

# Design and Analysis of Algorithms



20 November, 2024

Q. Linear probing and quadratic probing না probe number এর difference কৈমন?

→ Linear probing না কৈমন-

• Unsuccessful search না এবং space occupied

পাওয়ার probability  $\frac{n}{m}$

নিম্নেরটি occupied পাওয়ার probability:  $\frac{n-1}{m-1}$   
ঠাই পথে  $\therefore \frac{n-2}{m-2}$

∴ Total:

$$\frac{n}{m} \cdot \frac{n-1}{m-1} \cdot \frac{n-2}{m-2} \dots \frac{n-i+1}{m-i+1} \leq \left(\frac{n}{m}\right)^{i-1}$$

$$= \frac{1}{1-\alpha} \quad (\alpha = \frac{n}{m})$$

unsuccessful search

→ এই ক্ষেত্র used random variable  $Z(m)$ -  
discrete random variable.

→ successful search না  $Z$  indicator random  
variable

## Convex Hull

Some points are given. We have to determine the smallest possible area that covers all the points.



② Graham Scan → finding the boundary of polynomial.

→ Algorithm কোথা রাখবার পরে এই point সম্পর্কে stack করবেন, those are the boundary points of the required polygon.

- For collinear point, we will consider the farthest since I want to find the boundary without losing anything.

Incourse syllabus: Trie, suffix Tree, Hashing, NP

Exam A proof. ৩ অংকের মতো,  
simulation ৩ অংকের মতো

- RK took this course of 26.

25/11/2024

# NUMBER THEORY (Chapter 3)

- Chinese Remainder theorem ← review on my own
- GCD (Euclidean Algorithm)

$$\text{GCD}(a, b) = \text{gcd}(b, a \bmod b)$$

terminal condition:

if  $b == 0$  return  $a$

- Extended Euclidean:

$$d = ax + by$$

Extended-Ex ( $a, b$ )

if ( $b == 0$ ) return  $(a, 1, 0)$

else  $(d', x', y') = \text{extended-ex}(b, a \bmod b)$

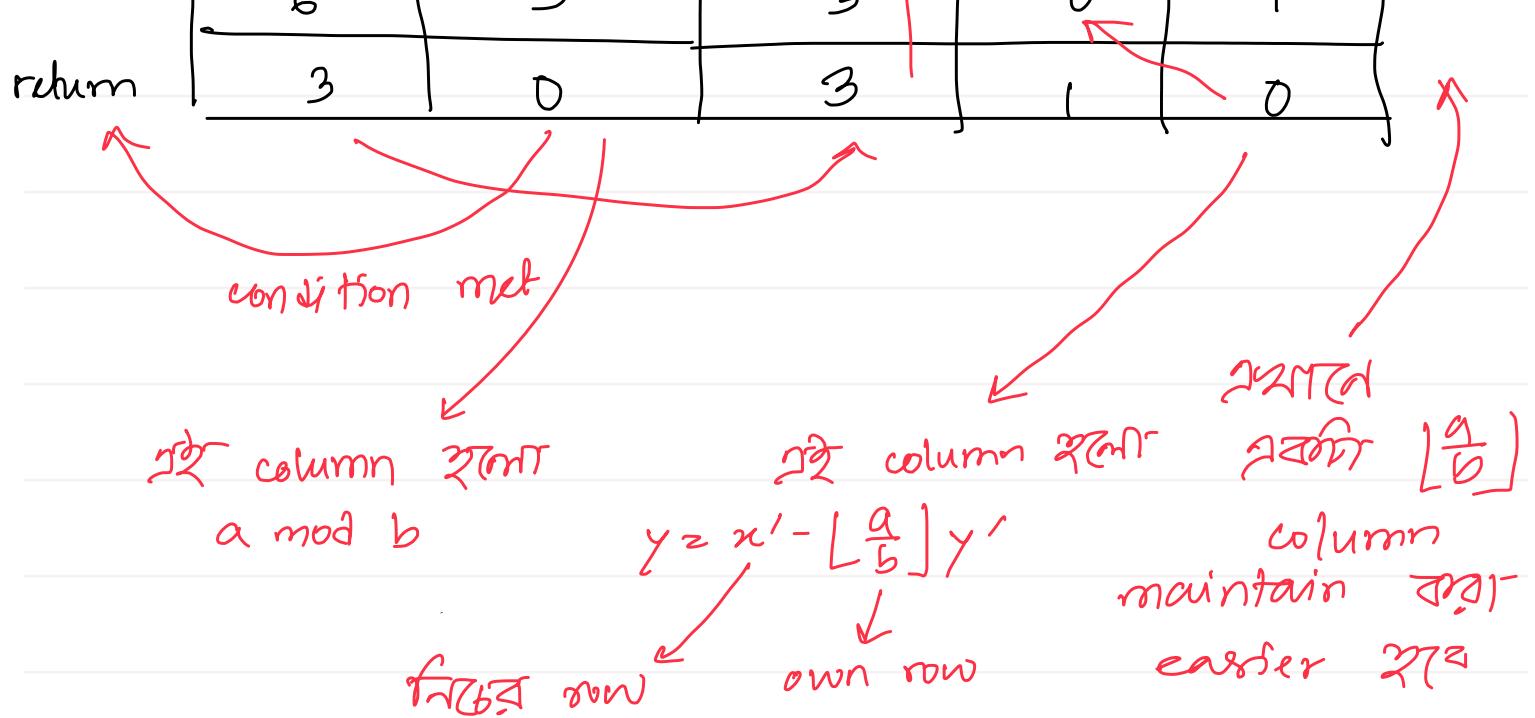
$$(d, x, y) = (d', y', x' - \lfloor \frac{a}{b} \rfloor y')$$

return  $(d, x, y)$

↓  
floor

Simulate: 99, 78

$a$	$b$	$d$	$x$	$y$
99	78	3	-11	14
78	21	3	3	-11
21	15	3	-2	3
15	6	3	1	-2
6	3	3	1	1
3	1	1	1	1



Q. what is the application of extended euclidean algorithm?

- Euler Totient Function

$\varphi(n)$  = the number of integers between 1 and  $n$  (inclusive) which are co-prime to  $n$ .

① If  $n$  is prime, then  $\varphi(n) = n - 1$

② If  $n$  is semi-prime (can be expressed as product of two primes  $p$  and  $q$ )

$$\varphi(n) = (p-1)(q-1)$$

③ If  $n$  is composite,

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots$$

↓

all prime  $\Rightarrow$  product is  $n$

## Fermat's Little Theorem



$$a^{p-1} \equiv 1 \pmod{p} \quad (\text{congruency})$$

basically  $a^{p-1} \bmod p = 1$  (equality)

$p$  = a prime

If  $p$  is not prime but  $a, n$  are co-prime

$$a^{p(n)} \equiv 1 \pmod{n}$$

(Euler) (Generalized)

## RSA

key  $\begin{cases} \rightarrow \text{public (公开鍵)} \\ \rightarrow \text{private} \end{cases}$

when  $A \xrightarrow{\text{message}} B$

- A will encrypt the message with B's public key. It becomes a cipher text C.
- B can decrypt the text C with its own private key.

message কে public key দ্বারা encrypt করলে private  
key দ্বারা decrypt করতে পারবে, again private key  
দ্বারা encrypt করলে public key দ্বারা decrypt  
করতে পারবে, It is commutative,

### challenge : Key Generation

$$\text{Let, } n = p \times q \xrightarrow{\text{prime}}$$

$$\varphi(n) = (p-1)(q-1)$$

$$\text{② } 1 < e < \varphi(n) \quad \text{and} \quad \underbrace{\text{gcd}(\varphi(n), e)}_{\text{relative prime}} = 1$$

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

$$\therefore de \equiv 1 \pmod{\varphi(n)}$$

multiplicative  
inverse of  $e$

Public key:  $\{e, n\}$

Private key:  $\{d, n\}$

মানের কাছে  $\varphi(n)$  কাছে মাত্র জামানীর কাছে  
হয় আছে, But  $n$  কে  $p, q$  কে factorize  
করতে challenging.

$p, q$  একই 1024 bit হবে,

Simulate:  $p = 3$ ,  $q = 11$

$$\phi(n) = 20$$

Let,  $e = 7$  (satisfies the two conditions)

Now, we have to find  $d$ .

$$de \bmod 20 = 1$$

$$\text{And, } d = 3$$

$$\therefore de = 21$$

$$\therefore 21 \bmod 20 = 1$$

### Encryption

$$C = M^e \bmod n$$

Let,  $M$  (message) = 100

$$M^e = 100^7$$

$$n = p \times q$$

$$= (10^2)^7$$

$$= 33$$

$$= 10^{14}$$

$$\text{Now, } 10^{14} \bmod 33 = 1 \rightarrow (100 \bmod 33)^7$$

$$= 1^7$$

$$= 1$$

### Decryption

$$M = C^d \bmod n$$

$$= 1^3 \bmod 33$$

$$= 1 \bmod 33$$

= 1  
↓  
same  $m$  on  $\overline{0 \dots n-1}$ , because this will always give a value less than  $n$ . So,  
 $M$  must be less than  $n$ .

### Restriction on $M$

- This method works due to modular arithmetic.

27 November, 2024

Prove: Any integer can be expressed as a product of primes.

→ induction ফলো করলে ইটটা থাবো,

Basis: 2

do on my own

→ Prove: This factorization will be unique

CRS: Complete Residue System

$\text{mod } 8$

→  $\{0, 1, 2, 3, 4, 5, 6, 7\}$

RRS: Reduced Residue System ( $\text{প্রথম } 8$  এবং  $8$  এর co-prime)

$\{1, 3, 5, 7\}$

$$\therefore \varphi(8) = 4$$

We want to prove Euler's theorem:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Here, let,  $a = 3$  [random number which is coprime with  $n$ ]

$$aa_i \rightarrow \{3, 9, 15, 21\}$$

$$aa_i \not\equiv aa_j \pmod{n} \quad (i \neq j)$$

This is a property of reduced residue system.

Here,

$$a \equiv b \pmod{n}$$

implies  $n$  divides  $a-b \rightarrow n | a-b$   
(notation)

Case 1:  $n = 1$

$$\varphi(1) = 1$$

$$a^{\varphi(n)} = a^1 \equiv 1 \pmod{1}$$

because  $1 | a-1$

Case 2:  $n > 1$

Let  $a_1, a_2, \dots, a_{\varphi(n)}$ : RRS mod  $n$

Then  $\gcd(a_i, n) = 1$ ,  $a_i \not\equiv a_j$   
 $i \neq j$

??

We want to show  $a_{\alpha i}$  is also RRS mod n.

WHAT THE FUCK??

$a_1, a_2, \dots, a_{\varphi(n)}$  is RRS

Then we can say

$$(aa_1)(aa_2) \cdots (aa_{\varphi(n)}) \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}$$

[Congruence]

or  $a^{\varphi(n)} (a_1 a_2 \cdots a_{\varphi(n)}) = (a_1 a_2 \cdots a_{\varphi(n)}) \pmod{n}$

$$\therefore a^{\varphi(n)} \equiv 1 \pmod{n}$$

## RSA

$M, e, d$

$$C = M^e \pmod{n}$$

Now,

$$M = C^d \pmod{n}$$

$$= (M^e \pmod{n})^d \pmod{n}$$

$$= M^{ed} \pmod{n} \quad (\text{modular arithmetic})$$

$\xrightarrow{M \pmod{n}}$  This is where we want to reach

We know

$$ed \equiv 1 \pmod{\varphi(n)}$$

$$\equiv 1 \pmod{(p-1)(q-1)}$$

$$\therefore ed = 1 + k(p-1)(q-1)$$

Now, from the pov of p-

$$\begin{aligned} M^{ed} &\equiv M^{1+k(p-1)(q-1)} \pmod{p} \\ &\equiv M \cdot M^{k(p-1)(q-1)} \pmod{p} \\ &\equiv M \cdot (M^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv M \cdot ((M \pmod{p})^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv M \cdot (1)^{k(q-1)} \pmod{p} \quad \left[ \text{Using Fermat's little theorem} \right] \\ &\equiv M \pmod{p} \end{aligned}$$

Now we are assuming  
m is not a multiple of p

If multiple of p then we have to do an extra step:

$$n \equiv 0 \pmod{p}$$

Similarly,  $M^c \equiv M \pmod{q}$

$$\therefore M^{ed} \equiv M \pmod{n}$$

(এটি পড়ার আবশ্যিক modular arithmetic টার  
ফিল্মগুলি পড়ে নিয়ে, পাশে রাখবো একটি  
টিপ্প সহজ)

পাঠকের class reading assignment  $\rightarrow$  23 Dec

# Exam 1 reduction part প্রিন্সিপ্ল অব্যুক্তি

NP most important

Hashing এর proofs পাওয়া

Trie and Suffix Trie এর input

এর ক্ষেত্রে difference কী? (Trie এর ক্ষেত্রে -  
separator এর মধ্যে, suffix <sup>tree</sup> ক্ষেত্রে blank  
space নাই, we have to focus on these  
conceptual things)

- what are the search approaches, কী এর  
search করি text → , trie কে এবং শব্দাব-  
র্ধন করো?

- occurrence এর location প্রদর্শন করেন ক্ষেত্রে  
ক্ষয়াপ্তিশীল, নববাচ ক্ষেত্রে - এখন এই, we  
need all possible occurrences.

23 December, 2024

- Correctness of RSA প্রমাণ ক্ষেত্রে congruence, Fermat's law নিয়ে প্রালোচনা করতে হবে।
- Proof of Euler theorem

What is CRS  $\rightarrow$  complete Residue System

what is RRS  $\rightarrow$  Reduced Residue System

$$\textcircled{a} \quad a^{\phi(n)} \equiv 1 \pmod{n}$$

• Proof for  $n=1$  and for  $n>1$ .

$$\textcircled{i} \quad a \equiv a \pmod{m}$$

$$\textcircled{ii} \quad a \equiv b \pmod{m}$$

$$\Rightarrow b \equiv a \pmod{m}$$

$$\textcircled{iii} \quad a \equiv b \pmod{m}$$

$$\& b \equiv c \pmod{m}$$

$$\stackrel{\textcircled{ii}}{\Rightarrow} a \equiv c \pmod{m}$$

$$\textcircled{iv} \quad a \equiv b \pmod{m}$$

and  $c \equiv d \pmod{m}$

#

$$ax + cy \equiv (bx + dy) \pmod{m}$$

$$a+c = (b+d) \pmod{m}$$

④ Prove  $a \equiv b \pmod{m}$  iff  $a$  and  $b$  have the same remainder w.r.t  $m$ .

$$a = q_1 m + r_1$$

$$b = q_2 m + r_2$$

$$\Rightarrow a - b = (q_1 - q_2)m + r_1 - r_2$$

Since  $m | (a - b)$ ,  $r_1 - r_2$  must be 0

$$\therefore r_1 - r_2 = 0$$

$\therefore r_1 = r_2$ , both remainders are same.

opposite side 3 ~~TOP RT~~

## CHINESE REMAINDER THEOREM

Let,  $m_1, m_2, \dots, m_n$  be relatively prime numbers such that  $\gcd(m_i, m_j) = 1$ ; if  $i \neq j$  then the linear congruence

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

:

$$x = a_n \pmod{m_n}$$

has a simultaneous solution which is unique modulo  $(m_1, m_2, \dots, m_n)$

• Proof outline.

$$M = m_1 m_2 \dots m_n$$

$$M_1 = \frac{M}{m_1} = m_2 \dots m_n$$

$$M_2 = \frac{M}{m_2} = m_1 m_3 \dots m_n$$

$$M_n = \frac{M}{m_n} = m_1 m_2 \dots m_{n-1}$$

$$\gcd(M_1, m_1) = 1$$

$$\gcd(M_k, m_k) = 1 \quad \forall k = 1 \dots n$$

ff

$$m_k x_k \equiv 1 \pmod{m_k} \quad (\text{any random } x, \exists x \text{ defined by } m_k)$$

$$\bullet x^* = a_1 M_1 x_1 + a_2 M_2 x_2 + \dots + a_n M_n x_n$$

$$m_k \mid M_i \quad (i \neq k) \quad M_i \equiv 0 \pmod{m_k}$$

$$= a_i m_i x$$

এখন  $\frac{a_1}{M_1}, \frac{a_2}{M_2}, \dots, \frac{a_n}{M_n}$  এর পদটির ক্ষেত্রে পুরোটা হবে।

$$a_k M_k x_k = 0$$

Proof- এই পদটির পাশে  $\rightarrow$  solution হবে ক্ষেত্রে হবে,  
then একমাত্র solution হবে।

30.12.2024

Q. Real life application of Chinese Remainder Theorem is what?

Concrete example  $\rightarrow$  next class

Q. What is simultaneous solution?

Q. Euler's theorem  $\Rightarrow m=1$  case ক্ষেত্রে পরিসংখ্যান করে,

④ CRT ৰ' x = a; M<sub>i</sub>; γ; কেন? Simultaneous solution দিব'ব দ্বয়তে হ'বে,

CRT চাইলে CLRS ন'ব পাশাপাশি' we can read Discrete Math book (Stewart)

## BACKTRACKING

- দ্বয় problem গ'ব গুরুবি'k' solution exist বলৈ,

- Brute force -

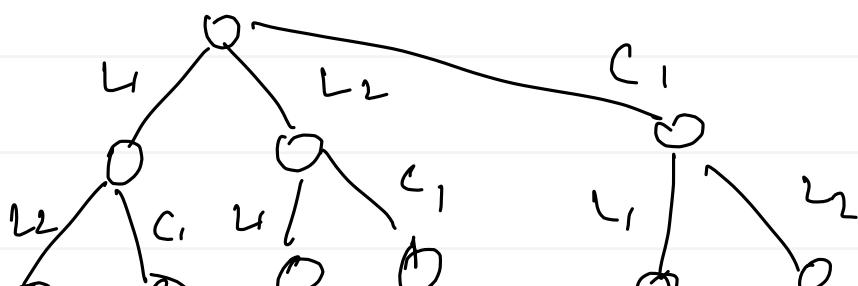
• Backtracking vs DP

CSP: Constraint Satisfaction Problem

- দ্বয়ন'নে অগুণীয়'র বিশ্লেষণ শৃঙ্খলা প্রৰণ' করতে হ'ব,

• Solution is represented on State Space Tree (SST)

def, L<sub>1</sub>, L<sub>2</sub>, C<sub>1</sub>





leaf nodes are giving the solutions.

Let, we place a restriction that C1 cannot be in the middle.

$$\therefore 6 - 2 = 4$$

Q. How to design the bounding function?

- N-Queen Problems

$N \times N$  size chessboard  $\rightarrow$  N n' queen राजा.

Queen can attack row, column & diagonal wise.

$\therefore$  एक रोड़, कॉलन, डायगोनल  $\rightarrow$  multiple queen राजा निर्वाचन,

Let,  $N = 4$

	Q1		
			Q2
		Q3	
			Q4

$Q_1$  place কোর টেবিল  $Q_2$  place পার্স  
 মাইক্রো কিনা, and so on. place না ব্যবহা  
 র কৈল আবার  $Q_1$ , এর ডিফরেন্স change  
 করবে।

## SUM OF SUBSETS SUBSET-SUM PROBLEM

We have a set of numbers. We want to find subsets which have a certain sum.

$$W = \{5, 10, 12, 13, 15, 18\}$$

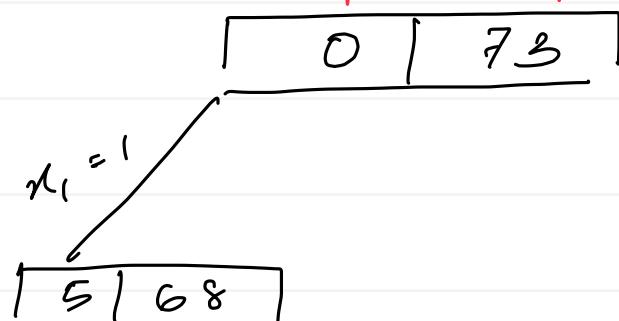
$$\text{sum} = 30$$

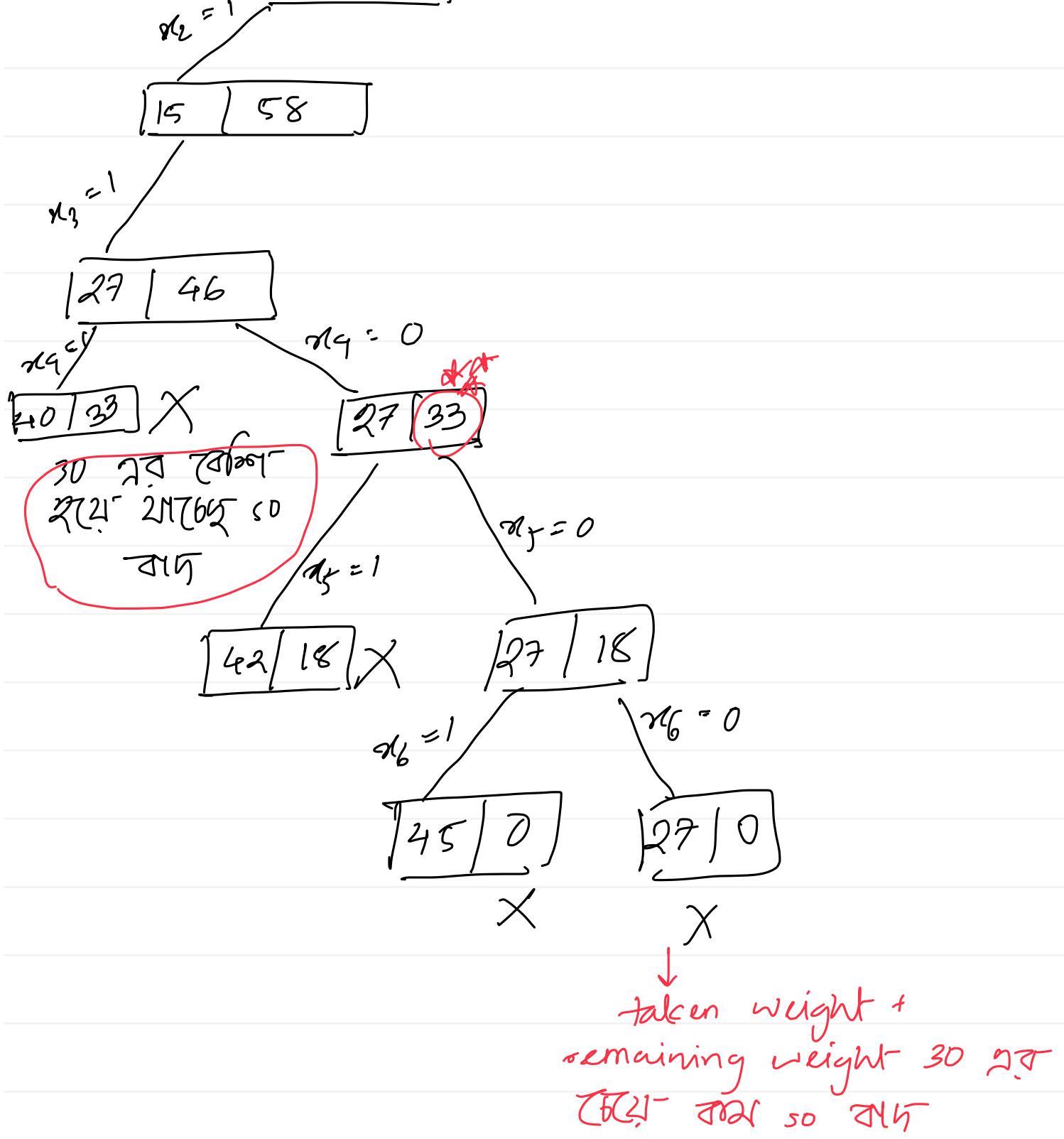
1	1	1	0	0	1	0
1	2	3	4	5	6	

এই element include করব এটি 1.

The solution:

বর্ণ নথিএই  
 ↑  
 বর্ণ সমি





∴ Terminating condition:

$$\sum_{i=1}^t w_i + \sum_{i=t+1}^n w_i < m$$

Explore ক্ষেত্র condition:

$$\sum_{i=1}^k w_i + w_{k+1} \leq m$$

একটি solution পর্যন্ত leaf টি complete  
করবে আলোচনা হবে।

1/1/2025

Subset sum problem  $\nearrow$  set it sorted করলে,  
না আবায় কী কোনো difference আছে?

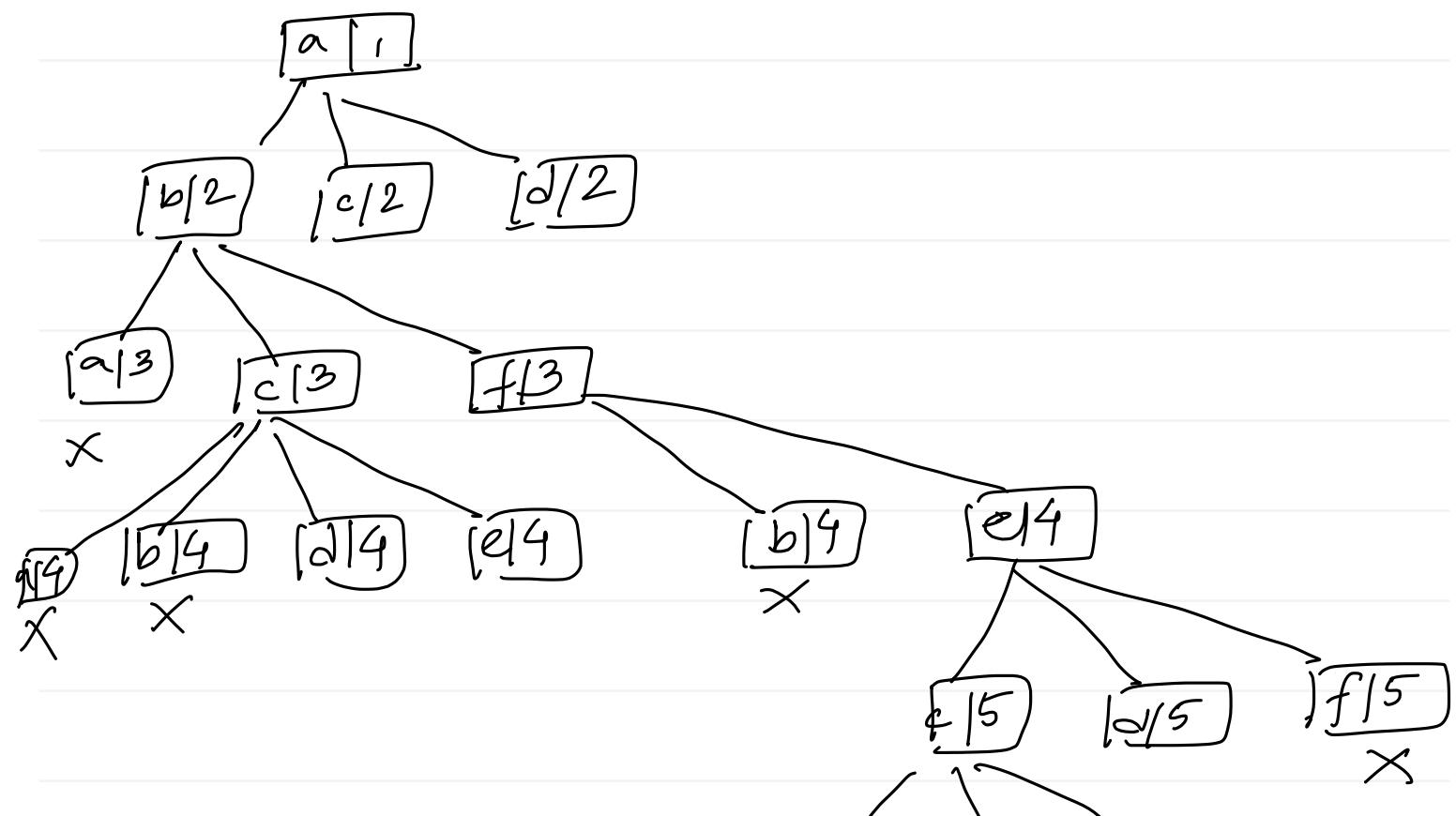
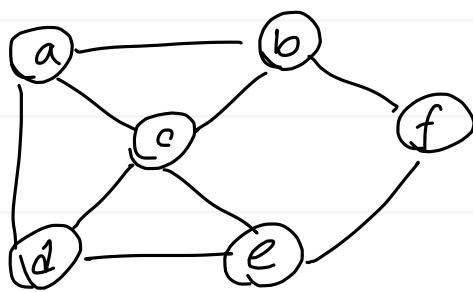
→ sorted না করলে problem নাই, but করলে  
few advantage আছে। Easily বুঝতে  
পারবেো এখন we should stop checking  
the next elements

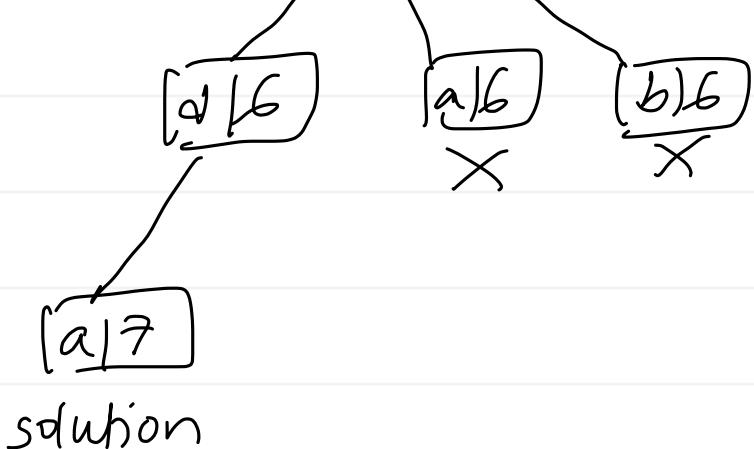
## FEATURES OF BACKTRACKING

Backtracking  $\rightarrow$  we find a feasible solution, and branch and bound approach  $\rightarrow$  we find the optimal solution.

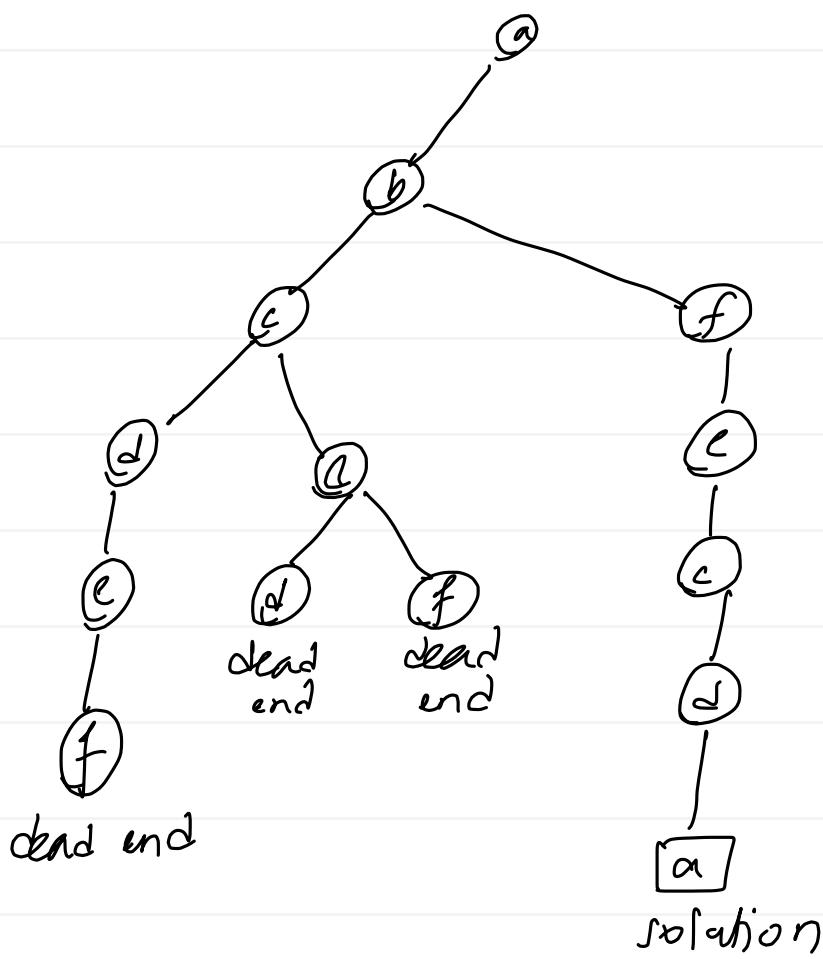
## HAMILTONIAN CIRCUIT

- visit all the nodes and create a cycle.





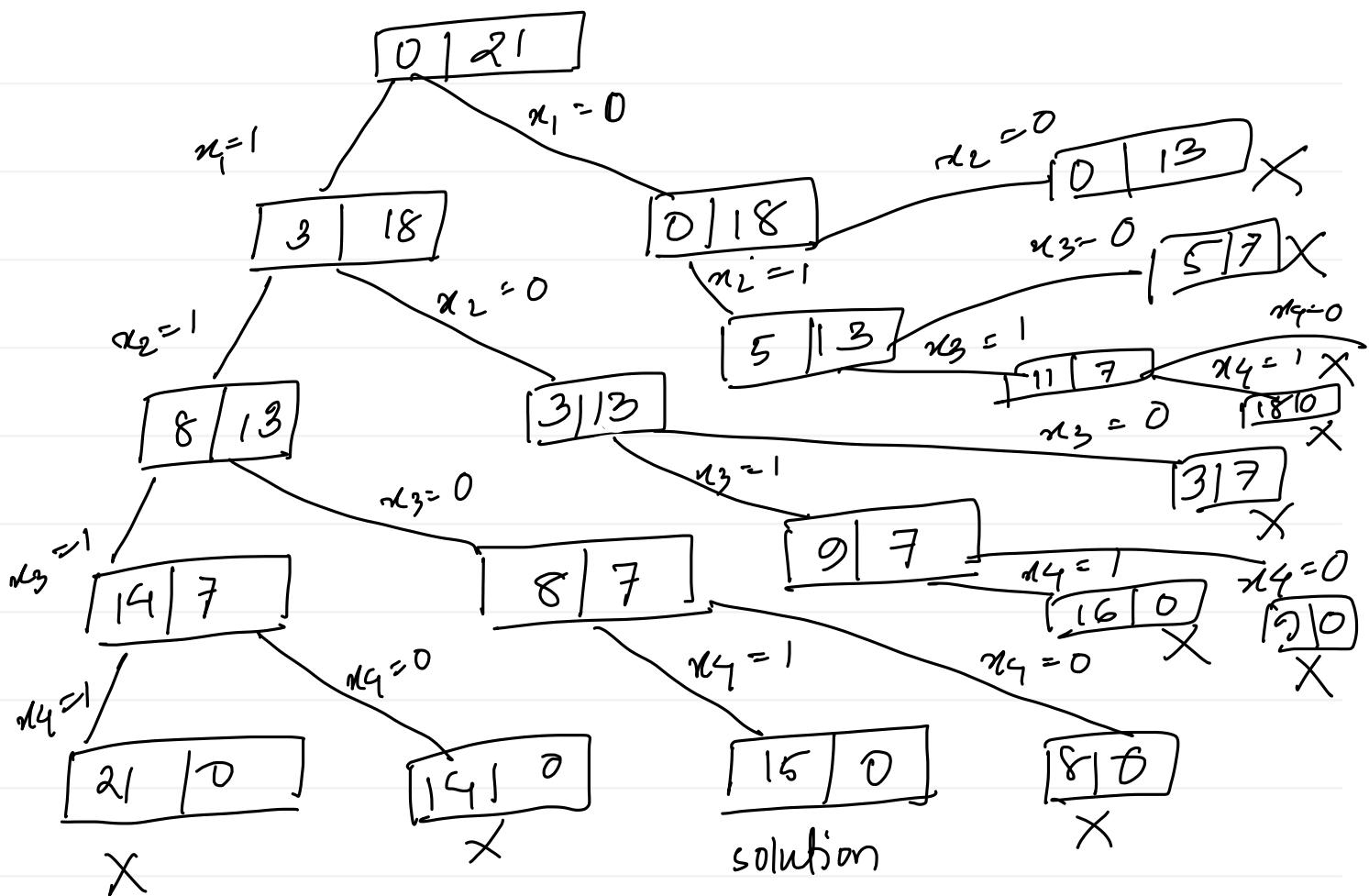
ମତ୍ତାରେ ବସ୍ତୁବଳୀ, BFS approach ରେ, DFS  
approach ଟି ଅନ୍ତର୍ଭବେ।



Q. Draw the state space tree of this subset sum problem:

$$S = \{3, 5, 6, 7\}$$

$$d = 15$$



# Define the bounding functions formally

④ Branch and bound → we want the optimal solution, let's minimal lengths, minimum cost, etc. So, backtracking এবং

Those two additional items:

- bound on the best value of the objective function
- 2 ways breadth first manner to explore  
ব্রেডথ, 3 ways:

① queue

② stack

③ least cost

- track the value of the best solution so far

3 conditions for termination:

- ① not the best solution
- ② not a feasible solution
- ③ no further option/choice is left.

Ques, DP ফর্ম 0/1 knapsack solve কৈবল্য,  
branch and bound ফর্ম 3 solve কৈবল্য,  
Now what are the differences between  
them?

6/01/2025

## Problems related to Branch & Bound

### JOB ASSIGNMENT PROBLEM

	job 1	job 2	job 3	job 4	
person a	9	2	7	8	
person b	6	4	3	7	
person c	5	8	1	8	
person d	7	6	9	4	

- Want to assign the jobs so that total cost is minimum.
- what is the lower bound?

Initially প্রতি person এর কোন সেটের lowest cost  
কি কোরে lower bound হবে ফির i.e., এবেক্ষণে  
কোরে এবেক্ষণে হবেন।

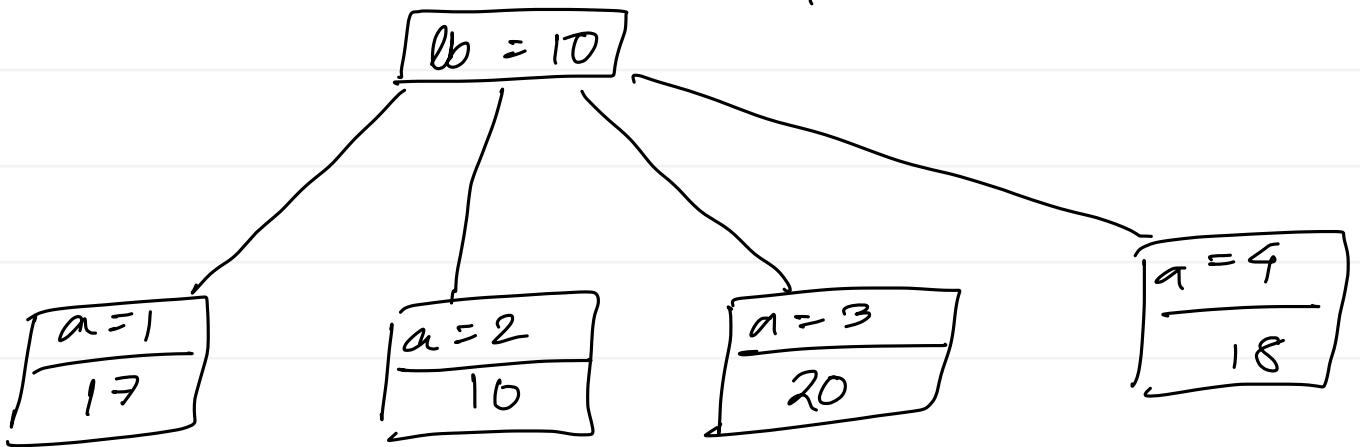
$$\therefore 2 + 3 + 1 + 4 = 10 \text{ (lower bound)}$$

↓

But it's actually feasible as  
since same job cannot be  
assigned to two people (job 3  
to person b and c)

i.e., lower bound  $\hat{C}_L$  & the solution  $\hat{C}_U$ ,  
that is not guaranteed.

\*  $lb = \text{lower bound}$



\* ~~মানুষ~~  $lb = 10$  এর ক্ষেত্রে  $2, 3, 1, 4$ .  $212\pi$   
a assigned job  $\Rightarrow$  উত্তর  $2, 3, 1, 4$ . ~~মানুষ~~  
first  $\hat{C}$  update হবে, যদিও  $a_1, a_2, a_3$  3'rd  
column রেজিস্টার সাফার  
When  $a \rightarrow 2$ , same.

$2, 3, 1, 4$

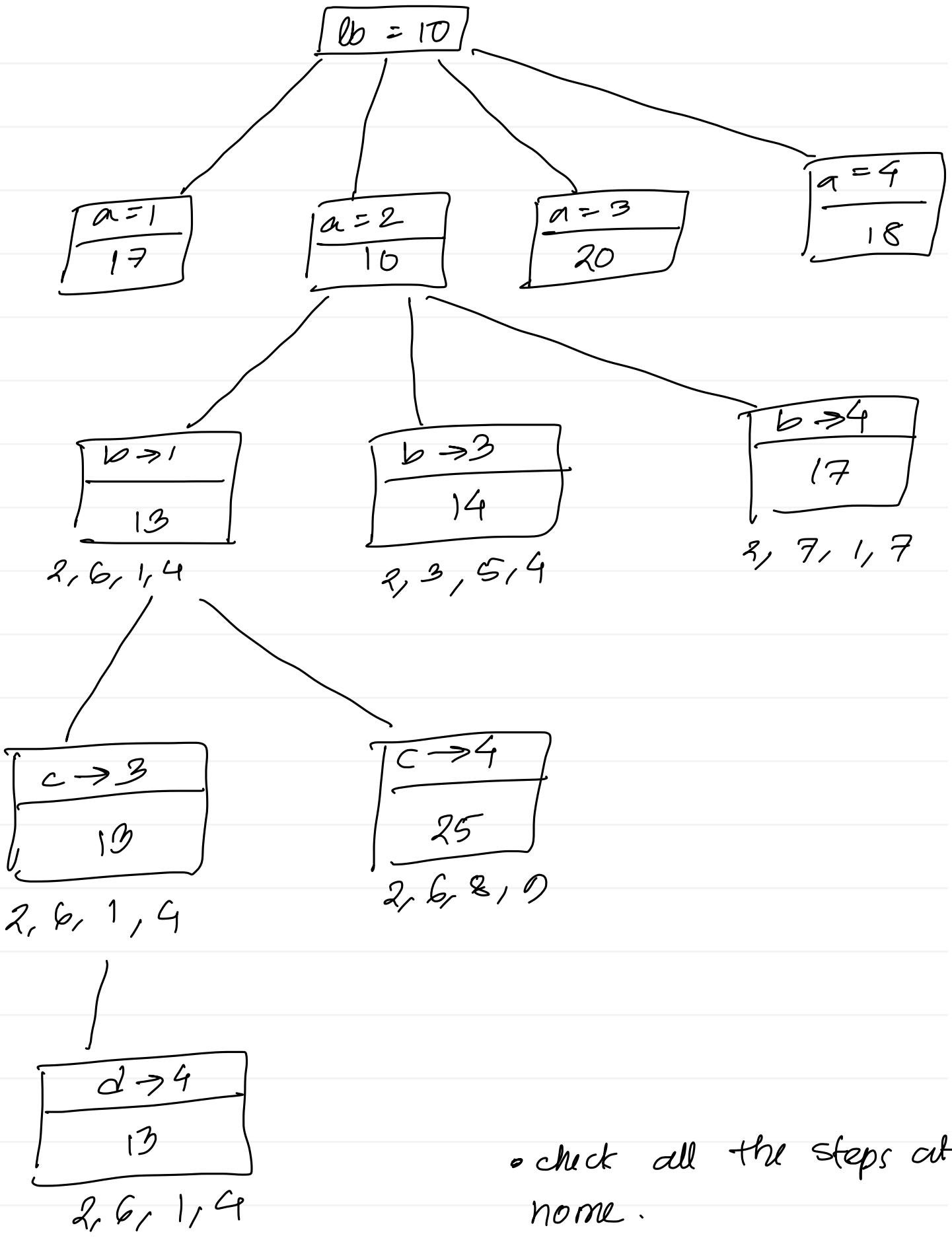
when  $a \rightarrow 3$ ,

$7, 4, 5, 6$

when  $a \rightarrow 4$

$8, 3, 1, 6$

Then  $\hat{C}_U$  closest to initial lower  
bound, এখন  $\hat{C}_U$  next stage  
explosion হবে,



- check all the steps at home.

Once we assign a job to a column  
 we can fix it. Now column 3 has  
 4 jobs each row has minimum 3 fix.  
 The job will assign to it, if  
 column is conflict with others, that  
 is not a problem.

# KNAPSACK PROBLEM

fractional knapsack  $\rightarrow$  greedy

0/1 knapsack  $\rightarrow$  DP

Now, we will try to do 0/1 knapsack with branch and bound.

- It is an optimization problem.
    - maximization problem.

what is the initial upper bound?

item	weight	value	<del>value/weight</del>
1	4	\$40	10
2	7	\$42	6
3	5	\$25	5
4	3	\$12	4

The knapsack's capacity  $w$  is 10.

Initial upper bound:

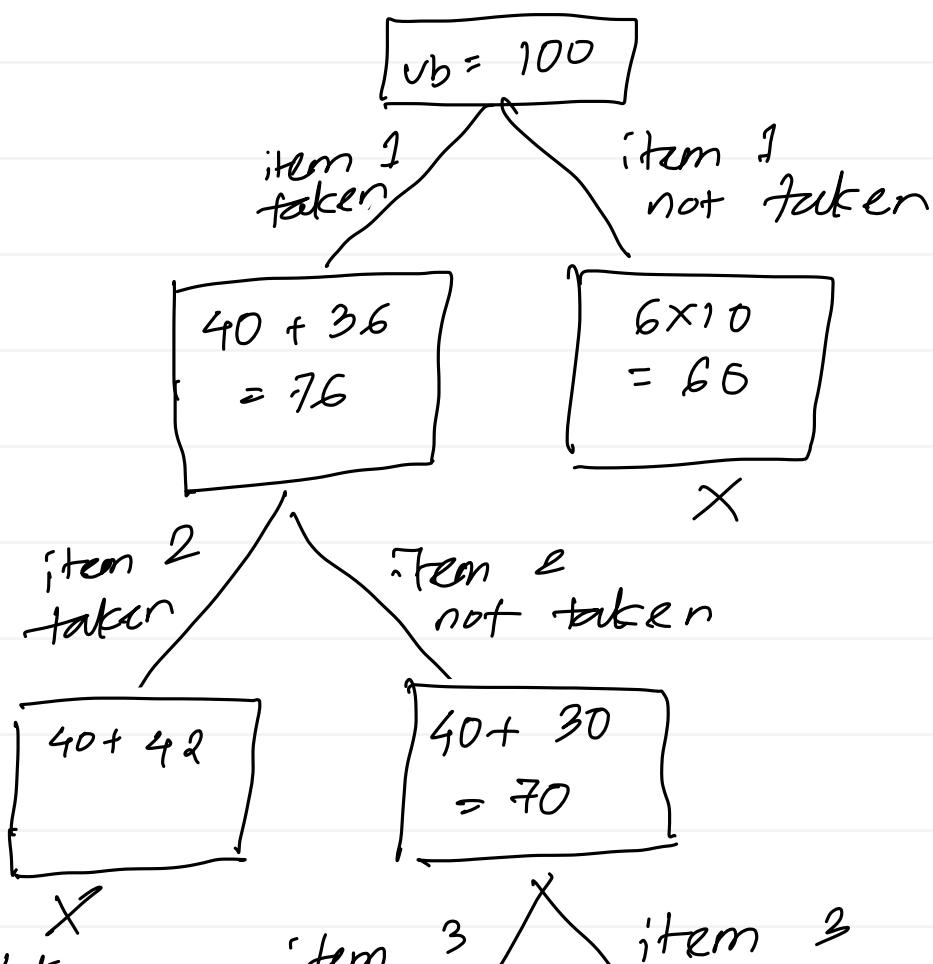
$$\text{maximum per unit value} \times \text{capacity} = \text{upper bound}$$

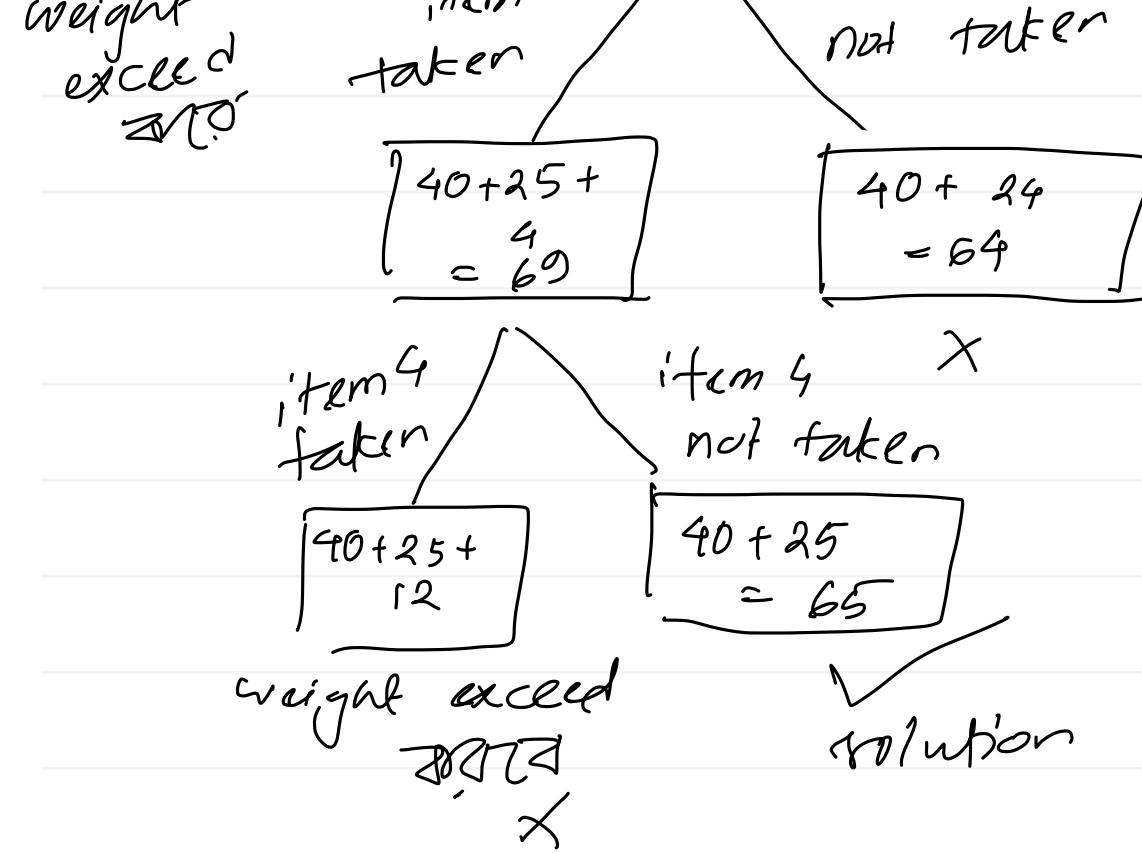
কাটো choose রয়েছে upper bound:

$$\text{Already taken} + \text{Remaining capacity} \times \frac{\text{max per unit value remaining}}{\text{unit value}}$$

$$ub = v + (w-w) \times \frac{v_i}{w_i} (\text{max.})$$

$$\text{initially } v=0 \quad w=0$$





\* ② for node  $\geq$  value, upper bound and weight ৰাখিব, আবাবে just upper bound  
বি- ক্ষেত্ৰে,

## ONLINE ALGORITHMS

- offline algorithm  $\Rightarrow$  we have all the data.
- online algorithm  $\Rightarrow$  we only have knowledge about the past, then we have to deal with the future.
- we measure the performance of an online algorithm using competitive ratio.

competitive ratio,  $CR(A) = \max_i \frac{A(i)}{OPT(i)}$

$\rightarrow$  ratio of what the online algorithm 'pays' to what the optimal offline algorithm 'pays'

## SKI-RENTAL PROBLEM

- we don't know how many days we are going to ski for.

per day rent : 500 tk

one time buying cost : 1500 tk

optimal offline  $\Rightarrow$  we know ~~number of days~~, then we can take the decision accordingly. but here, we don't have that knowledge.

• online  $\Rightarrow$  there could be a few different approaches:

① keep renting

② buy  $\Rightarrow$

③ buy after rent, then buy on 3rd day

①  $\Rightarrow$

$$CR = \max \left( \frac{500}{500}, \frac{1000}{1000}, \frac{1500}{1500}, \frac{2000}{1500}, \frac{2500}{1500}, \dots \right)$$

$$= \infty$$

②  $\Rightarrow$

$$CR = \max \left( \frac{1500}{500}, \frac{1500}{1000}, \frac{1500}{1500}, \frac{1500}{1500}, \dots \right)$$

$$= 3$$

$$\textcircled{3} \Rightarrow CR = \max \left( \frac{500}{500}, \frac{1000}{1000}, \frac{2500}{1500}, \frac{2500}{1500}, \dots \right)$$

$$= 1.67$$

• Another problem: এই problem এর optimal solution কখনও আসে না।

# Linked List Search



Center element for binary search problem  
we will shift it 2 places left  
by bring it closer so that if I request  
the same item repeatedly, I will get it  
faster each time.

Let, I am requesting nth item each from .

$$\therefore n + (n-2) + (n-4) + \dots + \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases} \approx an^2$$

*(something constant)*

General term:  $(n - 2k)$

Optimal solution:

ମର୍ବାର ସ୍କ୍ରିପ୍ଟ ପଢ଼୍‌ଥାର ଏବଂ ତାହା ମର୍ବାର  
ମାଧ୍ୟମରେ ଲିଖିଯା ରହିଥାଏ because we  
already know the entire search  
sequence.

$$\therefore n+1+1+\dots+1 = 2n-1$$

after we can find a competitive ratio

$$\text{Here} \cdot \quad = \quad \frac{an^2}{2n-1} \quad \approx \quad \frac{n}{2}$$

However, if there is a random search sequence 1, 3, 2, 235, 5. ↗<sup>2</sup> ~~235~~ we don't know the optimal solution. [Adversary situation]

However, there is a claim:

• for move to front strategy, CR is 2.

Another claim:

There is no strategy for which CR is less than 2.

Many variations:

- ① next element hit ~~ব্যাক~~ এখন bring it to 1st position
- ② last position
- ③ middle position

We are trying to find a worst case scenario. Adversary situation/ worst case  $\Leftrightarrow$  next search element is always the last element of the linked list after each turn/ modification.

Adversary sequence,  $\sigma = x_1, x_2, \dots, x_n$

• अगमार तरीके sequence द्वाटेर all possible permutations find out करोगा तो.

$O_1 \rightarrow$  cost of finding every element in permutation  $\pi_1 (\pi_1)$

$$\pi_1 \rightarrow \left( \begin{smallmatrix} x_1 \\ c_{1,1} \end{smallmatrix} \right) \left( \begin{smallmatrix} x_2 \\ c_{1,2} \end{smallmatrix} \right) ( ) \dots$$

$$\text{Average cost} = \frac{(O_1 + O_2 + \dots + O_t)}{t}$$

[ $t$  त्रिप्रा permutation]

•  $x_k$  तरीके नुमार्क्स in all possible permutations i.e., all possible positions तरीके,

i.e. cost of finding :

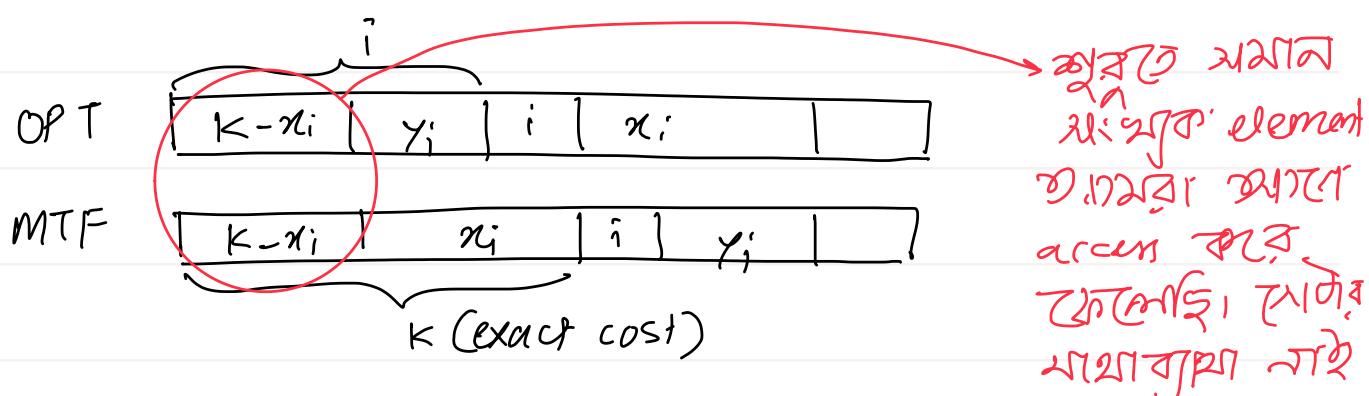
13.01.2025

Q) Let us compare OPT (Optimal) and MTF (move to front).

We assume that the optimal provides better results since it is optimal.

Sequence: 1, 2, 3, ... n

At step  $j$ , cost of MTF is  $k$ , OPT is  $i$ .



Amortized cost:  $\rightarrow$  Chap 17 of CLRS

$$T(j) = k + \text{INV}(j+1) - \text{INV}(j)$$

$\downarrow$   
exact cost +  $\hat{\text{cost}}$  operation টালালার অসরা

পরে sequence ক ক্ষেত্রে changes আবাহন দাওয়া  
cost

$$= k + (k - x_i + y_i - \alpha) - (x_i + y_i); \alpha = i \text{ খালি } \\ \text{পুরিমান ক্ষেত্র}$$

$$= 2k - 2x_i - \alpha \leq 2k - 2x_i$$

$$\leq r_i$$

(ক্ষেত্র রাখ ফিল্ট পথ  $\leq$ )

$\therefore$  At most 2;

Optimal এবং  $O$  at most 1. So, optimal  
এবং শুধুমাত্র,

[প্রতি step এ at most double]

Then extend করে যাবে তা overall এক-  
cost at most double.

HW:

Step  $j+1$  এর execution এর পর sketch  
বর্ণনা,

- Now, we will prove that there is no strategy whose CR is less than  $2 - \frac{2}{n+1}$

Adversary situation: sequence এ always  
new list এর last item choose ব্যবহার  
করে

$$\text{Adversary cost} = n + n + \dots + n$$

$$= nm \quad (\text{If no. of requests is } m \text{ and size of set is } n)$$

Optimal algorithm  $\Rightarrow$  imagine  $\exists$  an algorithm that knows the adversary sequence but we don't know the details of the algorithm.

We will make all possible permutations of my set. At least one will match the search sequence and it will give me the minimum cost. The minimum cost is obviously smaller than the average cost of all possible sequences.

$\therefore$  Upper bound of minimum cost  $\rightarrow$  average cost

$$\pi_1 = 1 \ 2 \ 3 \ \dots \ n$$

:

=

$$\pi_t$$

average

In all permutations, cost of finding 1st element be  $C(i_{1,1})$

$$= (n-1)! (1+2+3+\dots+n)$$

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

For finding  $m$  items,

$$\text{average cost} = \frac{m(n+1)}{2}$$

This is the upper bound of minimum cost.

$$\therefore \text{Competitive ratio} = \frac{\cancel{m n t}}{\cancel{m}(n+1)} \cdot \frac{2}{2}$$

$$= \frac{2n}{n+1}$$

$$= \frac{2n+2 - 2}{n+1}$$

$$= 2 - \frac{2}{n+1}$$

[Proved]

20/01/2025

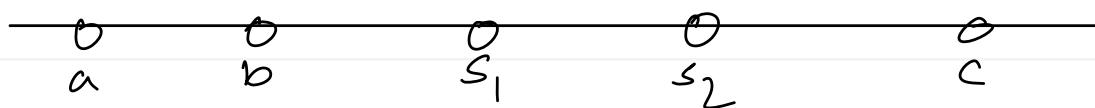
• Online algorithms are somewhat related to page replacement algorithm of OS.

• amortized analysis ഫർ അമ്മൈറ്റ് നാൻ ഇരുന്ത്  
potential method.

22/01/2025

## K-Server Problem

Let, there is a single road city, road 2327897 has houses, office etc. There is a company which provides internet service in this city. It deploys some vehicles/servers which solves connection problems.



$a, b, c \rightarrow$  client

$s_1, s_2 \rightarrow$  server

- Cost is proportional to how much road a server traverses.
- We want to reduce the overall cost.

### Greedy Approach

But competitive ratio is infinite.

Let's request sequence:

caba bab...

গুরুত্বে  $s_1, s_2$  constantly move রাখিয়ে and  
every step এ cost রাখিয়ে রাখিয়ে,

However, if we knew the entire  
sequence, গুরুত্বে a টি রাখিয়ে রাখিয়ে,  
গুরুত্বে b টি রাখিয়ে রাখিয়ে, গুরুত্বে  
lost আবি' রাখিয়েনা.

copy this from  
mukun

Another approach:

def, there are two service stations. Request  
মানুষ দুটির ফিল্ডের মধ্যে আন্তর, DRAM  
পদ্ধতিকে treat করা, and মানুষ দুটির  
বাইরের পথের আন্তর, then DRAMকে treat  
করা।

2nd class copy from mehenn

DR algorithm's competitive ratio is constant.

Double Coverage:

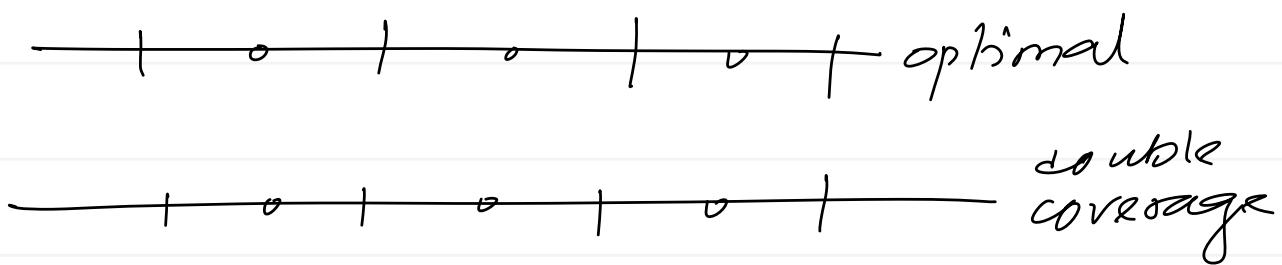
- if the request falls outside the convex hull of the server, score it with the nearest server. Otherwise, the request is in between two adjacent servers. In this case, move both these servers towards the request at equal speed until one server reaches it.

We will follow interleaving moving style.

Total cost of double coverage algorithm,

$$\sum_{DC} = \sum_{i \leq j} d(s_i, s_j)$$

↓  
ব্যুৎপন্ন pair of station এর  
distance এর sum হচ্ছে double  
coverage.



বিধির algorithm এর matching কর্তৃত minimum  
difference টাকি কোটি be  $M_{min}$ .

