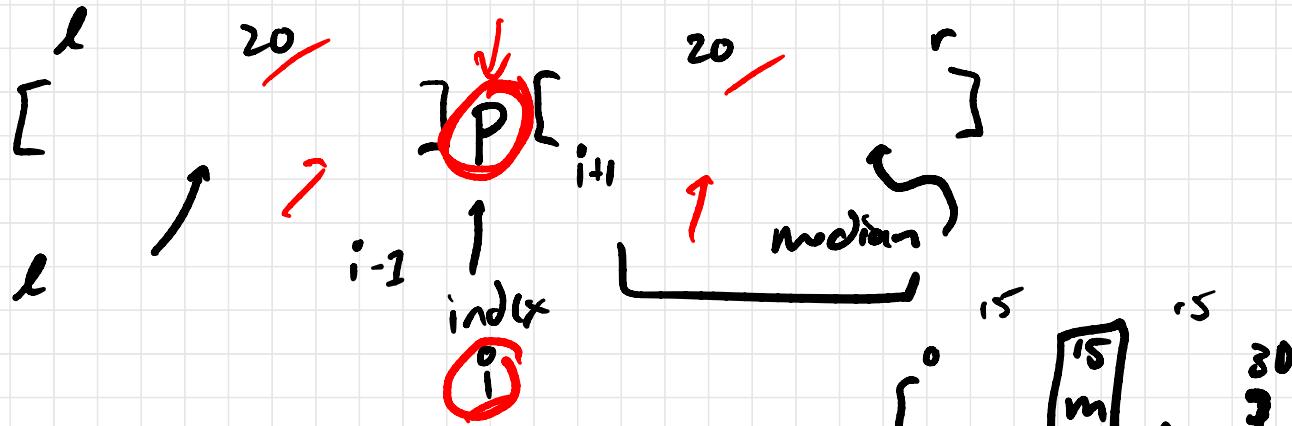
$$\left\{ \begin{array}{l} : a_0 = b_0, b_0 = r \\ q = \lfloor \frac{a_0}{b_0} \rfloor, r = a_0 - q \cdot b_0 \\ \quad \text{if } r > 0 \\ \quad \quad L \quad g = r \end{array} \right.$$

output  $g, s, t$

Note:

$$g = \underline{s} \cdot a + \underline{t} \cdot b$$

$\nearrow$   
gcd

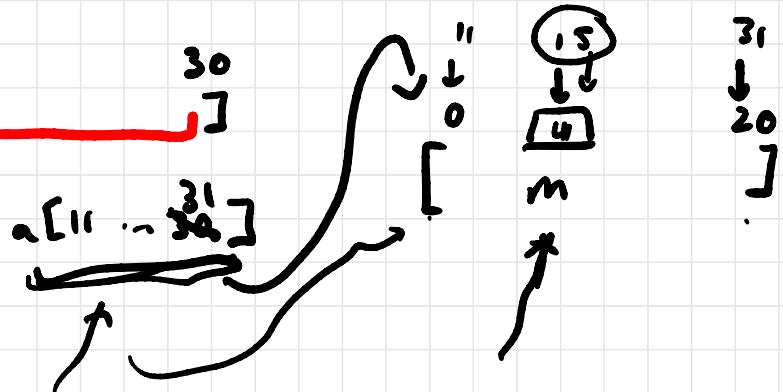


$$n = 31$$

$a$      $\lceil$

$9 \ 10 \ 11 \quad 15 \quad 30$   
 $\lfloor$

$\lceil$        $\sqrt$



$p_{loc}$

↓ partition



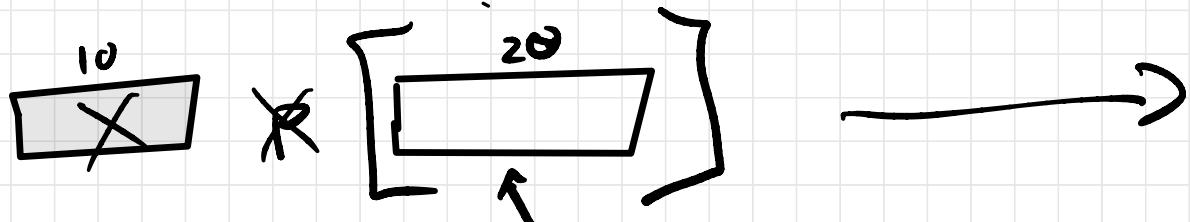
$\nearrow$   $\downarrow$   
index of  $p$

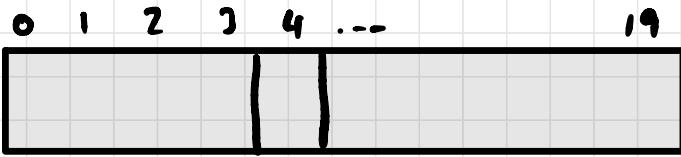
15

$n = 31$

index of  
median:  
if sorted

15





$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\} \leftarrow$  integer remainders of  
mod m

Ex:  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbb{Z}_m$  for any  $m \geq 2$  is a "~~ring~~" or "group"

Algebraic Structure:

• Closure  $x, y \in \mathbb{Z}_m, x+y \pmod{m}$   
is in  $\mathbb{Z}_m$

$x \cdot y \pmod{m}$   
 $\in \mathbb{Z}_m$

$$\mathbb{Z}_6 : \quad 2 + 5 \bmod 6 = 1$$

$$2 \times 5 \bmod 6 = 4$$

- Addition identity: 0

$$\forall a \in \mathbb{Z}_m, \quad 0 + a = a \in \mathbb{Z}_m$$

- mult. identity: 1

$$\forall a \in \mathbb{Z}_n \quad 1 \cdot a = a$$

• Addition inverse:

$$\forall x \in \mathbb{Z}_m \exists y \quad x+y = 0$$

$$\begin{array}{ccc} \mathbb{Z}_m: & \begin{matrix} x \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} & \rightarrow \begin{matrix} y \\ 0 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \end{array}$$

• Multiplication Inverse? ( $x$  other than 0)

$x \in \mathbb{Z}_m, \exists x^{-1}$  such that  $x \cdot x^{-1} = 1$

$\mathbb{Z}_6$

$$\begin{array}{c} x \\ \hline 1 \\ 2 \end{array}$$

$$\begin{array}{c} x^{-1} \\ \hline 1 \quad \checkmark \end{array}$$

$$5 = 5^{-1}$$

DNE = Does not exist

$$3 \longrightarrow 2 \cdot 3 \bmod 6 = 0 \text{ DNE}$$

$$4 \qquad 3 \cdot 3 \bmod 6 = 3$$

$$DNE \qquad 3 \cdot 4 \bmod 6 = 0$$

$$5 \qquad \boxed{ } \qquad 3 \cdot 5 \bmod 6 = 3$$

$$25 \bmod 6 = 1$$

$$x^{-1} = \frac{1}{x} \quad \mathbb{Q} \text{ rationals}$$

$$\mathbb{Z}_m$$

Fact:  $x \in \mathbb{Z}_m$ , a multiplication inverse  $x^{-1}$   
exists iff  $x$  and  $m$  are relatively  
prime: iff  $\gcd(x, m) = 1$

$$x \cdot x^{-1} = 1$$

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$\mathbb{Z}_p$  is a field

0 → no mult. inverse

1 → 1 is always its own inverse

2 ↔ 4

3 ↔ 5

6 ↔ 6

$$x \cdot y \rightarrow x \cdot y y^{-1} = x \cdot 1 \\ = x$$

$$\mathbb{Z}_m = \{0, \dots, m-1\}$$

- hash tables
- pseudo random # generators

$d_n(e_n(x)) \stackrel{?}{=} x$

a, b are inverses of each other  
mod  $\phi(n)$

$$d_n(x^a \text{ mod } n) * (x^a)^b \text{ mod } n \equiv \frac{n!}{n}$$

$$= x^{a \cdot b} \text{ mod } n$$

$$= x' \text{ mod } n$$

$$= x$$

$$b = a^{-1}$$

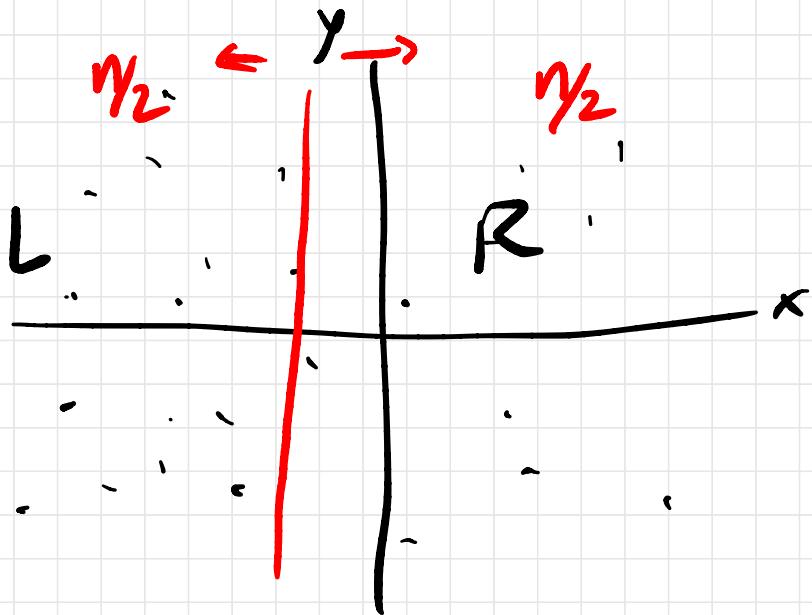
Given : a set of points in 2-D space

Find : The two closest pair

$O(n^2) \rightarrow$  Brute Force examined every pair

$$\binom{n}{2} \in O(n^2)$$

① Divide : divide it into 2 sets along the  $x$ -coordinate

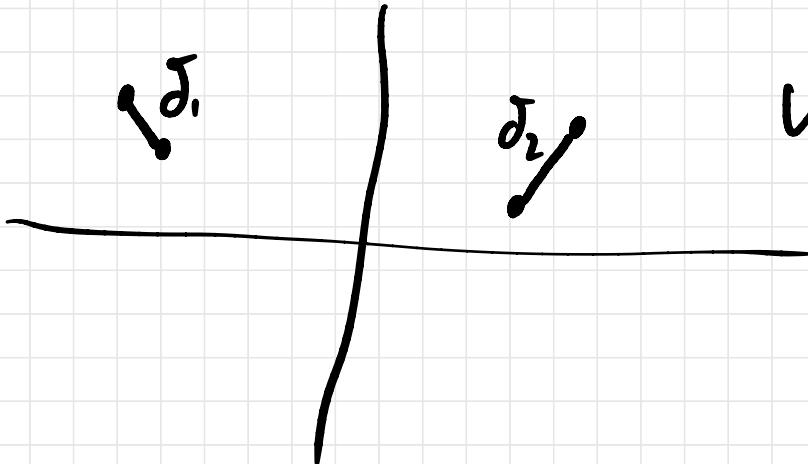


Conquer: 1) find the 2 closest pair in L  $(x_a, y_a), (x_b, y_b)$

Find the 2 closest pair in R  $(x_a', y_a'), (x_b', y_b')$

2) which pair is closer?

$$\delta = \min \{ \delta_1, \delta_2 \}$$

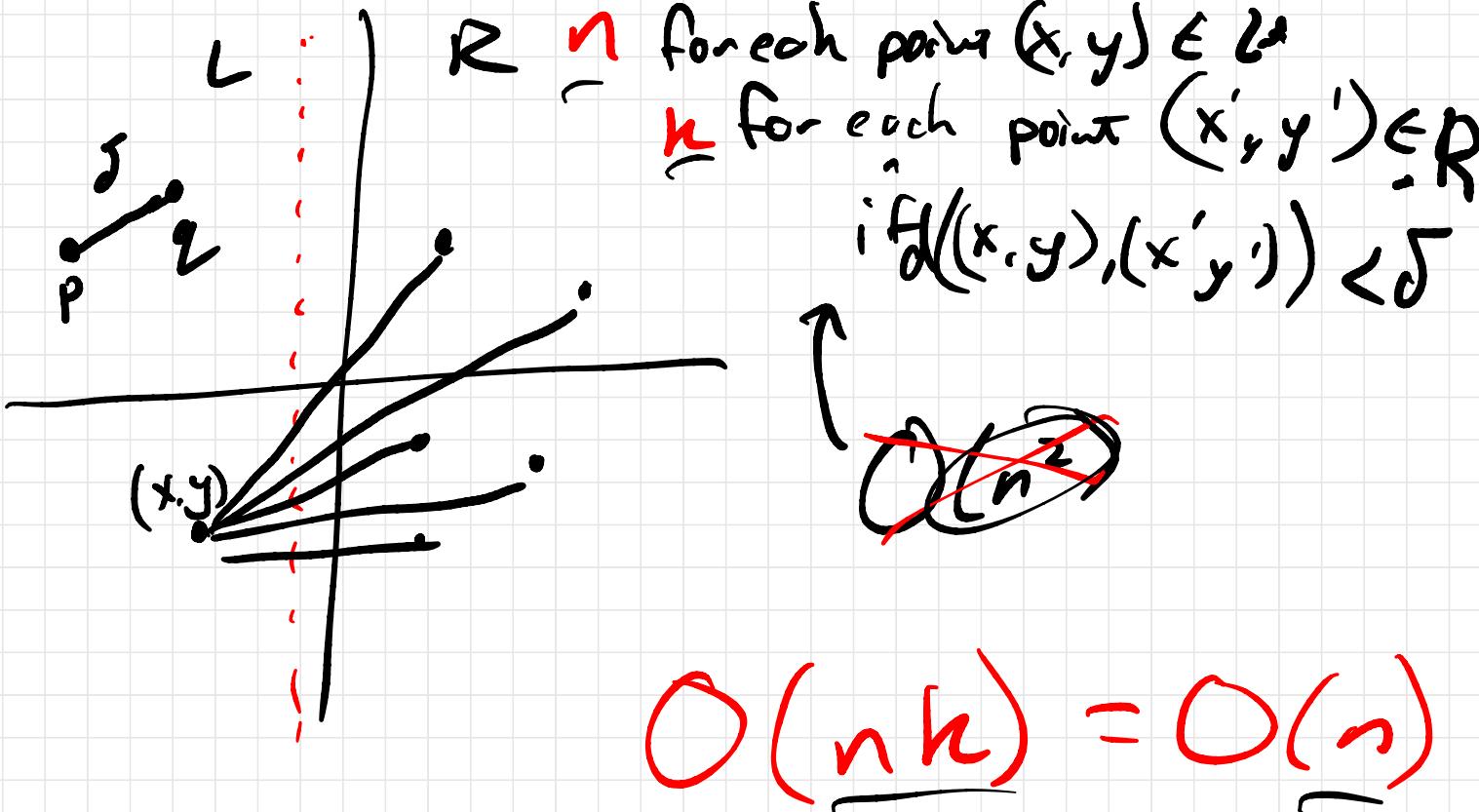


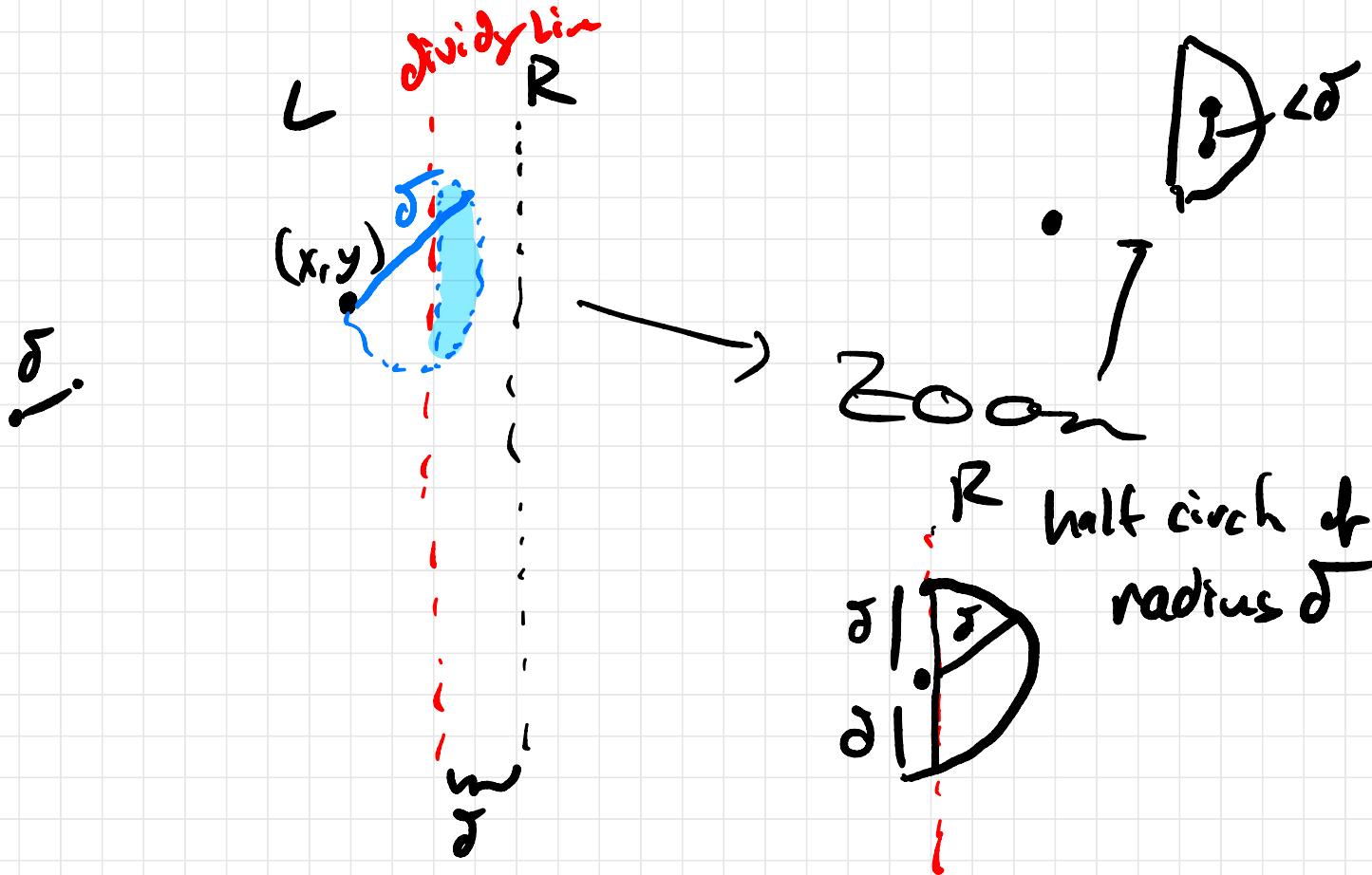
WLOG:  $\delta_1$  is min.

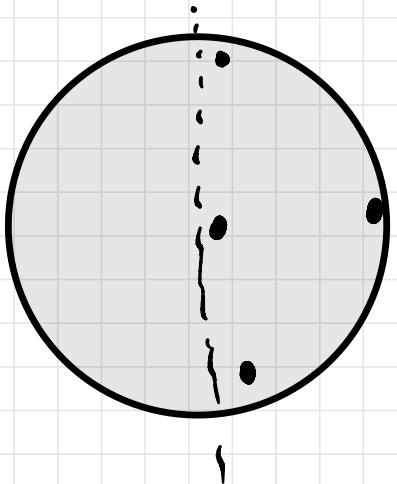
Digression: Base Case?

when  $n = 2$  : only 2 points

Stop. By definition you are done.







Fact: you can fit at most  $K$  points into a half circle of radius  $\delta$  such that each point is at least  $\delta$  distance from each other

## Hexagonal Packing:

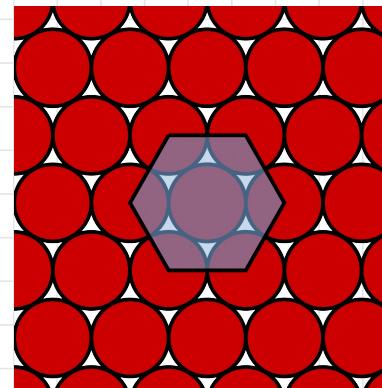
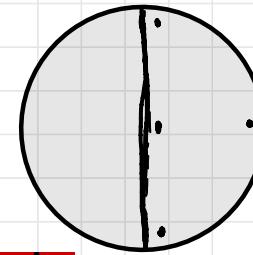
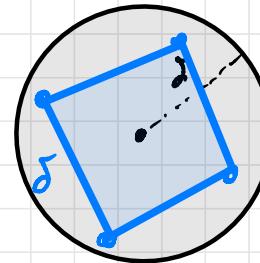
In a (convex?) polygon of Area  $A$ ,  
you can fit at most

$$\frac{4A}{\pi \delta^2}$$

points which are a distance  $\delta$  or  
greater from each other

Circles:  $A = \pi \delta^2$ , min distance:  $\delta$

$$\Rightarrow \frac{4 \pi \delta^2}{\pi \delta^2} = 4$$



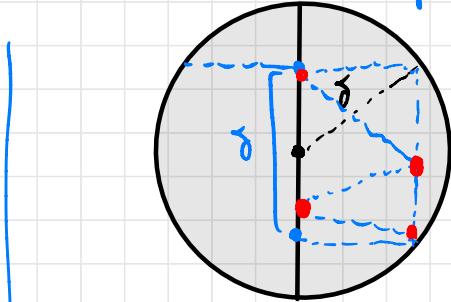
4 likely not possible  
but an acceptable  
over estimate.

Chord length:

$$2\sqrt{r^2 - d^2}$$

$d$  = distance from center

$$.866\delta$$

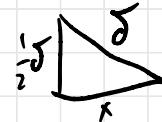
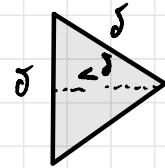


↓

$$2\sqrt{\delta^2 - \left(\frac{1}{2}\delta\right)^2} = 2 \cdot .866 \cdot \delta$$

$$= 2\sqrt{\delta^2 - \frac{1}{4}\delta^2} = 1.732\delta$$

$$= 2\sqrt{\frac{3}{4}\delta^2}$$

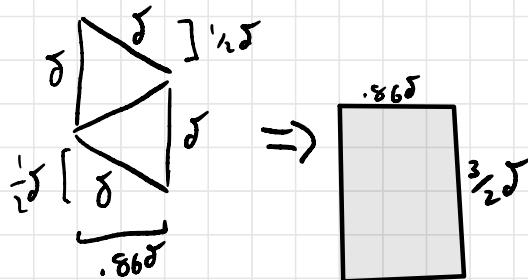


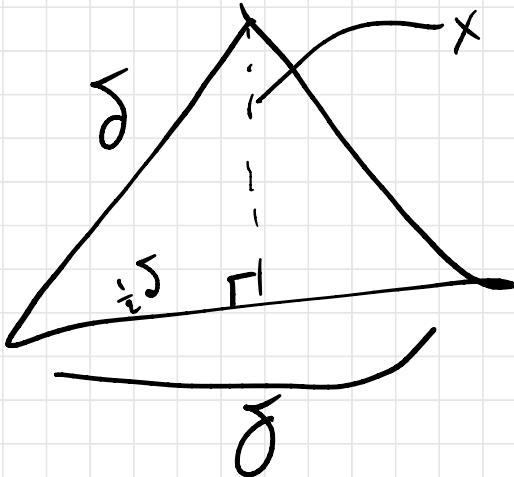
$$x^2 + \frac{1}{4}\delta^2 = \delta^2$$

$$x^2 = \frac{3}{4}\delta^2$$

$$x = \delta\sqrt{\frac{3}{4}}$$

$$= .86\delta$$





$$x^2 + \left(\frac{1}{2}d\right)^2 = d^2$$

$$x^2 + \frac{1}{4}d^2 = d^2$$

$$x^2 = \frac{3}{4}d^2$$

$$x = \sqrt{\frac{3}{4}d^2}$$

$$= d\sqrt{\frac{3}{4}}$$

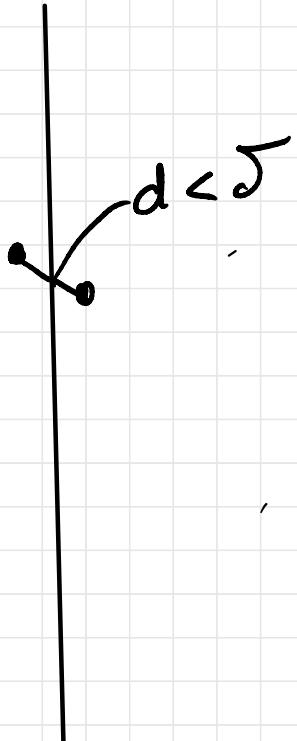
$$= 5 \cdot .866025$$

Left



$\eta/2$

N



Right

WLOG:

assume  $\delta_1 < \delta_2$

$\eta/2$   
points

Naive:

for each  $x$  in Left Partition:  $n/2$

    for each  $y$  in Right Partition:  $n/2$

$d \leftarrow \text{dist}(x, y)$       1

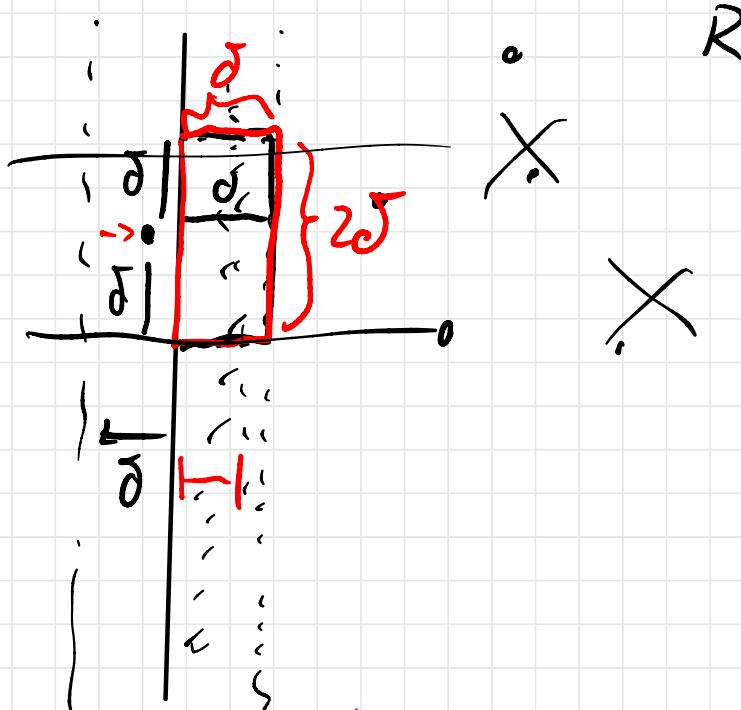
        if  $d < \delta$

            L update 2 closest pairs

$$\frac{n}{2} \cdot \frac{n}{2} = \boxed{\frac{1}{4}} n^2 \in \underline{O(n^2)}$$

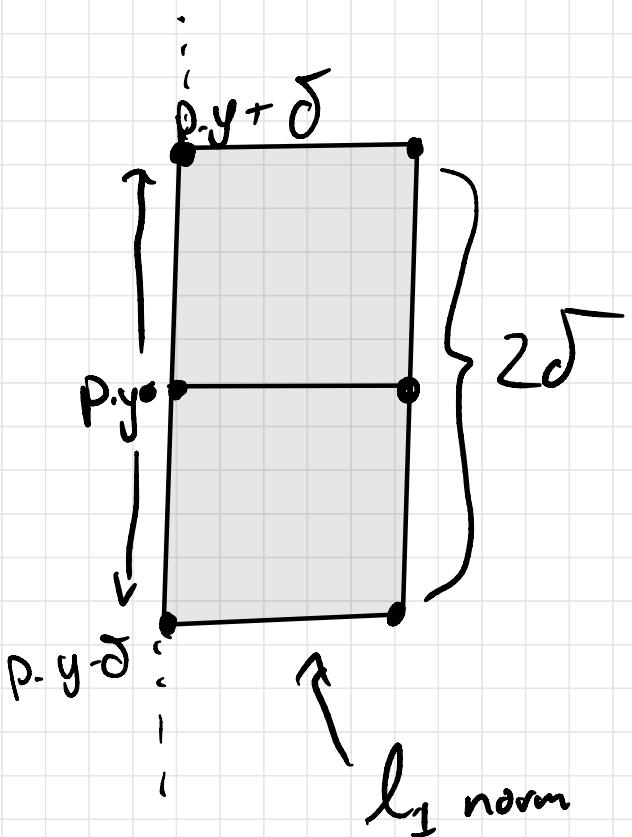
• consider 1 point i = L

L



right "slice"

R

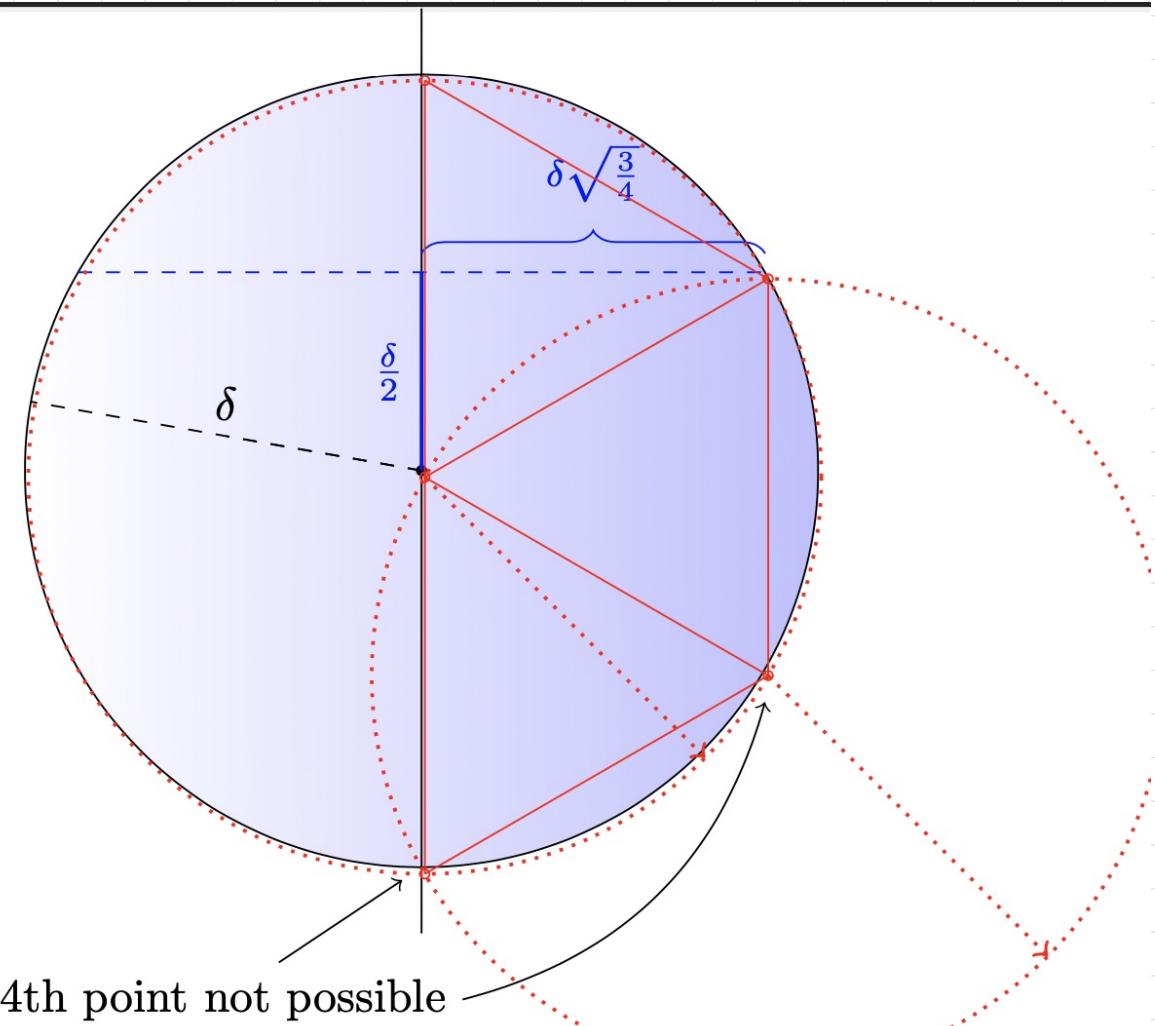


Observe: point within  
this region must be  
at least  $\delta$  distance  
away from each  
other

Observe: there are at most  $\boxed{k}$  points that are a distance  $< \delta$  from the point in the left slice

$$C(n) = 2C\left(\frac{n}{2}\right) + \underline{n \log(n)} + n$$

$$C(n) \in O(n \log^2(n))$$



for each  $x$  in Left Partition:  $n/2$

[ for each  $y$  in Right Partition:  $K$   
[      $d \leftarrow \text{dist}(x, y)$   
[     if  $d < \delta$   
[         L update 2 closest pairs

$$\frac{n}{2} \cdot K \cdot 1 \in \underline{\underline{O(n)}}$$

- 1) Divide points into 2 equal sets L, R
- 2) Recurse to find the closest pair in L, R
  - Base Case: 2 points by defn base are the closest.

3) Conquer:

closest pair in L  $\xrightarrow{\text{choose min}}$  closest pair in R

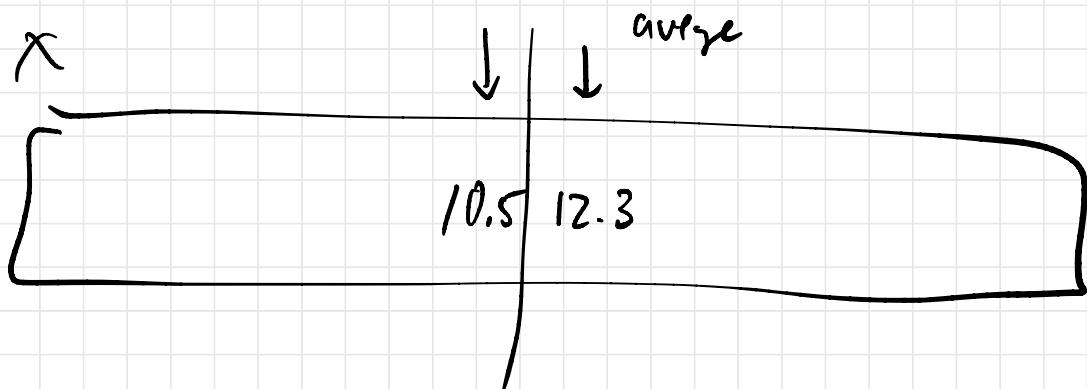
for each point on  $\mathcal{L}$ : consider it to  
the (at most 6) points that  
may be  $\leq 5$  away in  $\mathbb{R}$

$C(n)$  = number of distance calls or comparisons

$$= 2C\left(\frac{n}{2}\right) + \frac{6}{2}n$$

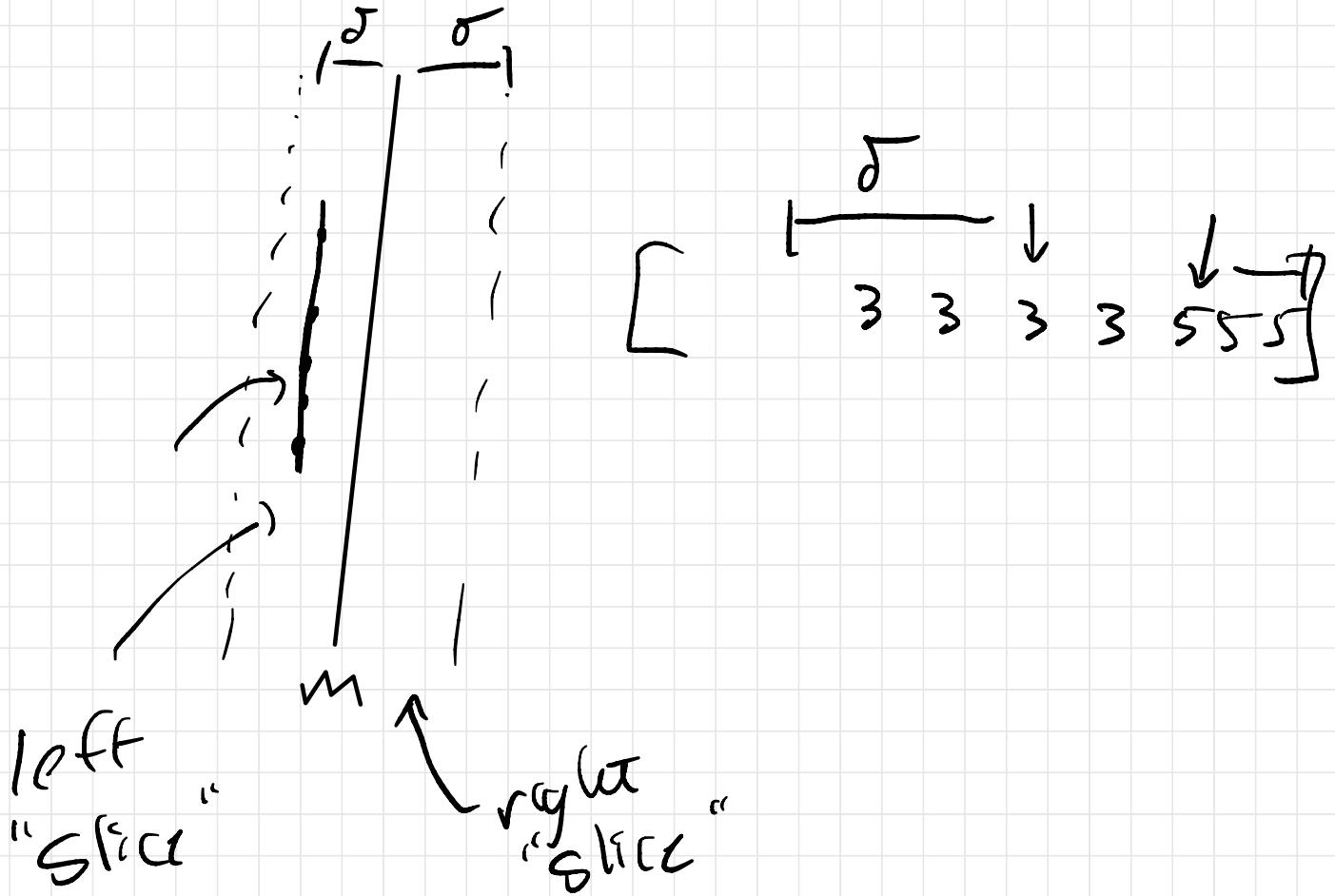
non recursive  
work

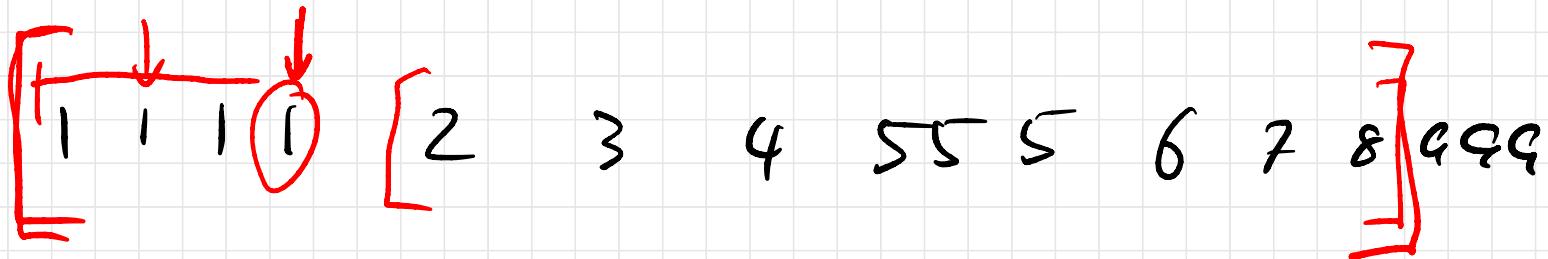
MT :  $a = 2$        $2 = 2^1$   
 $b = 2$   
 $d = 1$        $C(n) \in O(n^d \log(n))$   
                         $= O(n \log(n))$



median  $x$

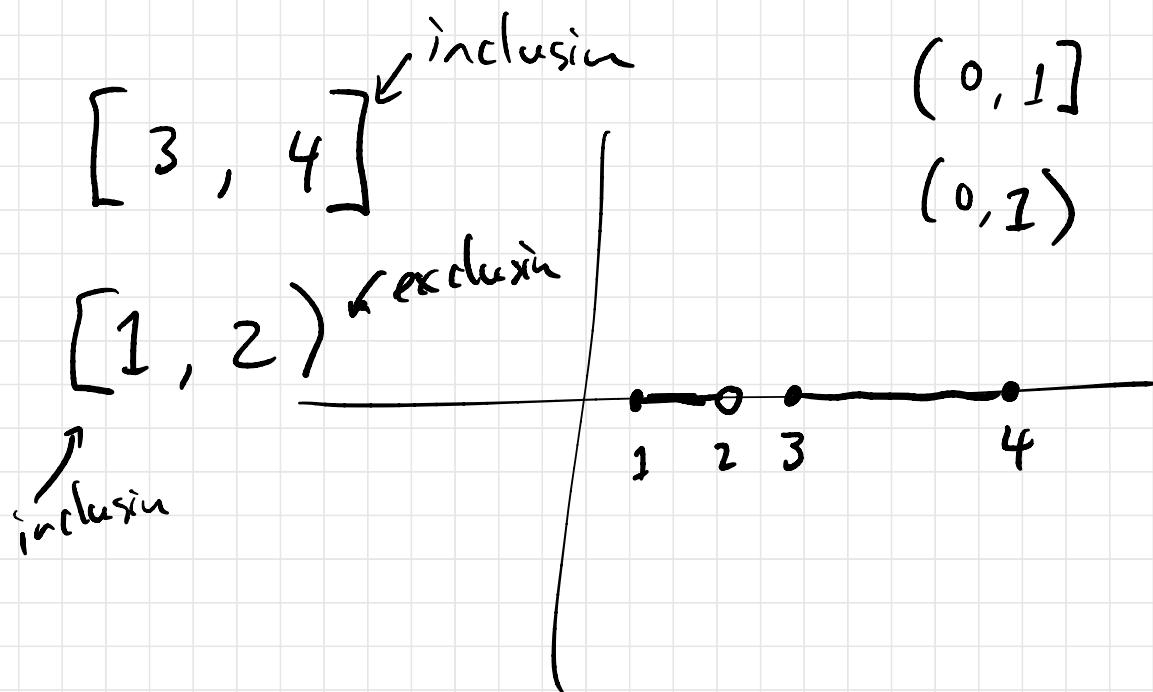
10.9





want: values [2.5, 8.5]

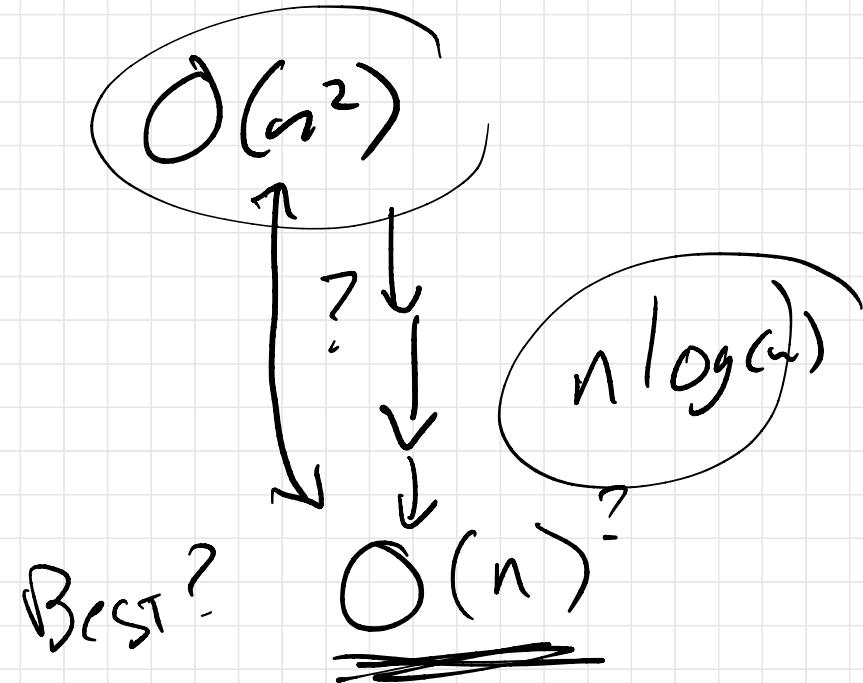
Bin Search :- 1 [1, 8.5]



$$\begin{array}{r}
 \begin{array}{r}
 2 & 5 & 4 \\
 7 & 3 & 8 & 7 \\
 \times & 4 & 5 & 6 & 2 \\
 \hline
 1 & 4 & 7 & 7 & 4 \\
 4 & 4 & 3 & 2 & 2 & 0 \\
 \hline
 \end{array}
 \end{array}$$

← 4      ← 4      ← 4      ← 4

$n$  digit  $\neq a$   
 $n$  digit  $\neq b$



$$\underline{47} \cdot \underline{51} = \left( \underbrace{4}_{a} \cdot \underbrace{10^2} + \underbrace{7}_{b} \cdot \underbrace{10^0} \right) \cdot \left( \underbrace{5}_{c} \cdot \underbrace{10^1} + \underbrace{1}_{d} \cdot \underbrace{10^0} \right)$$

shifts

$\downarrow$       2 digit mult.

$$(a+b)(c+cd) = ac + ad + bc + bd$$

FOIL

single digit  
mults

$$\underline{\underline{ad + bc}} = (a+b)(c+cd) - ac - bd$$

$n \text{ digits} \geq$

$a \cdot b$

$\rightarrow$

$$a = \begin{array}{c} a_1 \\ \hline \end{array} \quad \begin{array}{c} a_0 \\ \hline \end{array}$$

$n/2 \text{ digits}$        $n/2 \text{ digits}$

$$a = a_1 \cdot 10^{n/2} + a_0$$

$a_0 \ a_1 \ b_0 \ b_1$   
 $n/2 \text{ digit numbers}$

$$b = b_1 \cdot 10^{n/2} + b_0$$

$$\begin{aligned}
 a \cdot b &= (a_1 \cdot 10^{n/2} + a_0)(b_1 \cdot 10^{n/2} + b_0) \\
 &= a_1 b_1 10^n + \left[ (a_1 b_0 + a_0 b_1) \cdot 10^{n/2} \right] + a_0 b_0 \\
 &= a_1 b_1 10^n + \left[ (a_1 + a_0) \cdot (b_1 + b_0) - a_1 b_1 - a_0 b_0 \right] 10^{n/2} + a_0 b_0
 \end{aligned}$$

①      ③      ②

- ① + ② are  $\lceil n/2 \rceil$  digit numbers, reuse them
- $a_1 + a_0$  is a  $n/2 + 1$  digit number
- $b_1 + b_0$  "
- #3 is a  $\lceil n/2 \rceil$  digit multiplier.

# Karatsuba Multiplication

$M(n)$  = Number of 1 digit mults made  
on 2 n-digit numbers  $a, b$

$$M(n) = 3M\left(\frac{n}{2}\right) + O_n O(n^0)$$

$$\begin{array}{l} a = 3 \\ b = 2 \end{array}$$

$$d = 0$$

$$3 \geq 2^0$$

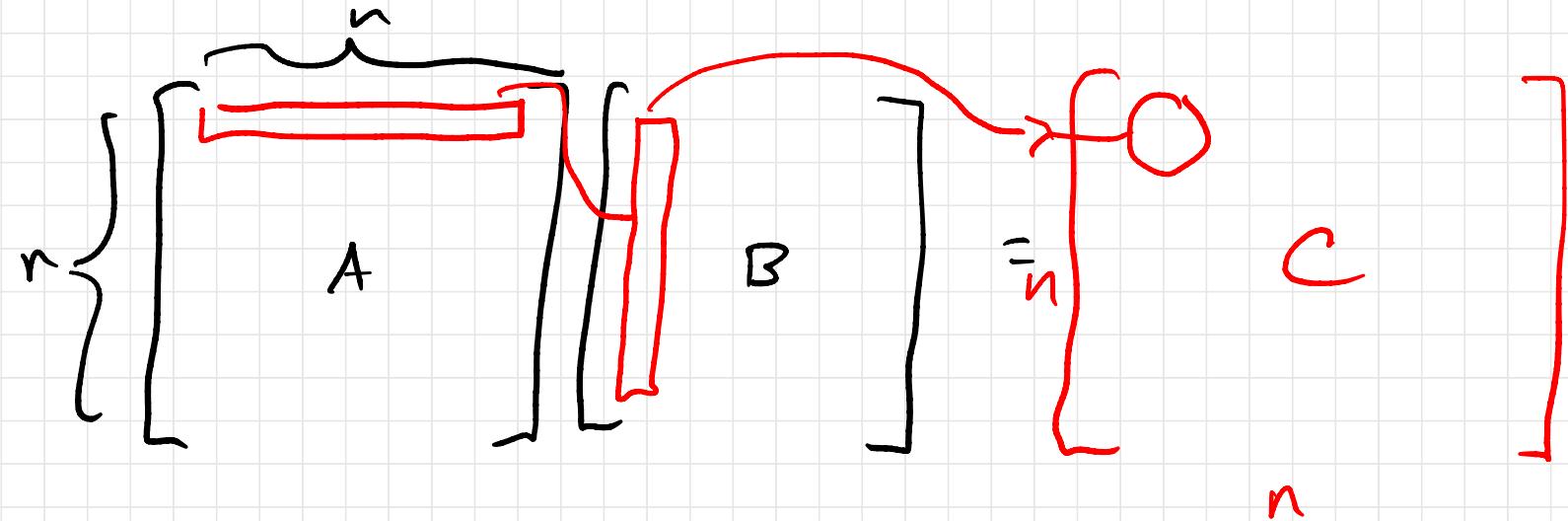
case 3 =

$$O(n^{\log_2(3)}) \approx O(n^{1.58...})$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}$$

$2 \times 2$ :

- 8 mults  $\rightarrow$  generalize
- 4 adds



- $n^2$  entries in  $C$
- for 1 entry:
  - $n$  mults
  - $n-1$  adds

Total:

- $n^3$  mults
- $n^2(n-1)$  additions
- $O(n^3)$

Can't:

input: 2 matrices ( $n \times n$ )

input size:  $2n^2$  (numbers)

$$N = n^2$$

$$O(n^3) = O(N^{1.5})$$

- technically

WLOG: assume input size is  $n$

$$\begin{aligned}
 m_1 &= (a_{00} + a_{11}) \cdot (b_{00} + b_{11}) && \bullet 7 \text{ multipls} && \text{vs} \\
 m_2 &= (a_{10} + a_{11}) \cdot b_{00} && && 8 \\
 m_3 &= a_{00} \cdot (b_{01} - b_{11}) && \bullet 18 \text{ additions} && 4 \\
 m_4 &= a_{11} \cdot (b_{10} - b_{00}) && && \\
 m_5 &= (a_{00} + a_{01}) \cdot b_{11} && && \\
 m_6 &= (a_{10} - a_{00}) \cdot (b_{00} + b_{01}) && && \\
 m_7 &= (a_{01} - a_{11}) \cdot (b_{10} + b_{11}) && &&
 \end{aligned}$$

$$A \cdot B = \begin{bmatrix} m_1 + m_4 - m_5 + m_7 & m_3 + m_5 \\ m_2 + m_4 & m_1 + m_3 - m_2 + m_6 \end{bmatrix}$$

$M(n) = \# \text{ mults by Strassen}$

$$= 7M\left(\frac{n}{2}\right) + \underline{0}$$

$$\begin{array}{ll} a = 7 & d = 0 \\ b = 2 & \end{array}$$

$$7 \geq 2^0$$

$$M(n) \in O(n^{\log_2(7)}) \approx O(n^{2.807})$$

vs  
 $O(n^3)$

Winograd:  $O\left(\frac{n^{2.375477}}{n^2}\right) \hookrightarrow O(n^{2.3727})$  (2012)

$$n \left[ \begin{array}{c|ccccc} & & & & & \\ & & \vdots & \textcircled{0} & \vdots & \\ & - & - & - & - & - \\ & \vdots & & & & \vdots \\ & & & & & \end{array} \right] - \frac{n^2}{4} = \left( \frac{n}{2} \right) \cancel{x}$$