IT-216 - Design and analysis of algorithms

$x \leftarrow$ n digits no.
$y \leftarrow$ n " no.

multiply x and y.

x * y

5 × 6 = 30

25 × 11 = 275

5 6 7 8 9 1 0 2
× 1 2 3 5 6 9

$x = 5\ 6\ 7\ 8$

$y = x\ 1\ 2\ 3\ y$

3

3

2

$2\ 2\ 7\ 1\ 2$

$1\ 7\ 0\ 3\ 4\ x$

$1\ 1\ 3\ 5\ 6\ x\ x$

$5\ 6\ 7\ 8\ x\ x\ x$

$7\ 0\ 0\ 6\ 6\ 5\ 2$

Q: How many Premitive operations are there?

sigle digit multiplication and addition are allowed.

Each row takes $\rightarrow 2n$ } total n rows takes $- 2n^2$

rows $- n$

Adding two rows takes $\rightarrow 2n$ operations.

Adding n rows takes $\rightarrow (n-1) \cdot 2n \cdot \leq 2n^2$

Total operations $\rightarrow 2n^2 + 2n^2 \leq 4n^2$

$\rightarrow$ constant $* n^2$

Algorithm designer's mantra

can we do better?

$x = a\,5\,6\,7\,8\,b$

$y = 1\,2\,3\,4$

$c \quad d$

step 1: compute ac ← $T(n/2)$

step 2: compute $b \cdot d$ ← $T(n/2)$ $2 \cdot n/2$

step 3: compute $(a+b)\cdot(c+d)$ ← $2 \cdot (2\frac{n}{2}) + T(n/2)$

step 4: compute step 3 − step 1 − step 2 ← constant · n

step 5: 10^4 step 1 $+ 10^2$ step 4 + step 2 ← constant · n.

Ans 7006652 (H.W)

$T(n)$ ← total number of operations to multiply two n digits number.

overall time:

$T(n) = 3T(n/2) + O(n^2)$

constant * n

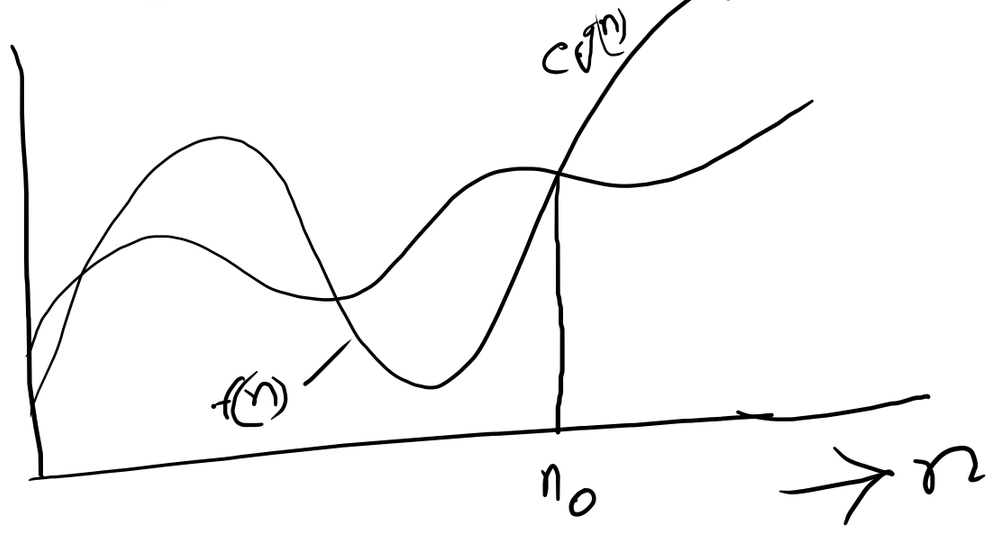
less than $2n^2$

Asymptotic notations

Big 'O' notation (upper bound)

Question When is $f(n) = O(g(n))$?

$f(n) = O(g(n))$ if there exists constants $c > 0$, $n_0 > 0$ such that $0 \leq f(n) \leq c\,g(n)$ for all $n \geq n_0$



$$x = 10^{n/2} a + b$$

$$y = 10^{n/2} c + d$$

$$x \cdot y = (10^{n/2} a + b)(10^{n/2} c + d)$$

$$= 10^{n} ac + 10^{n/2}(ad + bc) + bd$$

$$(a+b)(c+d) - ac - bd$$

Exm

$2n^2 = O(n^3)$

$c = 1$
$n_0 = 1$

$0 \le f(n) \le c\, g(n) \quad \forall\, n \ge n_0$

$2n_0^2 \le 1 \cdot n_0^3$

$2 \le 1$ ✗

$c = 1$
$n_0 = 2$

$2n^2 = O(n^3)$

$2n_0^2 \le 1\, n_0^3$

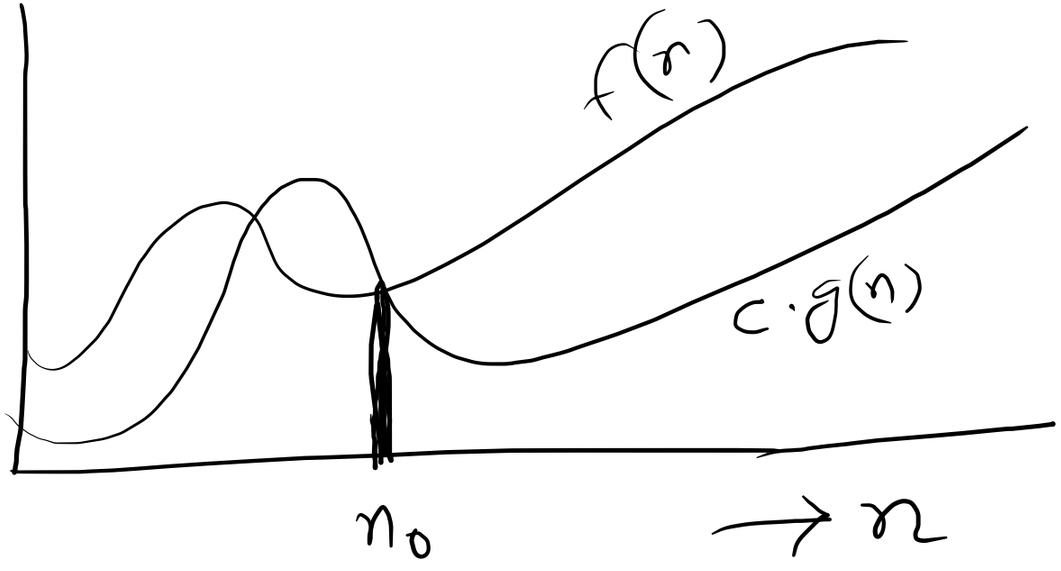
$2 \cdot 2^2 \le 1 \cdot 2^3$

$8 \le 8$ ✓

Big omega (Ω) notation

lower bound.

- $f(n) = \Omega(g(n))$ if there exists constants $c > 0, n_0 > 0$ such that $0 \leq c \cdot g(n) \leq f(n)$ $\forall$ $n \geq n_0$



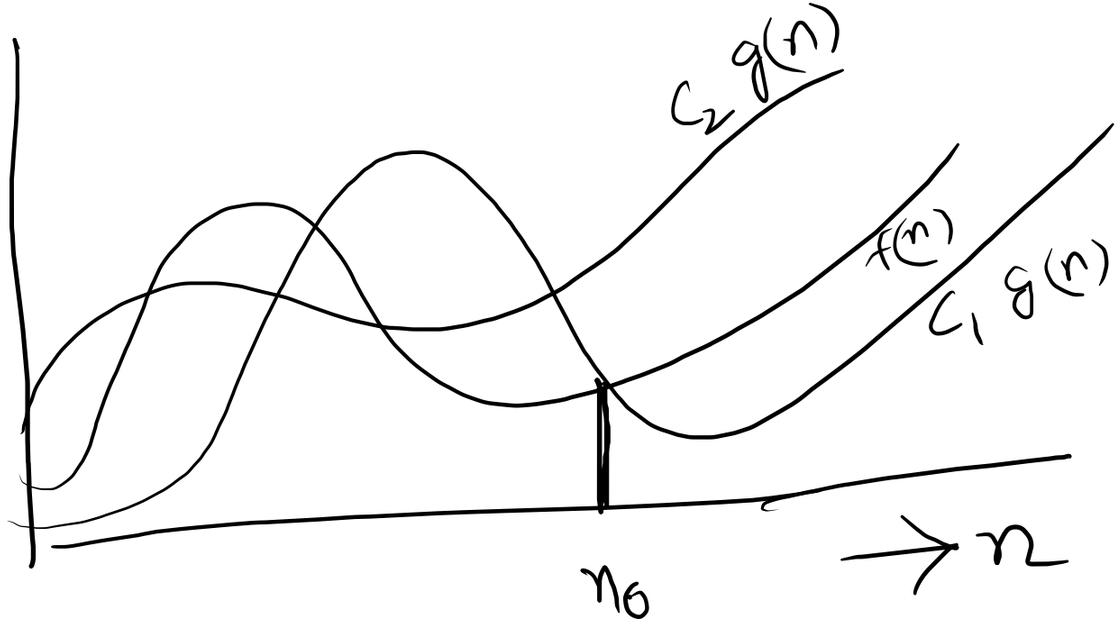
Ex n $5n^2 + 3n = \Omega(n^2)$

Theta notation

Tight bound

$f(n) = \theta(g(n))$ if $\exists$ constants $c_1 > 0, c_2 > 0, n_0 > 0$ such that

$$0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n) \quad \forall n \geq n_0$$



Ex: $3n + 2 = \theta(n)$

small 'o' and small ω.

$$f(n) = o(g(n))$$

$$0 \leq f(n) < c\, g(n)$$

$$f(n) = \omega(g(n))$$

$$0 \leq c\, g(n) < f(n)$$

$T(n) = 3T(\frac{n}{2}) + constant*n$ called recurrence equations.

Solving recurrences

- A recurrence is an equation or inequality that describes a function in terms of its value on smaller inputs.

- Analyse the running time of divide and conquer algorithm.

Methods to solve recurrences

1. Substitution method
2. Recursion tree method
3. The master method

Substitution method

This is the most general method

1. Guess the form of the solution
2. verify it by induction
3. Solve some constants.

Ex^m $T(n) = 4T(\frac{n}{2}) + n$

[Assume $T(1) =$ constant $\theta(1)$]

- Guess $O(n^3)$
- Assume that $T(k) \leq ck^3$ for $k < n$

we need to prove, $T(n) \leq cn^3$ by induction.

$$T(n) = 4T(\tfrac{n}{2}) + n$$
$$\leq 4 \cdot c \cdot (\tfrac{n}{2})^3 + n$$
$$= \tfrac{c}{2} n^3 + n$$
$$= cn^3 - \left[\tfrac{c}{2} n^3 - n\right]$$

cn^3: required, derived. $\left[\tfrac{c}{2} n^3 - n\right]$: residual.

$T(n) \leq cn^3$ whenever $\frac{c}{2} n^3 - n > 0$

this is true when $c \geq 2$, $n \geq 1$

So $T(n) = O(n^3)$

Guess: $O(n^2)$

I.H. $T(K) \le cK^2$ for $K < n$

$$T(n) = 4T(\tfrac{n}{2}) + n$$
$$\le 4 \cdot c \cdot (\tfrac{n}{2})^2 + n$$
$$= cn^2 + n$$
$$= cn^2 - [-n]$$

required — residual

H.W. Try solving examples

Strengthen

I.H. $T(K) \le c_1K^2 - c_2K$ for $K < n$

$$T(n) = 4T(\tfrac{n}{2}) + n$$
$$\le 4 \cdot c_1(\tfrac{n}{2})^2 - 4c_2\tfrac{n}{2} + n$$
$$= c_1n^2 - c_2n - [c_2n - n]$$

desired — required

$T(n) \le c_1n^2 - c_2n$ whenever $c_2n - n \ge 0$

$\Rightarrow c_2 \ge 1$

$T(n) = O(c_1n^2 - c_2n)$

$= O(n^2)$

Recursion tree method

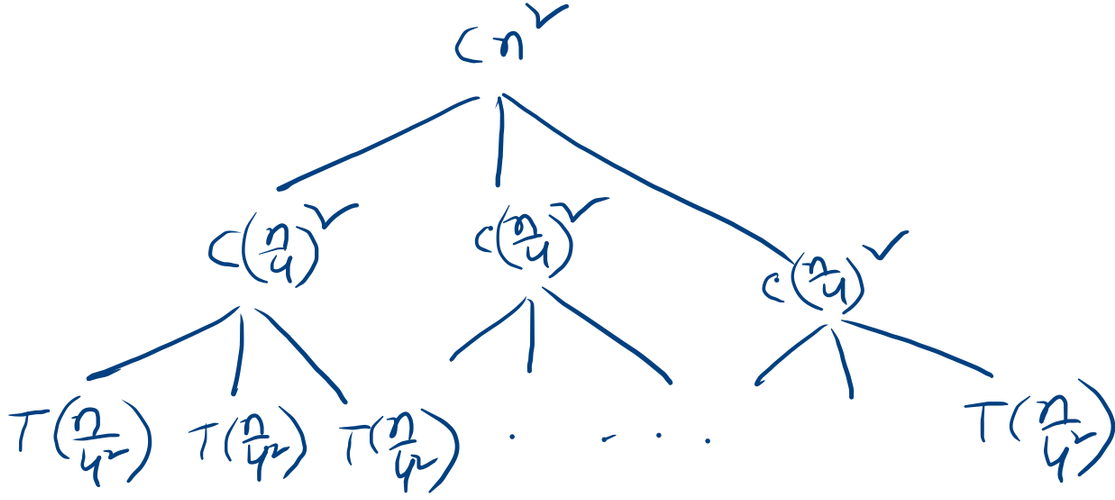
- A recursion tree models the cost (time) of a recursive execution of an algorithm.
- It is an intution of the running time of an algorithm
- It can be use as a guess for substitution method.

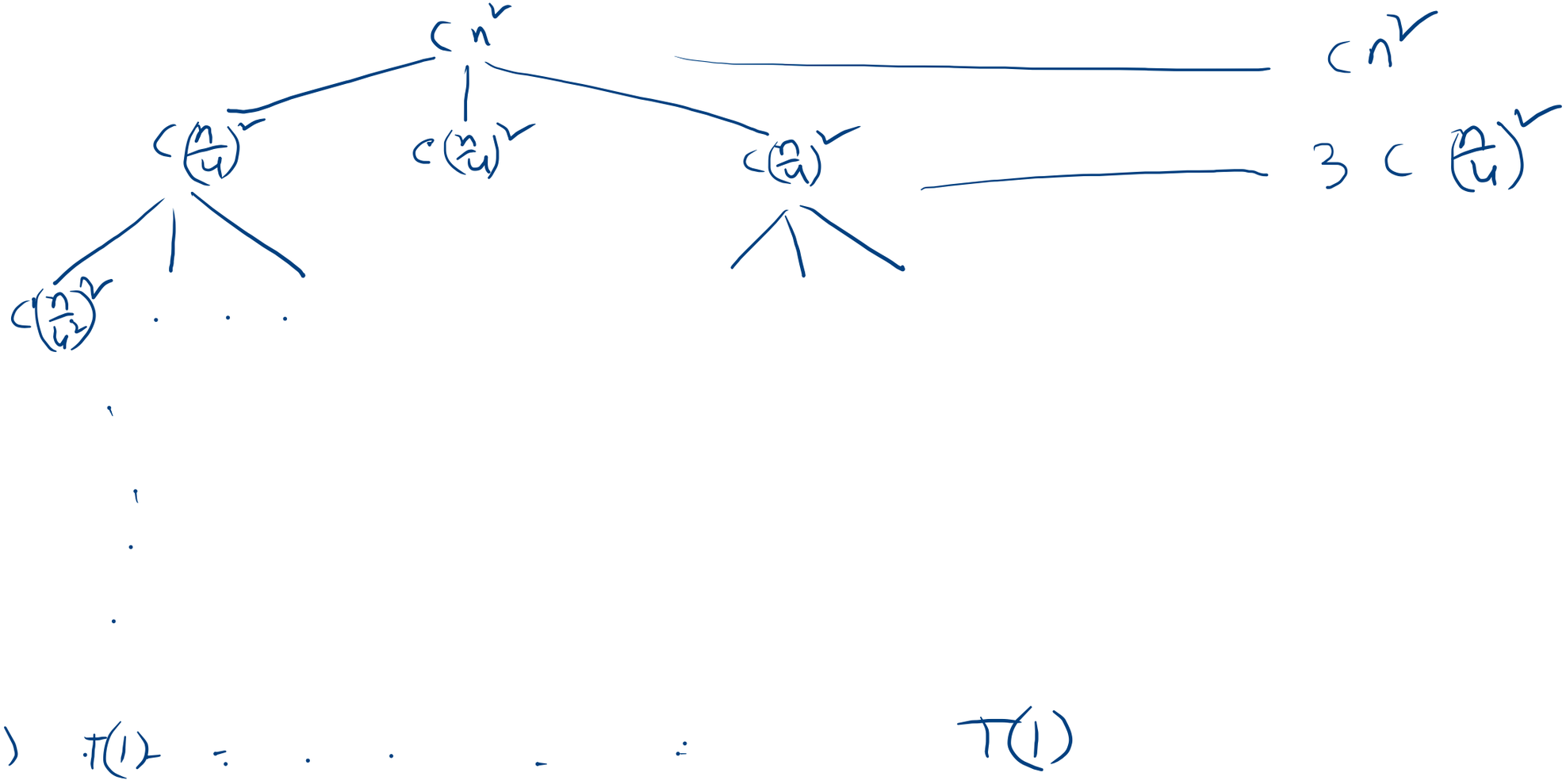
Guess the solution using recursion tree method.

$$T(n) = 3T\left(\frac{n}{4}\right) + \Theta(n^2)$$

$$\equiv \quad T(n) = 3T\left(\frac{n}{4}\right) + cn^2 \quad \text{for some constant } c.$$

$T(n)$ •




cn^2
cn^2
$c(\frac{n}{4})^2$
$c(\frac{n}{4})^2$
$c(\frac{n}{4})^2$
$3c(\frac{n}{4})^2$
$c(\frac{n}{16})^2$
T(1) T(1) T(1)

cost at i-th depth

nodes in i-th depth $\rightarrow 3^i$

cost of each node at depth i $\rightarrow c \cdot \left(\frac{n}{4^i}\right)^2$

cost at depth i $\Rightarrow 3^i \cdot c \cdot \left(\frac{n}{4^i}\right)^2 = \left(\frac{3}{16}\right)^i c\, n^2$

Height Let i be the height

$$\frac{n}{4^i} = 1 \Rightarrow i = \log_4 n$$

cost at last level $\rightarrow 3^{\log_4 n} \cdot T(1)$

Total cost of the tree.

$$T(n) = \sum_{i=0}^{\log_4 n - 1} \left(\frac{3}{16}\right)^i c n^2 + 3^{\log_4 n}$$

$$\leq \sum_{i=0}^{\infty} \left(\frac{3}{16}\right)^i c n^2 + n^{\log_4 3}$$

$$= \frac{1}{1 - \frac{3}{16}} c n^2 + n^{\log_4 3}$$

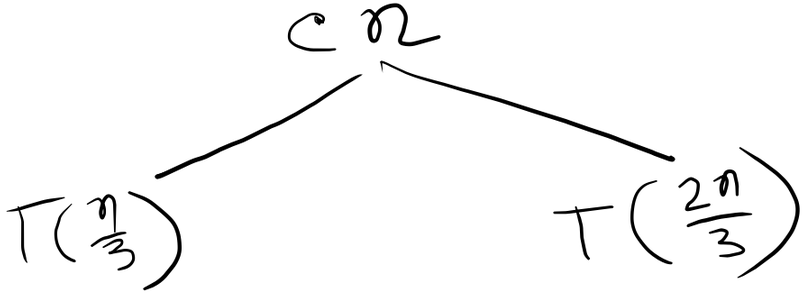
$$= O(n^2)$$

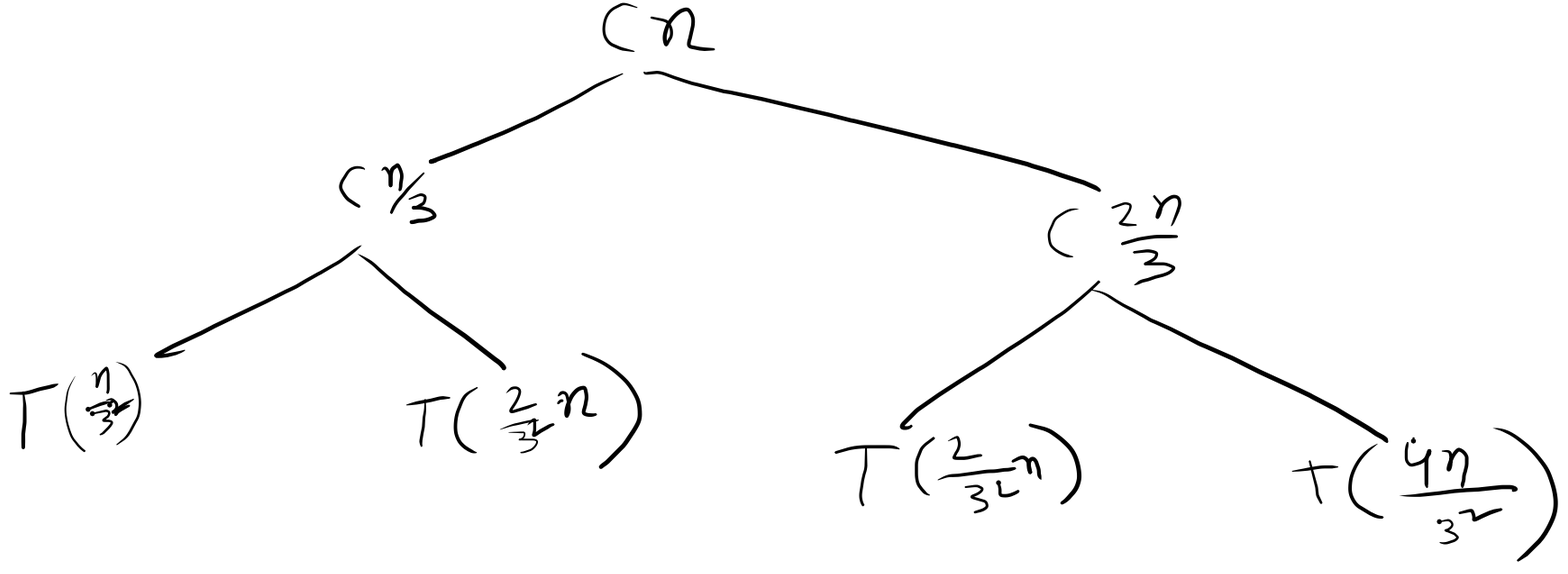
Recursion tree method

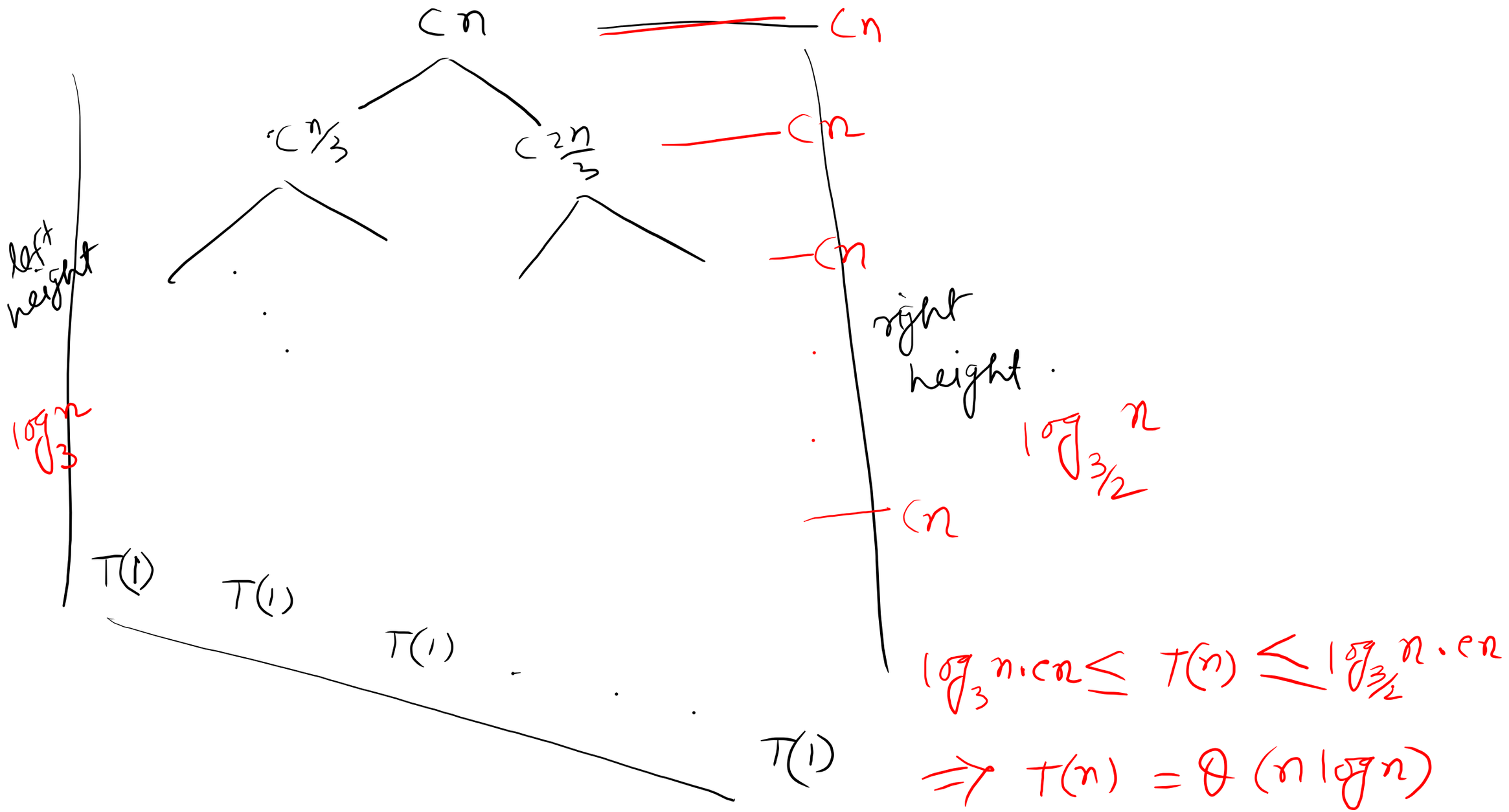
Ex^n $T(n) = T(\frac{n}{3}) + T(\frac{2n}{3}) + cn$

Find $T(n)$ using recursion tree.

$T(n)$







$\log_3 n \cdot cn \leq T(n) \leq \log_{3/2} n \cdot cn$

$\Rightarrow T(n) = \Theta(n \log n)$

The master method

This method applies to the recurrences of the form

$$T(n) = a\,T\left(\frac{n}{b}\right) + f(n)$$

$a \geq 1$, $b > 1$ and f is asymptotically positive

Three common cases based on comparing $f(n)$ and $n^{\log_b a}$

case 1: $f(n) = O\left(n^{\log_b a - \epsilon}\right)$ for $\epsilon > 0$

$f(n)$ grows polynomially slower than $n^{\log_b a}$ by a factor n^{ϵ}

solution: $T(n) = \theta\left(n^{\log_b a}\right)$

case 2 $f(n) = \theta\left(n^{\log_b a} \lg^k n\right)$

Solution: $T(n) = \theta\left(n^{\log_b a} \cdot \lg^{k+1} n\right)$

case 3: $f(n) = \Omega\left(n^{\log_b a + \epsilon}\right)$

Addition condition

$af\left(\frac{n}{b}\right) \leq cf(n)$ for some $c < 1$

regularity condition

Solution: $T(n) = \theta\left(f(n)\right)$

Exm i) $T(n) = 4T(\frac{n}{2}) + n$

$a = 4, \quad b = 2, \quad n^{\log_b a} = n^{\log_2 4} = n^2$

$f(n) = n$

$f(n) = O(n^{2-1}) = O(n^{\log_b a - 1})$

case 1 of master method applies here

solution is $T(n) = \theta(n^2)$

ii) $T(n) = 4T\left(\frac{n}{2}\right) + n^2$

$$T(n) = \theta(n^2 \lg n)$$

iii) $T(n) = 4T\left(\frac{n}{2}\right) + n^3$

$$n^3 = \Omega\left(n^{2+1}\right)$$

$af\left(\frac{n}{b}\right) \leq cf(n)$ for some $c < 1$

$$4\left(\frac{n}{2}\right)^3 \leq c \cdot n^3$$

$$\frac{n^3}{2} \leq cn^3 \qquad c \geq \frac{1}{2}$$

any value of c where, $.5 \leq c < 1$ satisfies regularity condition

solution $T(n) = \theta(n^3)$

iv) $T(n) = 4T(\frac{n}{2}) + \frac{n^2}{\lg n}$

$f(n) = \frac{n^2}{\lg n}$ $\qquad$ $n^{\log_b a} = n^2$

Master method cannot applied here ✗

$f(n) = n^2$ → upper bound

$f(n) = n$ ⇒ lower bound.

> your solution lies between these values.

H/W. Try examples

Algorithm design techniques

Divide and conquer paradigm

1. Divide the problem (instance) into subproblems.
2. Conquer recursively solving the subproblems.
3. Combine the solutions of the subproblems.

Ex^n Binary search problem

Defn: Given an array of n sorted numbers and an number K verify whether K is in the array or not.

simple algorithm:

Traverse the array one by one and compare each element

running time:- O(n)

can we do better?

Divide : check for the middle element

conquer : Recursively search one subarray

combine : Trivial.

```
BinarySearch (A, K, low, high)                    — T(n)
 if low > high                                    — θ(1)
      return no                                   — θ(1)
 else mid = ⌊(low + high)/2⌋                      — θ(1)
      if K == A[mid]                              — θ(1)
           return yes                             — θ(1)
      else if K > A[mid]                          — θ(1)
           BinarySearch (A, K, mid+1, high)       — T(n/2)
      else                                        — θ(1)
           Binarysearch (A, K, low, mid-1)        — T(n/2)
return no                                         — θ(1)
```

total time

$T(n) = T(\frac{n}{2}) + \theta(1)$

master method

$T(n) = \theta(\lg n)$

class code: hljk4tm

Integer multiplication

Primary school algorithm takes $O(n^2)$ time

Karatsuba algorithm

```
karatsuba(x, y)                                          ——— T(n)
 if (n == 1)                                             ——— θ(1)
     return x * y                                        ——— θ(1)
 else                                                    ——— θ(1)
     a, b = first and second half of x                   ——— O(n)
     c, d = "    "    "    "    "  of y                  ——— O(n)
     compute p = a + b                                   ——— O(n)
     "       q = c + d                                   ——— O(n)
     ac = karatsuba(a, c)                                ——— T(n/2)
     bd = karatsuba(b, d)                                ——— T(n/2)
     pq = karatsuba(p, q)                                ——— T(n/2)
     adbc = pq - ac - bd                                 ——— O(n)
     return 10^n ac + 10^(n/2) adbc + bd                 ——— O(n)
```

overall

$T(n) = 3T(\frac{n}{2}) + cn$

$T(n) = \theta(n^{\log_2 3})$

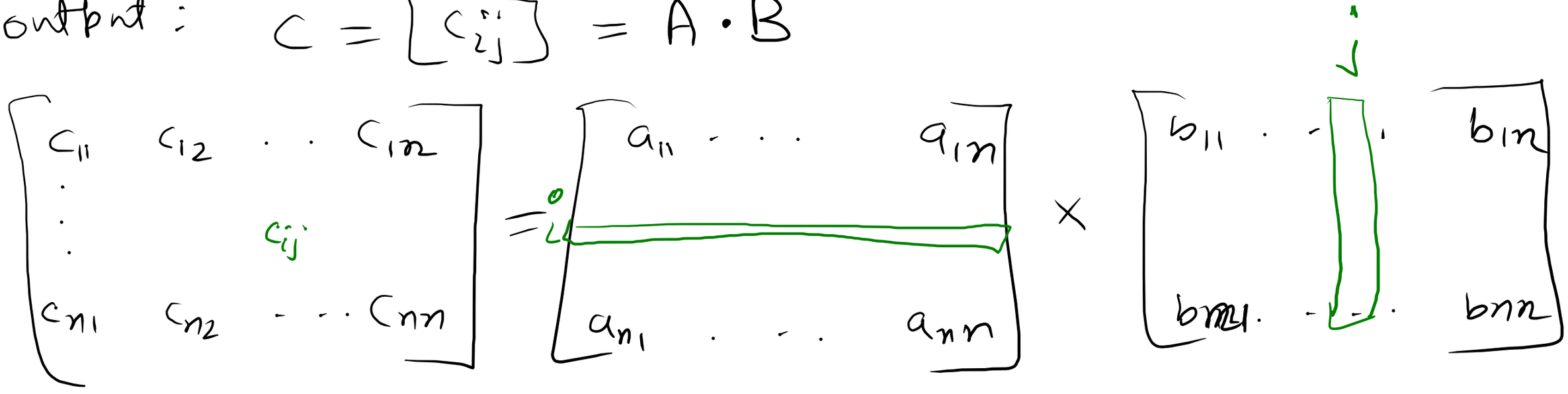
$\log_2 3 \approx 1.59$

$T(n) = \theta(n^{1.59})$

matrix multiplication

Input: $A = [a_{ij}]$, $B = [b_{ij}]$

output : $C = [c_{ij}] = A \cdot B$



$$c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{in} b_{nj}$$

$$= \sum_{k=1}^{n} a_{ik} b_{kj}$$

```
mat-mul (A, B)
 for i = 1 to n
      for j = 1 to n
           c_ij = 0
           for k = 1 to n
                c_ij = c_ij + a_ik · b_kj

 return C
```

Time: $O(n^3)$

can we do better?

Divide and conquer

$$C = AB$$

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

$C_{11} = A_{11} B_{11} + A_{12} B_{21}$

C_{12}

C_{21}

C_{22}

```
mat_mul (A, B)
if (n == 1)
    c11 = a11 b11
else
    partition A into A11 A12 A21 A22
        "     B  "  B11 B12 B21 B22
    c11 = ————————
    c12 = ————————
    c21 = ————————
    c22 = ————————
    return C
```

Total time

$$T(n) = 8T\left(\frac{n}{2}\right) + O(n^2)$$

$$T(n) = O(n^3)$$

No improvement

Idea: need to reduce # of recursive multiplication.

Strassen's algorithm (1969) It uses 7 multiplications.

$$E_1 = A_{11}(B_{12} - B_{21})$$
$$E_2 = (A_{11} + A_{12})B_{22}$$
$$E_3 = (A_{21} + A_{22})B_{11}$$
$$E_4 = A_{22}(B_{21} - B_{11})$$
$$E_5 = (A_{11} + A_{12})(B_{11} + B_{22})$$
$$E_6 = (A_{12} - A_{22})(B_{21} + B_{22})$$
$$E_7 = (A_{11} - A_{21})(B_{11} + B_{12})$$

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} = \begin{bmatrix} E_5 + E_4 - E_2 + E_6 & E_1 + E_2 \\ E_3 + E_4 & E_5 + E_1 - E_3 - E_7 \end{bmatrix}$$

Total time:

$$T(n) = 7T\left(\frac{n}{2}\right) + O(n^2)$$

$$T(n) = O(n^{\log_2 7})$$

$$\approx O(n^{2.808})$$

Progress of the algorithm

$O(n^3)$ — standart

$O(n^{2.808})$ — Strassen 1969

$O(n^{2.796})$ — Pan (1978)

$O(n^{2.522})$ — Schonhage (1981)

$O(n^{2.517})$ — Romani (1982)

$O(n^{2.496})$ — Coppersmith and Winograd (1982)

$O(n^{2.479})$ — Strassen (1986)

$O(n^{2.376})$ — Coppersmith and Winograd (1989)

$O(n^{2.374})$ — Stothers (2010)

$O(n^{2.3728642})$ — V Williams (2011)

$O(n^{2.3728639})$ — Le Gall (2014)

.

.

.

Powering a number

Problem compute a^n where $n \in \mathbb{N}$

Algorithm: multiply a n times.

Time $O(n)$

can we do better?

Divide and conquer

$$a^n = \begin{cases} a^{n/2} \cdot a^{n/2} & \text{if } n \text{ is even} \\ a^{n/2} \cdot a^{n/2} \cdot a & \text{if } n \text{ is odd} \end{cases}$$

$T(n) = 2T(\frac{n}{2}) + \theta(1)$

$\theta(n)$

```
Power (a, n)
 if (n == 1)
      return a
 else
   tmp = Power(a, n/2)
    if n is even
         return tmp * tmp
    else
         return tmp * tmp * a
```

$$T(n) = T\left(\frac{n}{2}\right) + \theta(1)$$

$$T(n) = \theta(\lg n)$$

Ti

Greedy algorithm design paradigm

- It constructs a solution by considering one step at at a time
- At each step it chooses the locally best solution
- In some cases it constructs a globally best solution by repeatedly choosing the locally best option.

Advantages vs challenges

Advantages: Simplicity :- Easy to describe
Efficiency :- efficiently implemented

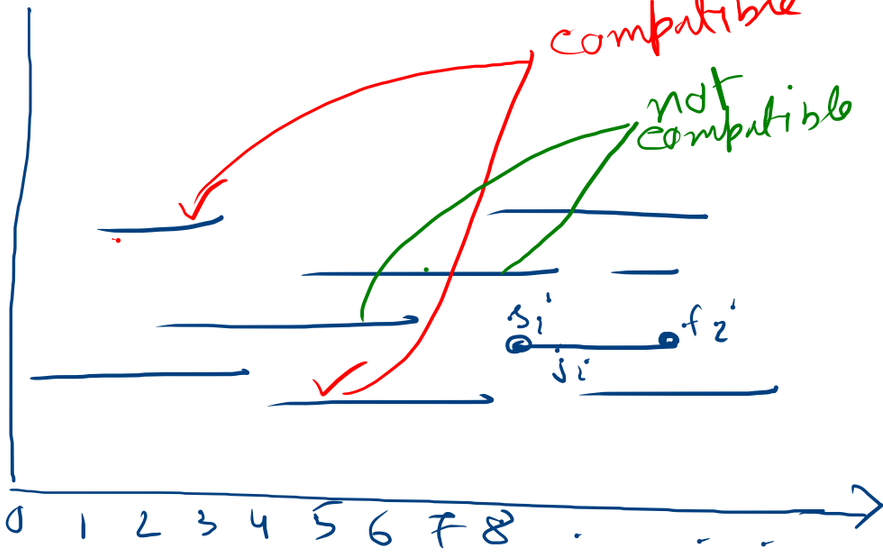
challenges: Hard to design: once you have the right greedy approach design greedy algorithm is easy.

Hard to verify: The correctness often requires critical arguments.

Activity selection Problem / interval scheduling problem
maximum independent set problem in intervals given on a line.

Input: n jobs $J = \{j_1, j_2, \ldots, j_n\}$

each job $j_i \in J$, start time s_i
finish time f_i



Feasible solution :-

Two jobs are **compatible** if they do not overlap.

Find a subset of jobs that are mutually compatible

objective: maximise the size of the mutually compatible set of jobs.

Pick the job which finishes earlier.

Greedy rule.

- Select jobs one after another using some rule

Rule 1 → Earliest start time

Rule 2 :- Smallest job first

Rule 3 :- Smallest conflict job first

Rule 4: Earliest finish time

Rule 1: not optimum

Rule 2:

H. W.

Rule 3:

H. W.

Rule 4: Earliest finish time

Greedy rule:

- Initially J be the set of jobs and A be an empty set
- While J is not empty
  - choose a job $j \in J$ that has the smallest finish time
  - Add j to A
  - Delete all jobs from J that are not compatible with j
- Return A

$O(n \log n + n)$

$= O(n \log n)$

correctness :-

claim: A is a feasible solution.

Proof straightforward.

claim: A is optimum

A ← set of jobs return by the algorithm

opt ← largest set of pairwise non-overlapping jobs.

what we have to prove?

A must be as large as opt

$$|A| = |opt|$$

$A = \{A_1, A_2, \ldots, A_K\}$
$Opt = \{O_1, O_2, \ldots, O_m\}$
} Assume A and Opt are sorted.

A = ——— ——— ——— ———

Opt = ——— ——— ——— ——— ———

Question: What is the relation between K & m

Answer: $K \leq m$

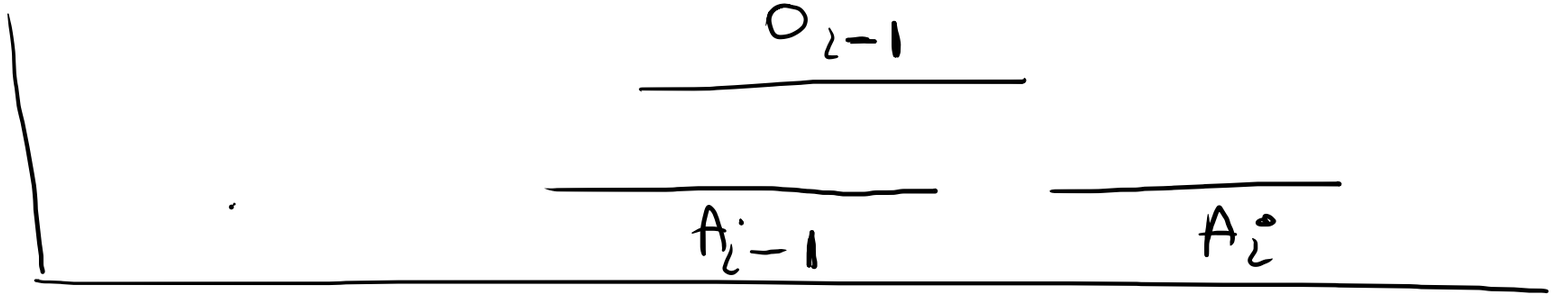
our aim :- ~~K~~ = m

claim for every $i \leq K$
A_i finishes not later than O_i

Proof prove using induction

Base case:- $i = 1$ it is true A_1 finishes not later than O_1

I.H: A_{i-1} finishes not later than O_{i-1}



If O_i finishes before A_i then it would overlap with A_{i-1} that means it overlap with O_{i-1}

$\Rightarrow \Leftarrow$

Main claim A is the optimum solution.

Proof we need to prove $k = m$.

If $k = m$ we are done.

Assume that $k < m$.

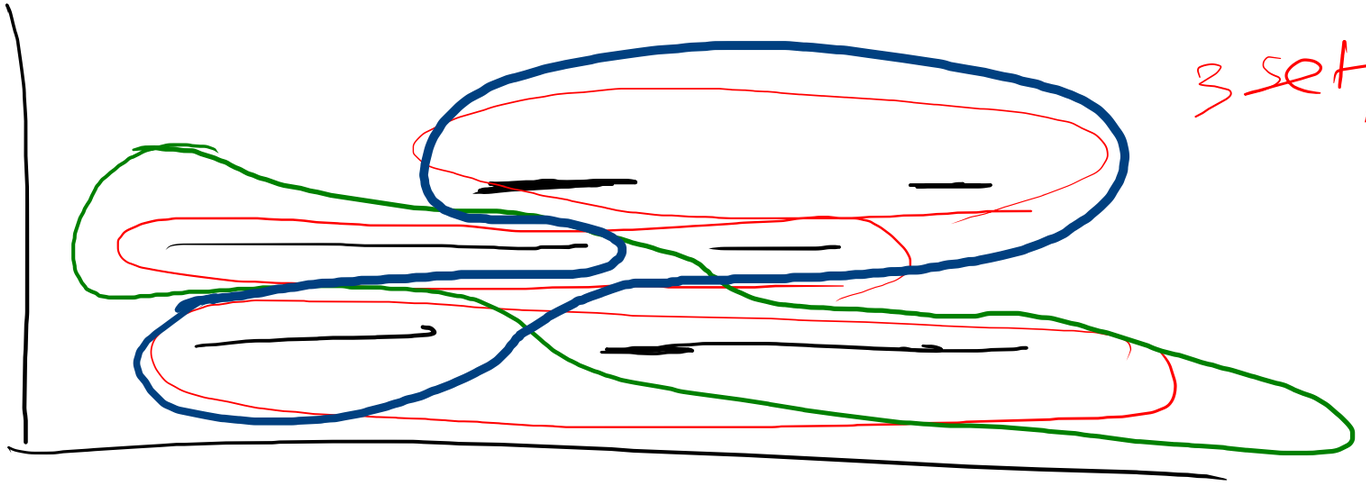
O_{k+1} starts after O_k and consequently A_k we could add O_{k+1} in A and obtain a bigger solution. $\Rightarrow\!\Leftarrow$

Interval partitioning problem

Input: A set of n jobs $J = \{J_1, J_2, \ldots, J_n\}$ where each job J_i has a start time s_i and a finish time f_i.

Output: A partition of the jobs in J into K sets such that each set of jobs are mutually compatible.

Objective: minimize K



3 sets $K=3$

green, blue } 2 sets $K=2$

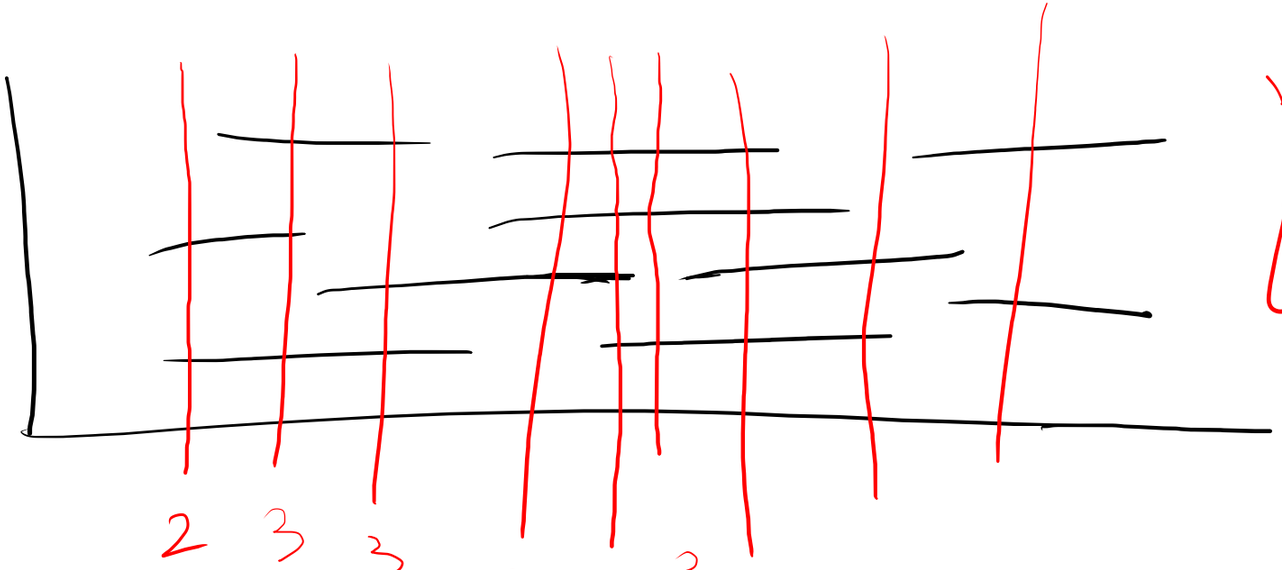
Situations where the problem appears

i) you have a set of fixed jobs and want to schedule them using minimum resources.

ii) There are a set of lectures that are schedule in some classrooms.
one wants to schedule the lectures using minimum classrooms.

Depth of a set of intervals

The maximum number of intervals that contain any given time



depth = 4

observation: Number of sets must be $K \geq$ depth

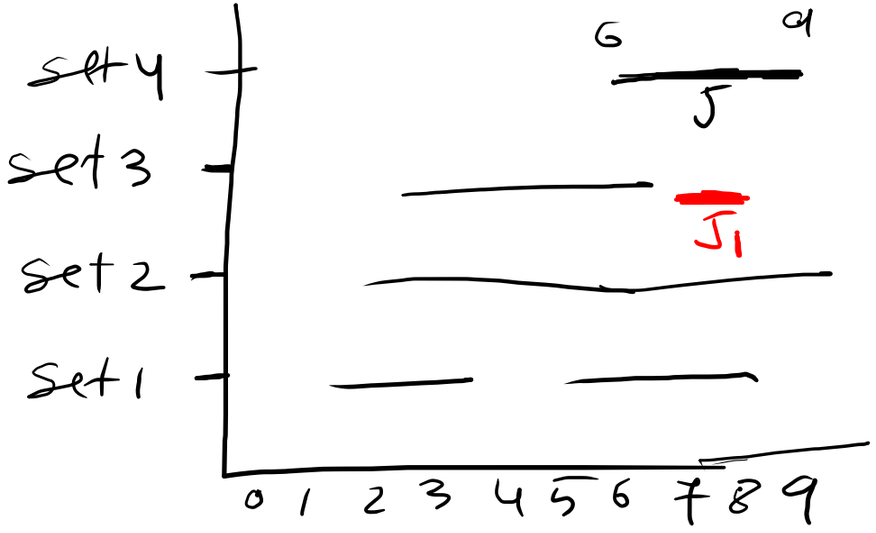
Question: What about K = depth ??

$\Rightarrow$ schedule is optimum.

Target: — Need a solution with depth number of sets.

We design greedy algorithm

- consider the jobs in some order — Which order?
- Assign each job to an available set — Which set?
  - If all the ~~sets~~ are not available then create a new set.



j → 6 — 9

J_1 → 7 - 8

rule 1 : Earliest finish time ✗

rule 2 : shortest interval first ✗

rule 3 : Fewest conflict ✗

rule 4 : Earliest start time. ✓

H.W. counter examples

Earliest start time

Input $(n, (s_1, f_1), (s_2, f_2), \ldots, (s_n, f_n))$

- Sort the jobs in increasing order of their start time. — $O(n \log n)$

$$s_1 \leq s_2 \leq s_3 \leq \cdots \leq s_n$$

- depth 0 — $\theta(1)$
- for $i = 1$ to n — $O(n)$ times
  - if J_i is compatible with some job in any set — $O(n)$
    - assign J_i in such set.

Priority queue $O(\log n)$

  - else
    - create a new set — $\theta(1)$
    - schedule J_i in depth+1 set
    - depth = depth + 1
- return the schedule.

Total time $O(n^2)$

improved $O(n \log n)$

correctness

claim: The algorithm never schedule two incompatible jobs in the same set.

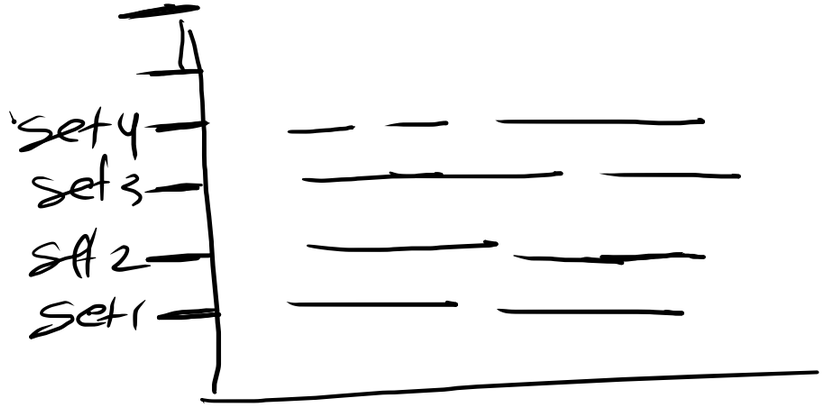
straightforward.

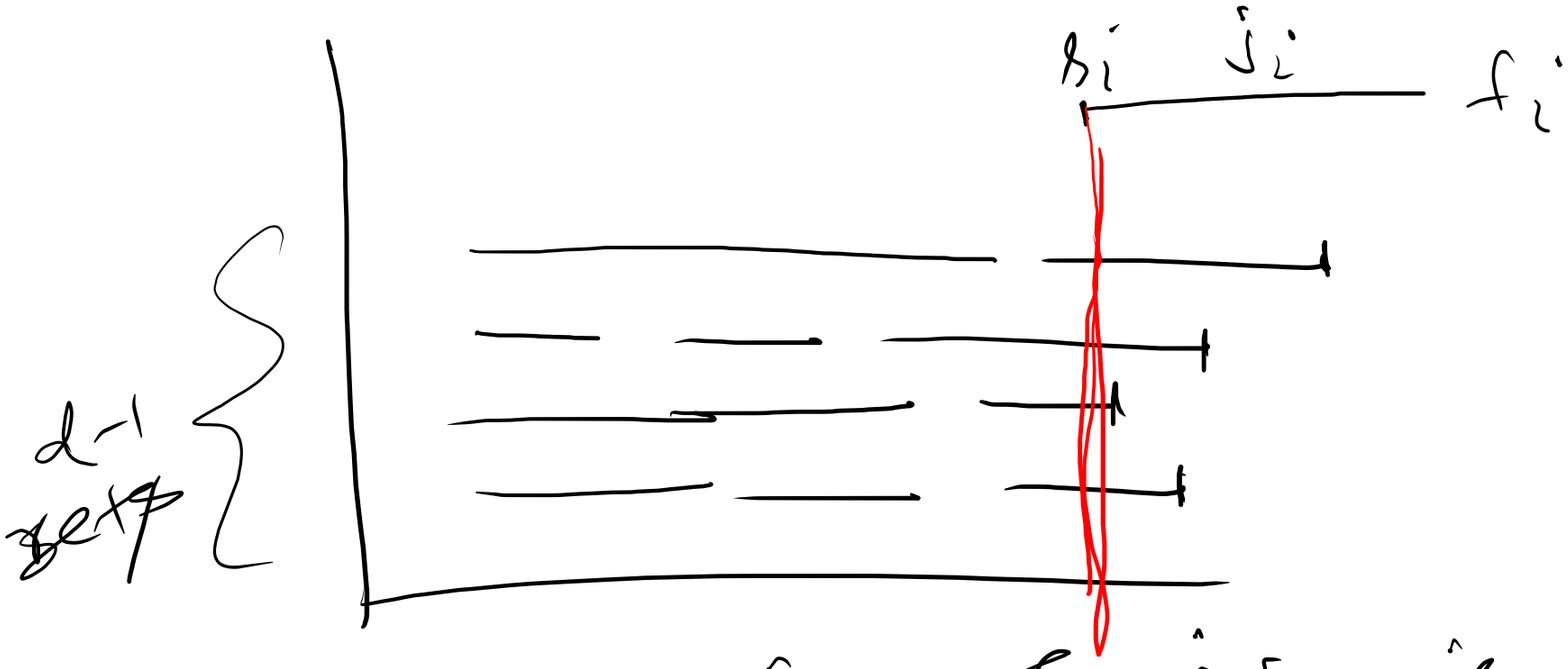
claim: The greedy algorithm is optimal.

Proof: Let d be the no. of sets the algorithm returns.

Question: When the last set ie, the d-th set first used?

The algorithm trying to add J_i^{th} job but it is incompatible with all other $d-1$ sets.





The start time of j_i is in between the start time and finish time of all the last jobs in d-1 sets.

Therefore the algorithm uses d sets only because of ther are d overlapping jobs ie, the depth of the problem is d.

Minimize the maximum lateness

Assume that there is only one processor

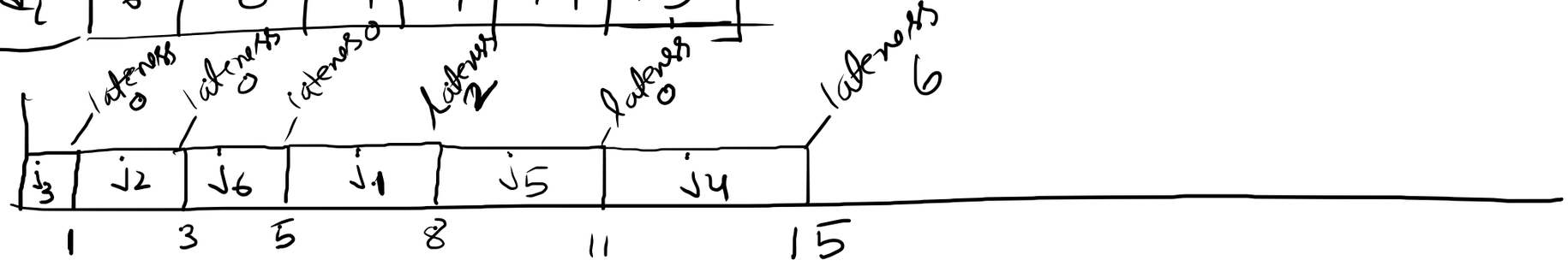
Input: A set J of n jobs $j_1, j_2, \ldots, j_n$ where each job j_i has a processing time t_i and a deadline d_i

output: Schedule the jobs in one processor such that the maximum amount time that any single job is past its deadline is minimized.

objective:

Exm

	j_1	j_2	j_3	j_4	j_5	j_6
t_i	3	2	1	4	3	2
d_i	6	8	9	9	14	15



$j_3 \rightarrow j_2 \rightarrow j_6 \rightarrow j_1 \rightarrow j_5 \rightarrow j_4$

objective: Find a schedule that minimizes the lateness

greedy template:

- consider the jobs in some order Which order ??
- Assign the jobs in this order to the resource.

rule 1: shortest processing time ✗ H.W: counterexample

rule 2: shortest slack time ✗

$d_i - t_i$

rule 3: Earliest deadline first ✓

Algorithm

Earliest deadline first $(n, (t_1, d_1), (t_2, d_2), \ldots, (t_n, d_n))$

- sort the jobs by their deadlines.
- $d_1 \leq d_2 \leq \cdots \leq d_n$ be the order
- $t = 0$
- for $i = 1$ to n

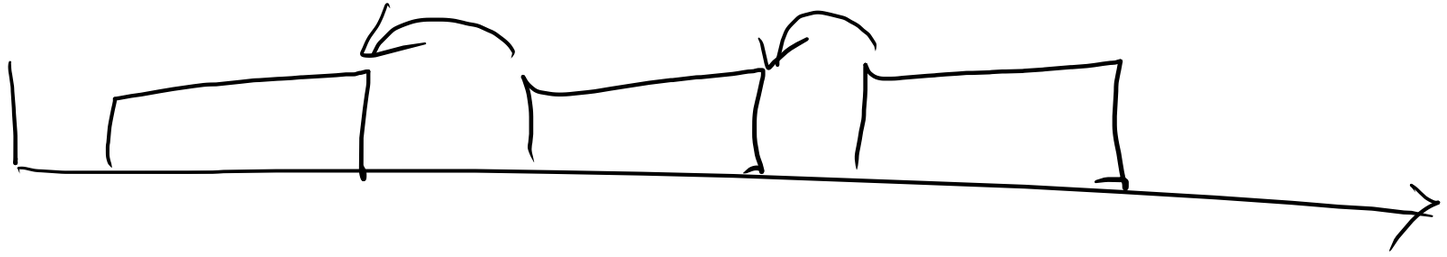
  $s_i = t$, $f_i = t + t_i$

  $t = t + t_i$
- output intervals: $[s_1, f_1], [s_2, f_2], \ldots, [s_n, f_n]$

running time $O(n \log n)$

correctness

observation: There exists an optimum schedule with no idle time.

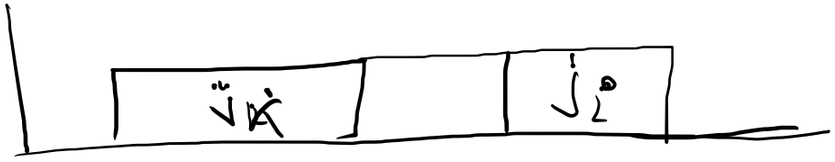


observation about our greedy schedule

EDF algo returns a schedule with no idle time

Definition inversion

An inversion is a pair of jobs j_i and j_k such that $d_i < d_k$ but j_k is scheduled before j_i



However $d_k > d_i$

observation about greedy

EDF does not have any inversion.

Claim If an idle-free schedule has an inversion then it is an adjacent inversion.

Proof j_i and j_K be a closest inversion but not adjacent.

$d_i < d_K$

There are two cases

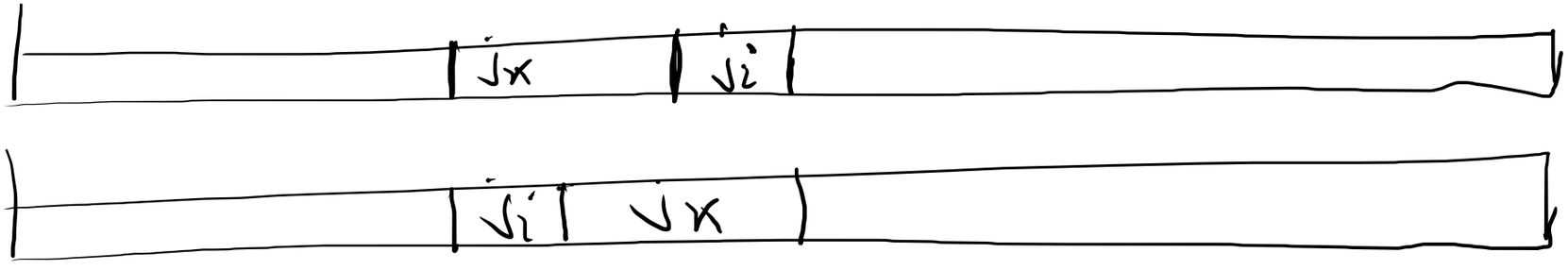
- $d_K > d_\ell \Rightarrow$ j_K and j_ℓ are inverted jobs.

- $d_K < d_\ell \Rightarrow$ $d_i < d_K < d_\ell$

j_ℓ and j_i are inverted jobs. $\Rightarrow\Leftarrow$

claim If we invert two adjacent inverted jobs j_i and j_k then it reduces the number of inversions by 1 and does not increase the maximum lateness.

Proof



- $L \leftarrow$ ~~be~~ the lateness before exchange
  $L' \leftarrow$ " " after exchange.
- For all other jobs other than j_i and j_k their lateness remain same.
- For the i-th job j_i:
  $l_i^{new} \leq l_i^{old}$ as it scheduled before now.

we want to show, $l_k^{new} \leq l_i^{old}$.

- If the job j_k is late.

$$l_k^{new} = f_k^{new} - d_k \quad \text{def}^n \text{ of lateness}$$

$$= f_i^{old} - d_k \quad \text{as } j_k \text{ finishes}^{now} \text{ at time } j_i \text{ in old schedule.}$$

$$\leq f_i^{old} - d_i^{old} \quad d_i \leq d_k \text{ by def}^n \text{ of inversion}$$

$$= l_i^{old}$$

lateness of j_k can not be more than the lateness of l_i in the old schedule.

$$\text{current lateness} = \max \{ l_1^{new}, l_2^{new}, \ldots l_k^{new}, l_i^{new}, \ldots l_n^{new} \}$$

$$\leq \max \{ l_1^{old}, l_2^{old}, \ldots, l_i^{old}, l_i^{old}, \ldots, l_n^{old} \}$$

- The algorithm produces a schedule with no inversion and no idle-time
- There is an optimum schedule with no inversion and no idle time.
- All schedule with no inversions and idle-free have the same lateness.

=> Greedy EDF is optimum.

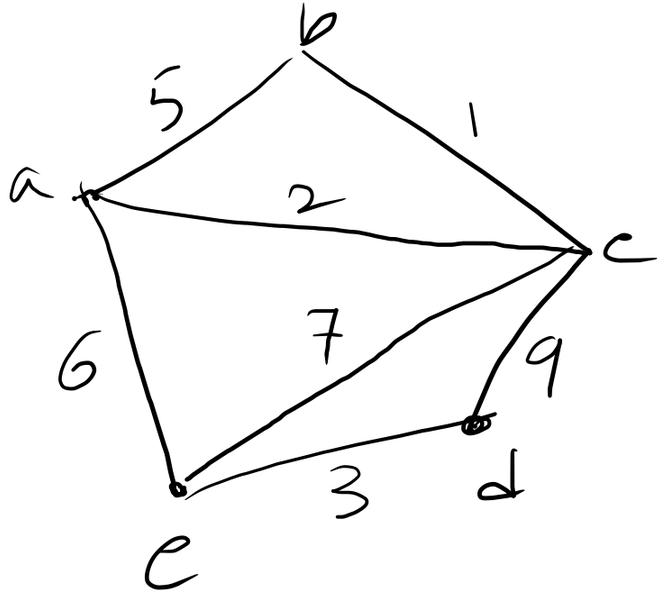
Minimum spanning tree (MST)

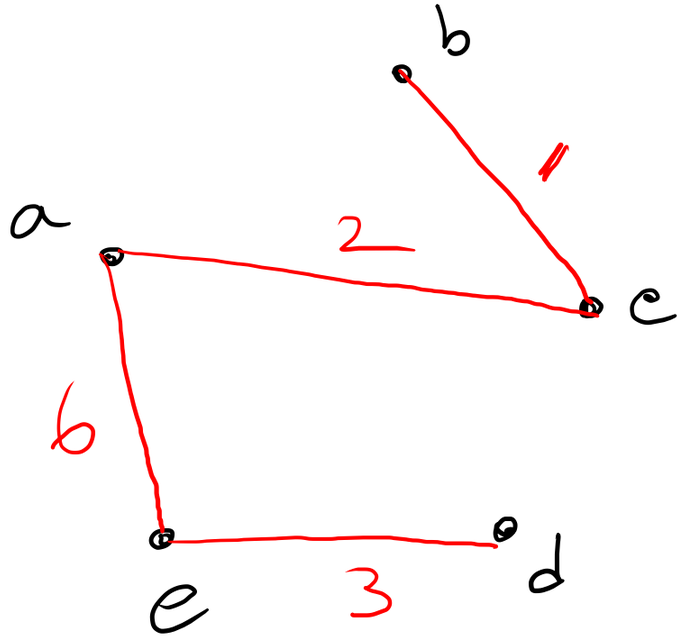
Problem: A connected graph $G(V, E)$ with edge costs.

$$w : E \rightarrow \mathbb{R}^+$$

Feasible solution: A subset $T \subseteq E$ such that $G_T(V, T)$ is connected

objective Total cost of all the edges in T is minimum.





cost of $T = 12$

Greedy algorithm

```
Generic-MST (G, w)
T is empty
while E is not empty
        choose e in E
        if (e satisfies some condition)
                add e to T
Return the set T
```

The graph $G_T = (V, T)$ is MST.

main task: → In what order should the edges be processed?
→ when should an edge be a part of the spanning tree?

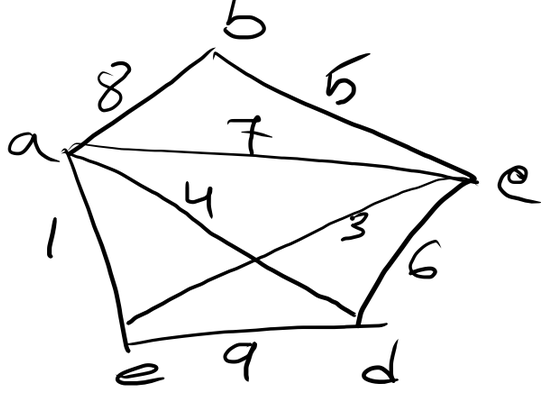
Kruskal's algorithm

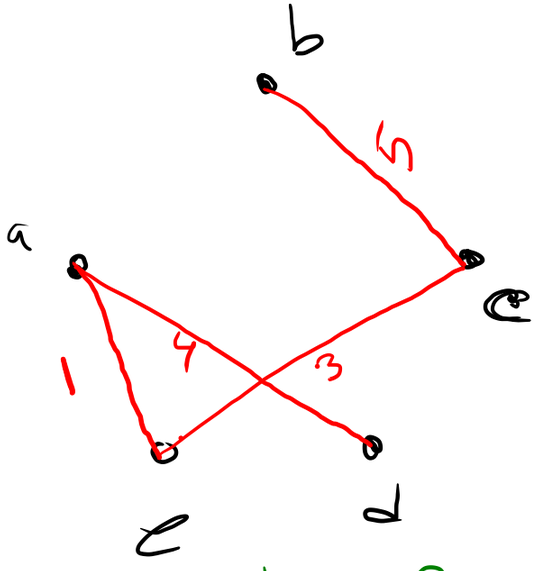
Kruskal-MST(G, w)

- T is empty
- sort the edges of G in non-decreasing order by their weights
- while E is none empty
  - choose $e \in E$ in the above order
    - if (e does not form a cycle with the edges in T)
      - add e to T
  - return the set T.

✓ ✓ ✓ ✓ X X X X
1 3 4 5 6 7 8 9

$T = \{(a,e), (c,e), (a,d), (b,c),$





cost = 13

Prim's algorithm

Prim - MST (G, w)

- T is empty
- $X = \{s\}$ where s is an arbitrary start vertex.
- while there is an edge $e = (u, v)$ where $u \in X$ and $v \notin X$

  $e^* = (u^*, v^*)$ be a minimum such edge

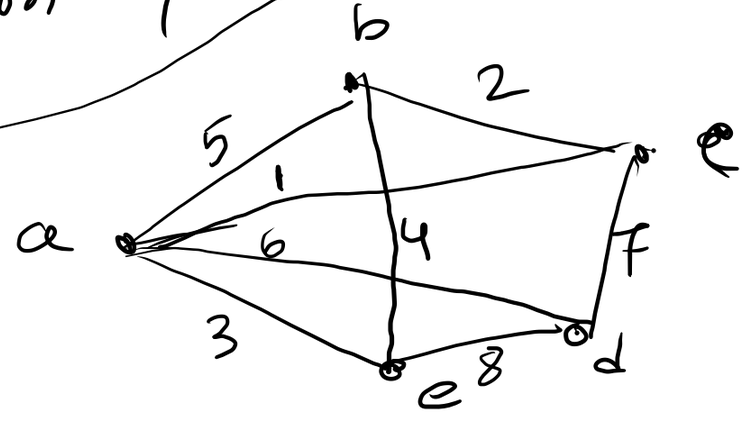
  add v^* in X

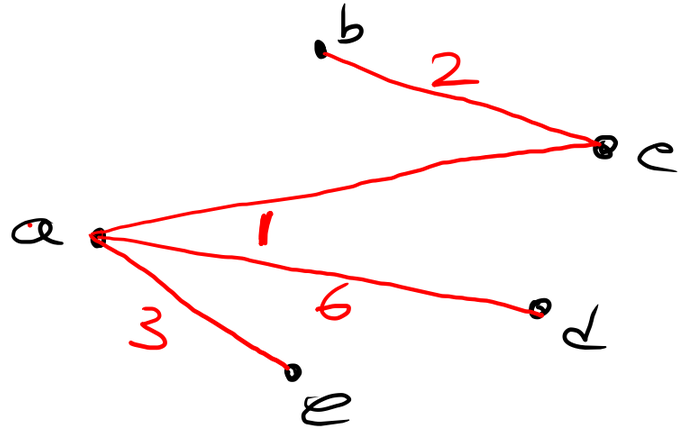
  add e^* in T

return T

$T = \{(a,c), (c,b), (a,e), (a,d)\}$

$X = \{a, c, b, e, d\}$

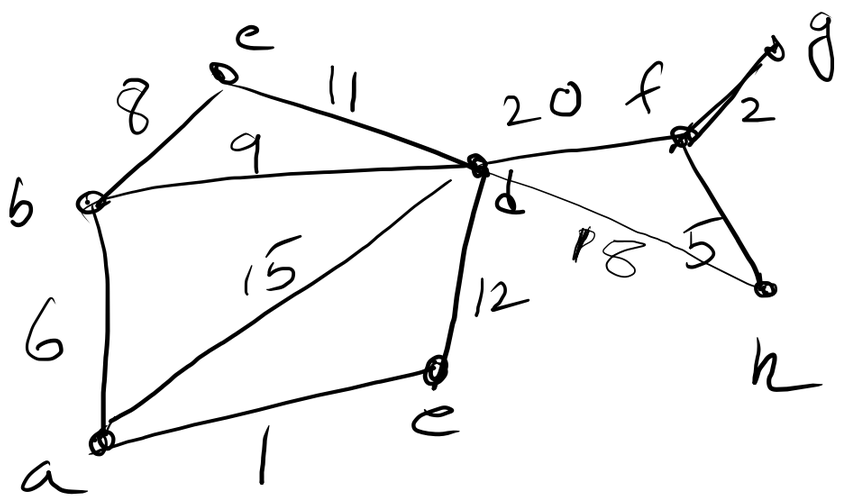


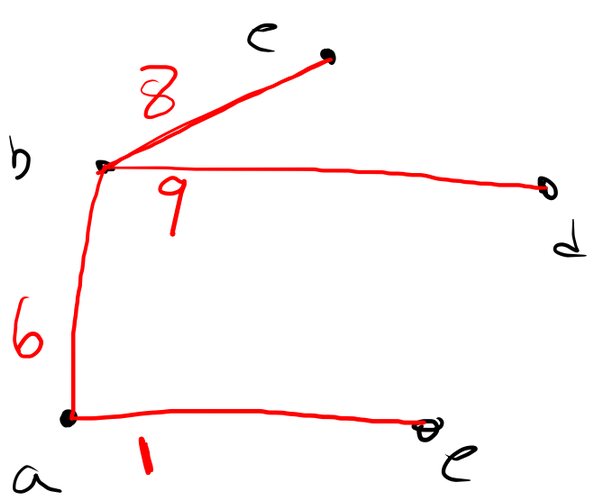


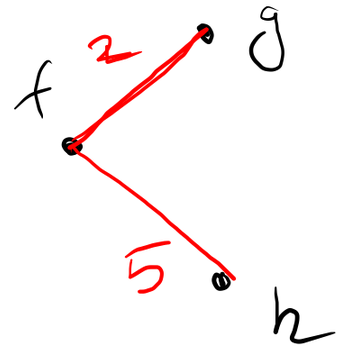
Boruvka's algorithm

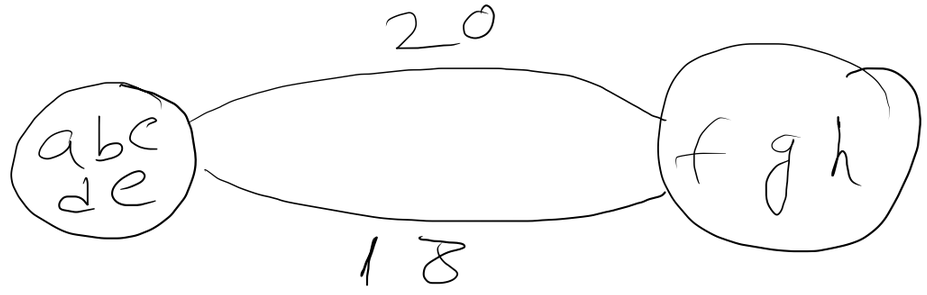
Boruvka-MST(G, w)

- T is empty
  (assume that each vertex is a connected component)
- for each vertex $v \in V$
  - add the edge in T whose weight is minimum over all edges incident on v.
- G' be the graph generated by contracted all the edges of T
- T' be the MST computing recursively on G'
- return the set $T \cup T'$









$T' = (d, h)$ of weight 18

Reverse delete

Reverse-delete-MST(G, w)

- T is E
- sort the edges in E in non-increasing order by their weights.
- while E is not-empty:
  - choose e with largest weight
    - if removing e does not disconnect T
      remove e from T

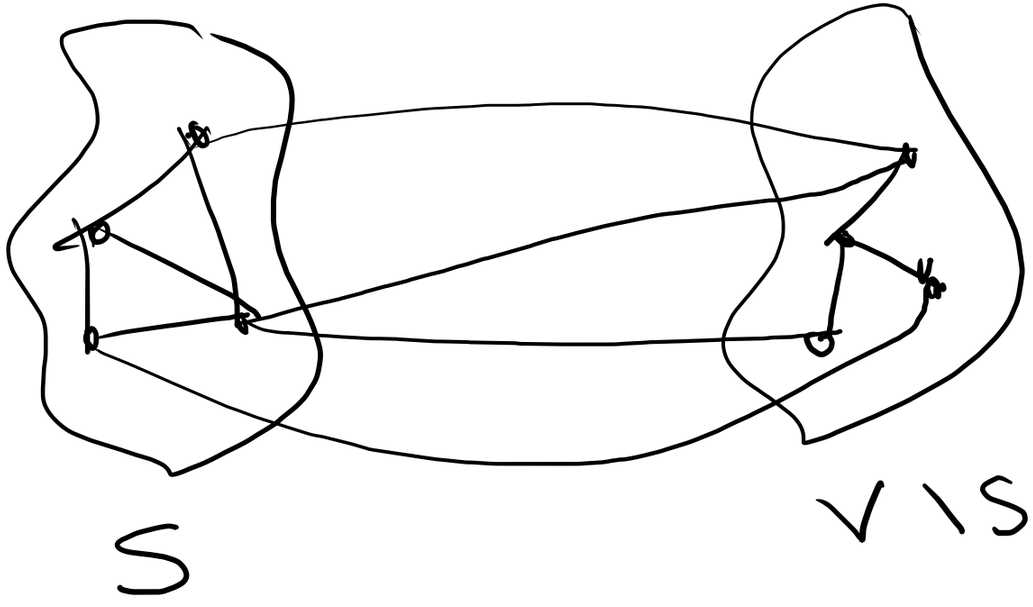
return the set T.

Correctness of MST algorithms

- There are many MST finding algorithms
- All of them rely on some basic properties of MST
  - cut property
  - cycle ,,

- Assume that edge costs are distinct.

cut: Partition of vertex set of a graph in S and $V \setminus S$

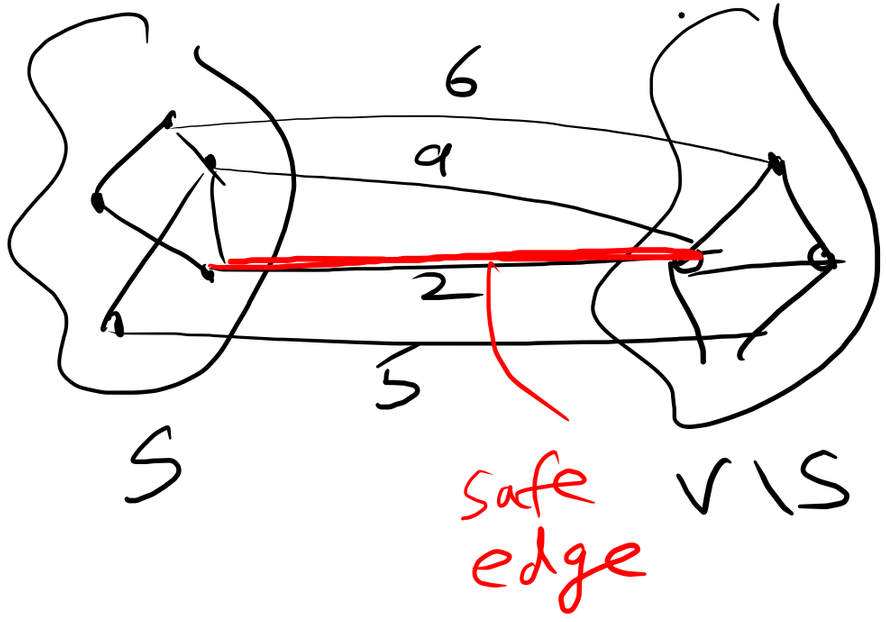


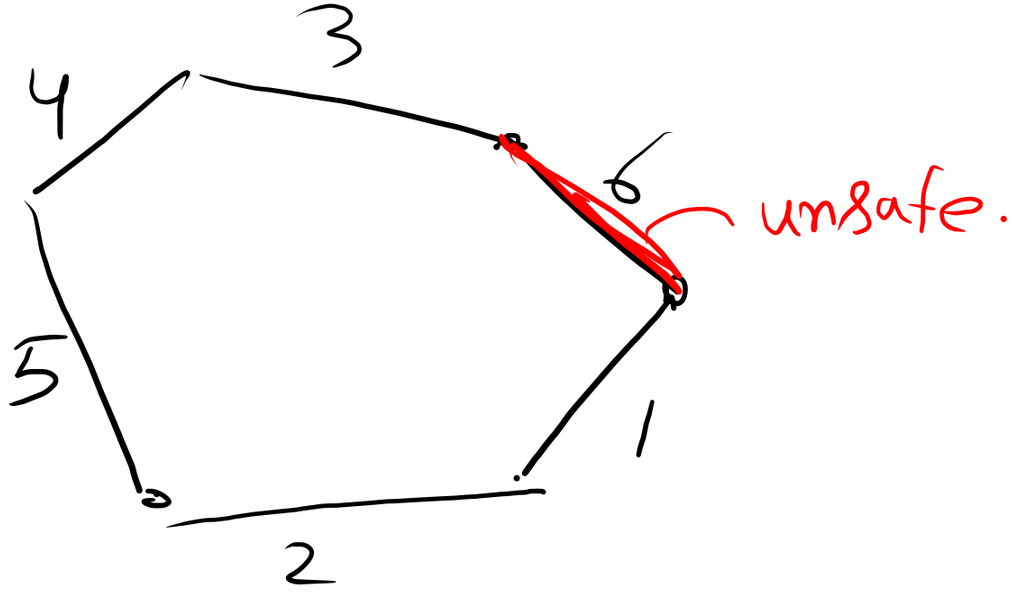
edges in the cut: edges crossing the cut.
one end in S and another in $V \setminus S$

Safe and unsafe edges

safe edge: unique minimum weight edge crossing a cut.

unsafe edge: unique maximum weight edge of a cycle.



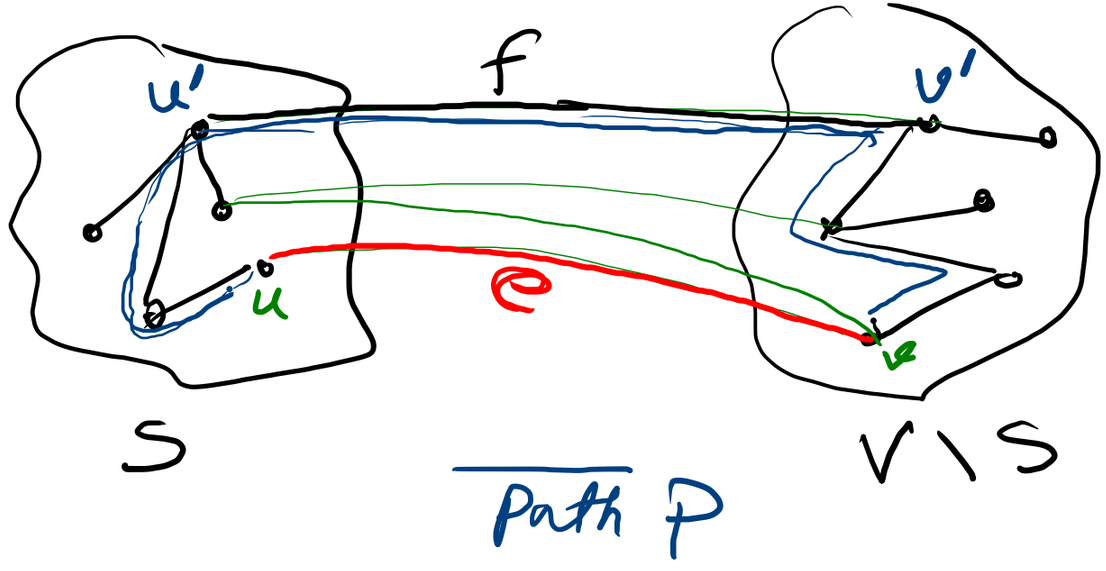


cut property and its correctness

cut property: Let S be any subset of vertices of V and $e=(u,v)$ be the minimum cost edge with one end point in S and the other in $V \setminus S$. Then every MST contains e.

Proof By contradiction.

- G_T be a MST that does not contain e.
- Assume that $u \in S$ then $v \notin S$
- Since G_T is a MST there is a unique path P from u to v.



- $f = (u', v')$
- v' is the first vertex on P (starting from u) in $V \setminus S$
- u' is just befor v'
- consider the graph $G_{T'} = (G_T \setminus \{f\}) \cup \{e\}$

If $G_{T'}$ is a spanning tree → we need to prove.

we have a contradiction due to G_T is a MST

claim $G_{T'}$ is a spanning tree

i) $G_{T'}$ is connected. ✓

ii) $G_{T'}$ is a tree ✓

iii) $G_{T'}$ has lower cost than G_T ✓

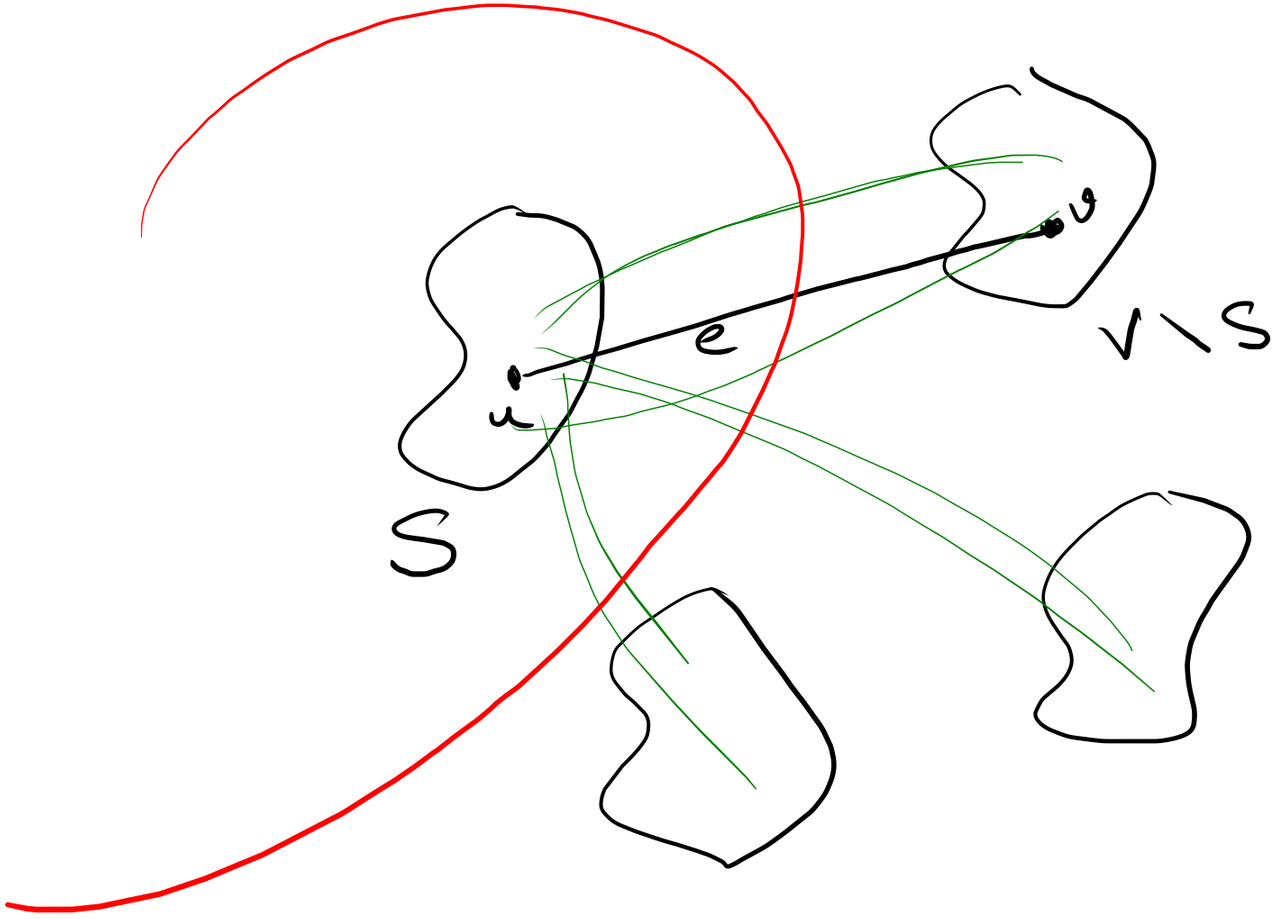
cycle property :—

H.W.

- $e = (u, v)$ be a edge of smallest weight not creating any cycle.

- e does not belong to a single component.

-



Boruvka's algo
Reverse delete } H.W.

Running time

G has n vertices
m edges

Kruskal $\rightarrow O(m \lg m + m \cdot n)$

$\rightarrow O(mn)$

Prims $\rightarrow O(mn)$

Boruvka's $\rightarrow T(mn) = T\left(\frac{n}{2} m\right) + O(m)$

Reverse delete $\rightarrow O(mn)$

Kruskal's algorithm : Efficient implementation

Kruskal-MST (G, w)

- T is empty
- Sort the edges based on non-decreasing weights.
- each vertex v is placed in a set ⟸ make set
- while E is not empty
  - choose $e = (u, v) \in E$
  - if u and v belongs to two different sets ⟸ Find(u) ≠ Find(v)
    - add e to T
    - merge the sets containing u and v ⟸ Union(u, v)
- return the set T

Sorting — $O(|E| \log |E|)$

$|V|$ ← makeset operations.

$2|E|$ ← Find(u) " "

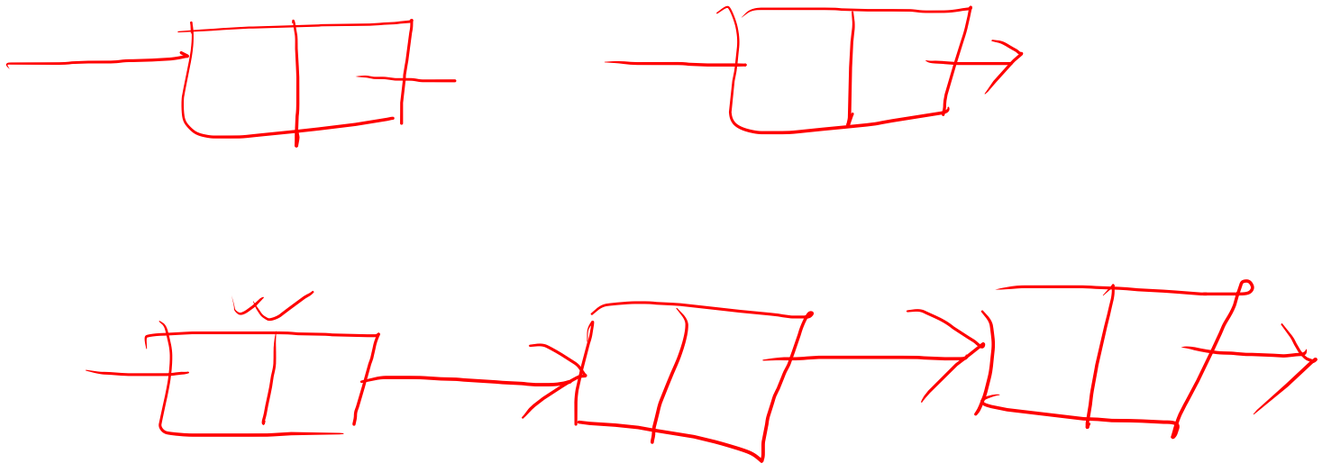
$|V| - 1$ ← Union "

Total running time $O(|E| \log |E|) + |E| \log |V|$

If we implement disjoint set operations by union by rank.

then makeset $O(1)$ Union — $O(\log |V|)$

Find(u) — $O(\log |V|)$



Merge .

Prim's algorithm

$\pi(v) \leftarrow$ minimum cost between v and s

$Pred[v] \leftarrow$ vertex just before v

Prim-mst(G, w) — T

- T is empty — $\theta(1)$
- $X = \{s\}$ — $\theta(1)$
- for each vertex $v \neq s$ — $O(|V|)$
  $\pi[v] \leftarrow \infty$, $Pred[v] \leftarrow$ Null — $\theta(1)$
- $\pi[s] \leftarrow 0$ — $\theta(1)$
- create an empty priority queue Q — $\theta(|V|)$
- for each vertex $v \in V$ — $\theta(|V|)$
  Insert (Q, v, $\pi[v]$) — T_{insert}
- while Q is not empty — $O(|V|)$ times
  $u \leftarrow$ Extract-min (Q)
  for each edge $v \in Adj[u]$ — $O(|E|)$ times
  if $v \in Q$ and $w(u,v) < \pi[v]$
  Decrease-key (Q, v, $\pi[v]$)
  $Pred[v] \leftarrow u$

$T = O(|V|)\, T_{insert} + O(|V|)\, T_{extractmin} + O(|E|)\, T_{Decrease\text{-}key}$

priority queue	$T_{extract\text{-}min}$	$T_{decrease\ key}$	Total.
Array	$O(\|V\|)$	$O(1)$	$O(\|V\|^2)$
Binary heap	$O(\lg \|V\|)$	$O(\lg \|V\|)$	$O(\|E\| \lg \|V\|)$
Fibonacci heap	$O(\lg \|V\|)$ amortized	$O(1)$ Amortized	$O(\|E\| + \|V\| \lg \|V\|)$ Amortized

Shortest path problem

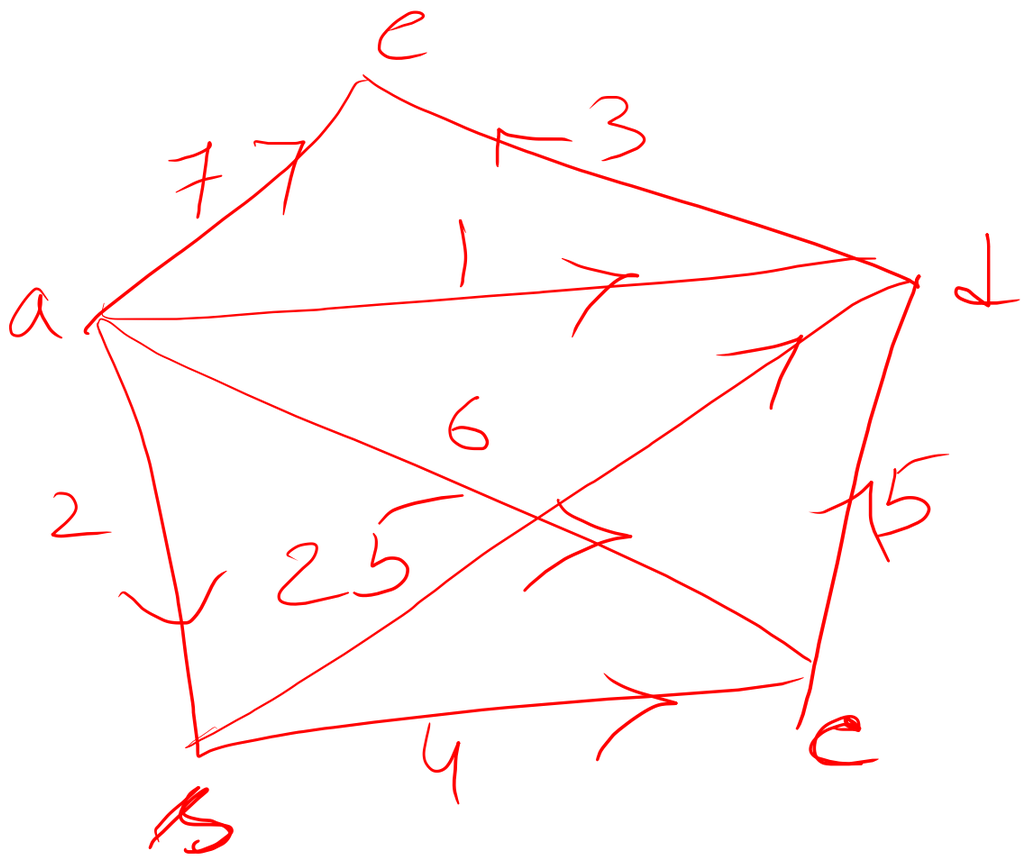
- Given a (directed or undirected) graph $G(V, E)$ with edge costs $w : E \to \mathbb{R}^+$

output: i) Given $s, t \in V$ find shortest path from s to t

ii) Given $s \in V$ find shortest path from s to all other vertices

iii) Find shortest paths from all pairs of vertices.

→ single source shortest path



d = t

s → c → d (=t) cost 9

s → d (=t) cost 25

Shortest path problem

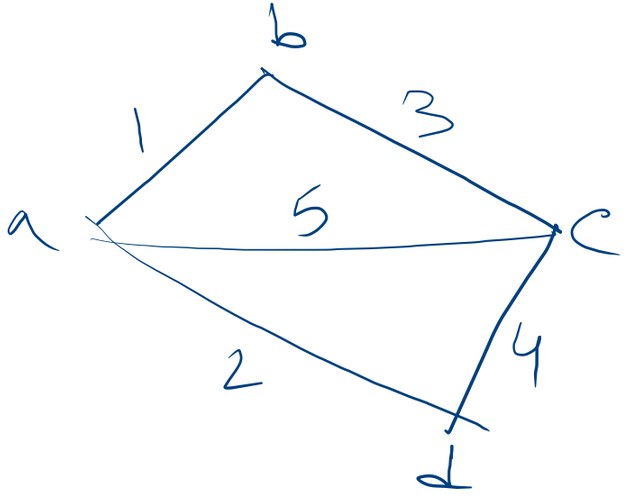
- single source shortest path problem.

  Given s find shortest path from s to all other vertices

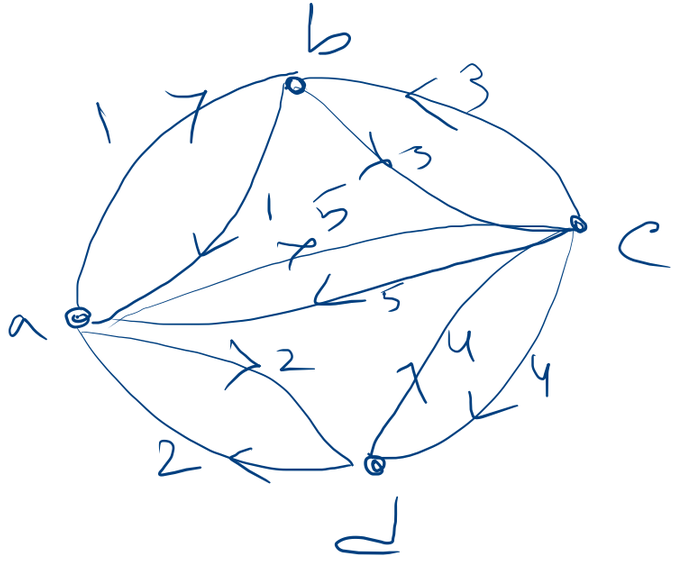
  Given s, t " " " " from s to t.

⇒ we will concentrate on directed graphs only.

Why?.



⟹



H.W.

Special cases 1

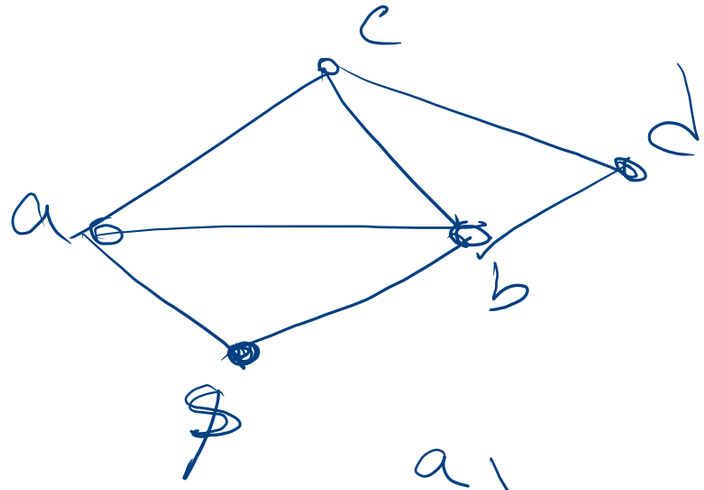
— Assume the edge weights are all 1.

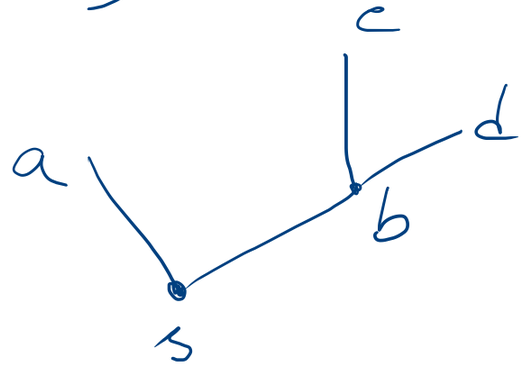
— use BFS algorithm.

Time: $O(|V|+|E|)$

$|V| = n$

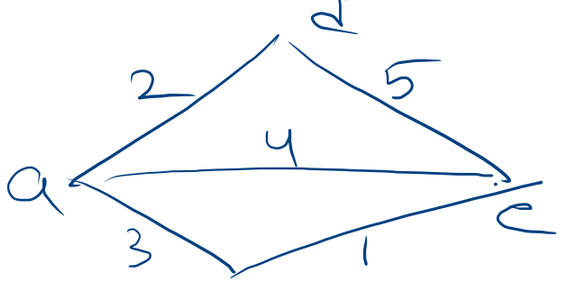
$|E| = m$

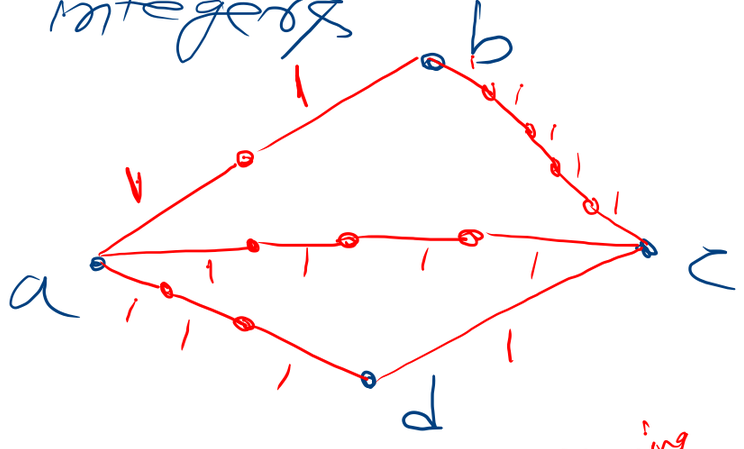




Special case 2

— All edge weights are integers





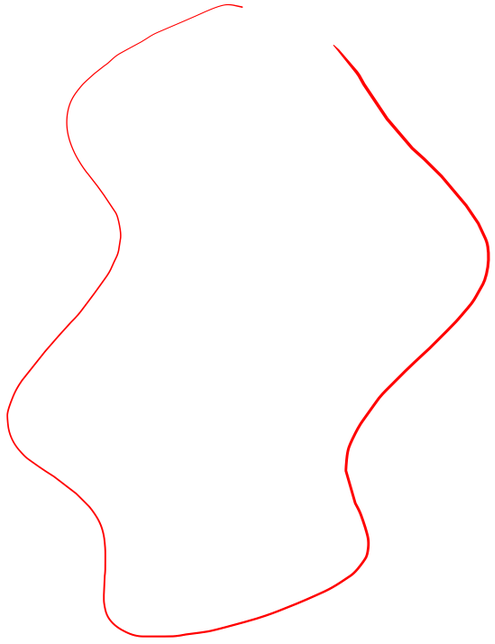
L = maximum Number of edges added in an old edge

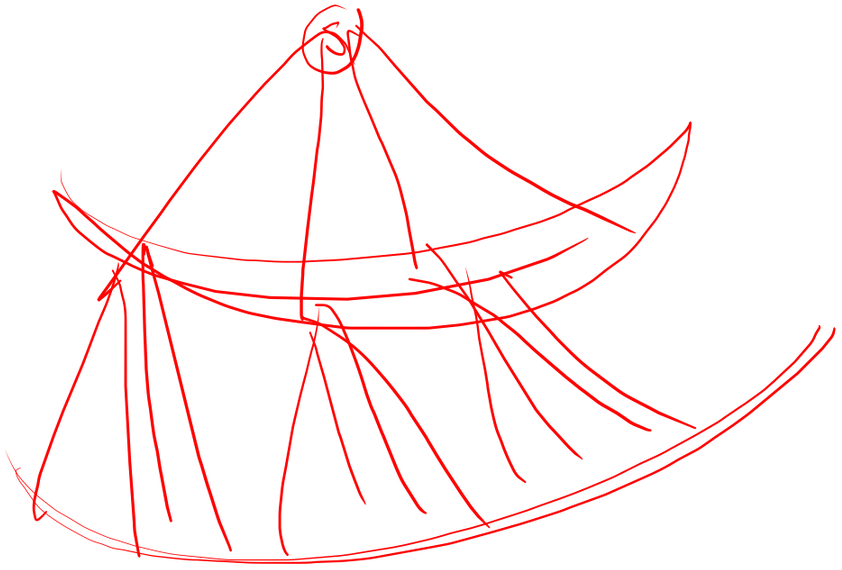
vertices = $mL+n$

edges = mL

running time: $O(mL+n)$

For large L, this algorithm is not efficient.

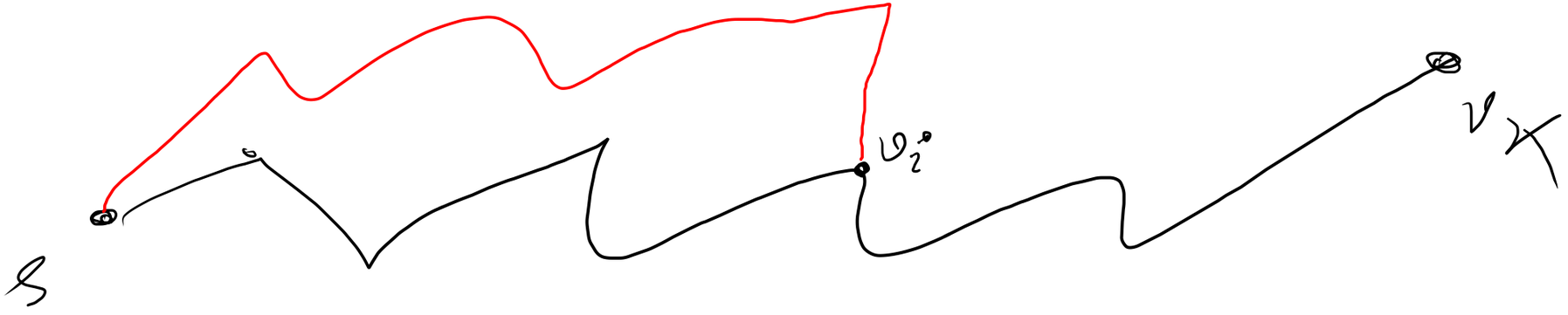




Let G be a directed graph with non-negative edge weights. Let $dist(s, v)$ is the shortest path weight from s to v.

If $s = v_0 \to v_1 \to v_2 \cdots \to v_K$ be the shortest path from s to v_K then for $1 \le i \le K$

- $s = v_0 \to v_1 \to \cdots \to v_i$ is a shortest path from s to v_i
- $dist(s, v_i) \le dist(s, v_K)$



General case

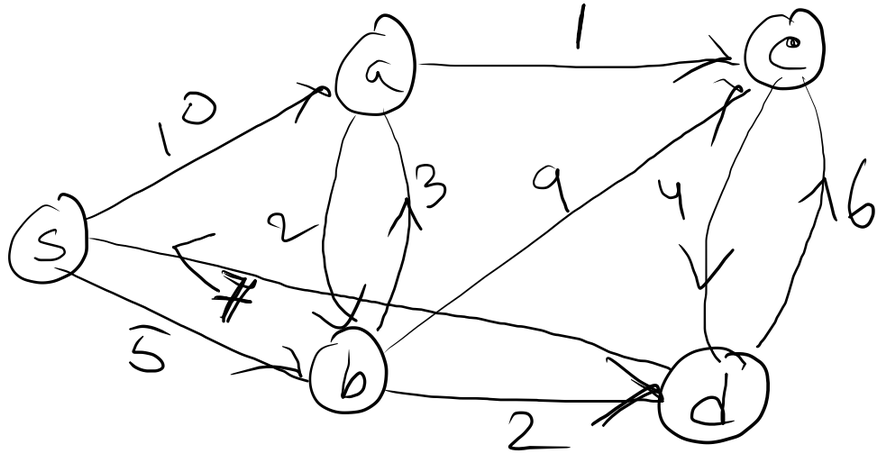
$d[v] \leftarrow$ shortest path distance from s to v
$\pi[v] \leftarrow$ parent of v.

Dijkstra's algorithm

```
Dijkstra (G, w, s)
d[s] = 0
for each vertex v ∈ V \{s}
        d[v] ← ∞ , π[v] ← NIL
S ← ϕ (empty set)
Q ← V   // Q ← a priority queue
While Q ≠ ϕ
    u = Extract-min (Q)
    S = S ∪ {u}
    for each vertex v ∈ Adj[u]
        if d[v] > d[u] + w(u,v)
            d[v] = d[u] + w(u,v)
            π[v] ← u
```

Running time:

$O(|V|) \cdot T_{\text{extract-min}} + O(|E|) T_{\text{decrease-key}}$



Q	d	Π
s	0	NIL
a	∞	NIL
b	∞	NIL
c	∞	NIL
d	∞	NIL

S = { }

	Q	d	Π
X	s	0	NIL
	a	10	s
	b	5	s
	c	∞	NIL
	d	∞	NIL

s ← Extract-min (Q)

S = {s}

$b \leftarrow$ Extract-min (Q) $\quad S = \{s, b\}$

	Q	d	$\overline{\Pi}$
X	~~s~~	0	~~NIL~~
	a	~~10~~ 8	~~b~~
X	~~b~~	5	~~s~~
	c	~~14~~ 6	b
	d	~~7~~	b

Final table

Q	d	π
s	0	NIL
a	8	b
b	5	s
c	9	a
d	7	b

Shortest paths:

s to a

weight is 8

$s \rightarrow b \rightarrow a$

Divide and conquer

Sorting algorithms

Sorting: Given a sequence of numbers

$$a_1, a_2, \ldots, a_n$$

output: Return a permutation of the numbers such that

$$a_{i_1} \leq a_{i_2} \leq \ldots \leq a_{i_n}$$

Ex^m Input: 2 1 6 3 9

output: 1 2 3 6 9

Merge Sort

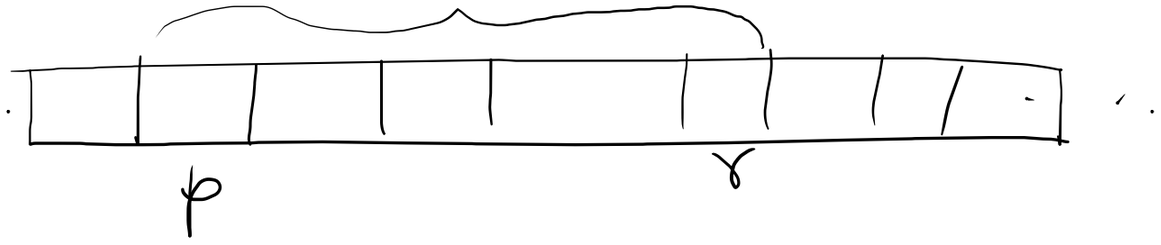
High-level idea

- Divide the array(A) into roughly two equal partitions :- L and R
- sort the array L
- sort the array R
- merge the two sorted arrays L & R to get the sorted array A.

Mergesort (A, p, r) — T(n)

if p < r — Θ(1)

$q = \frac{p+r}{2}$ — Θ(1)



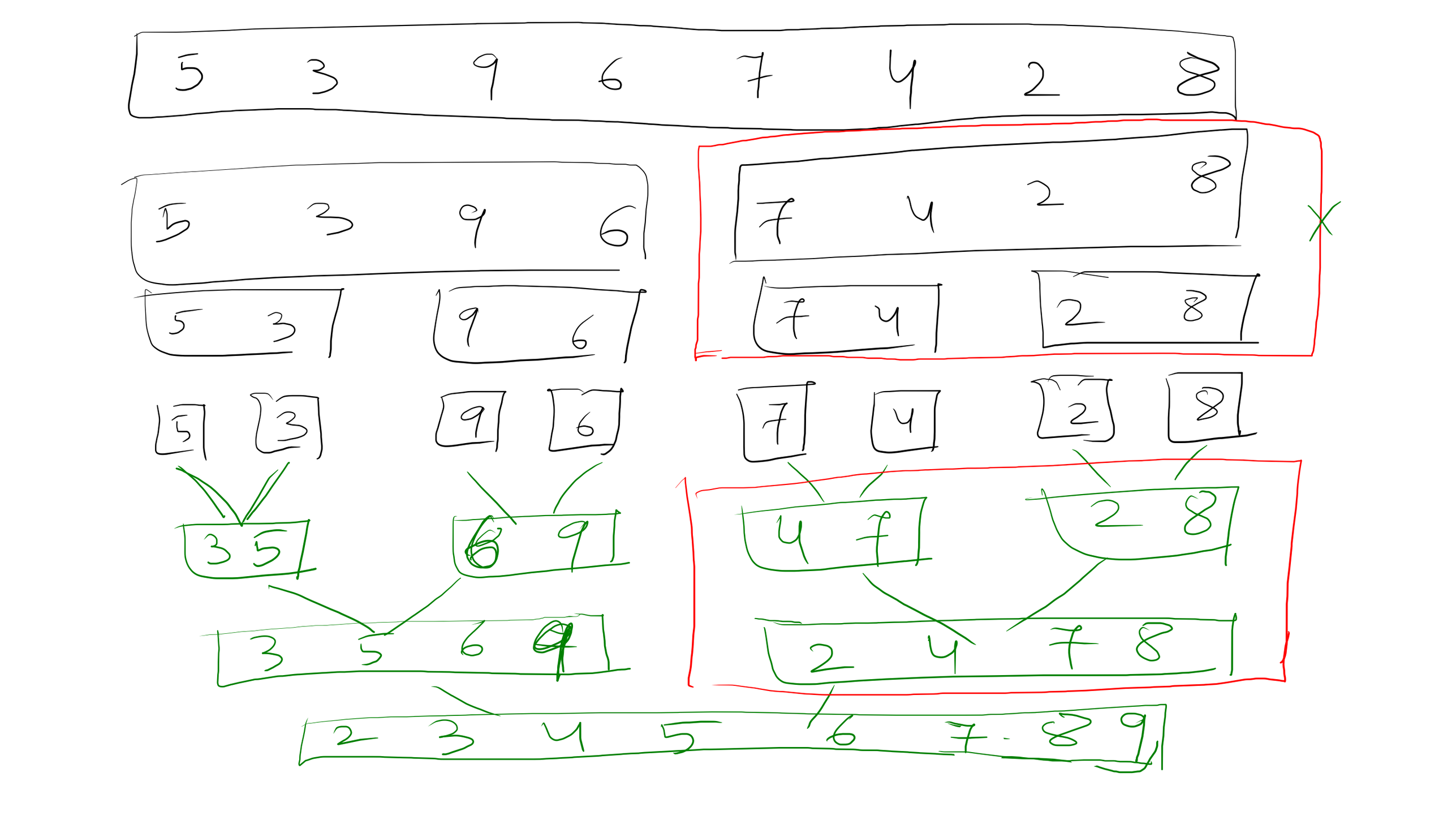
mergesort (A, p, q) — $T(\frac{n}{2})$

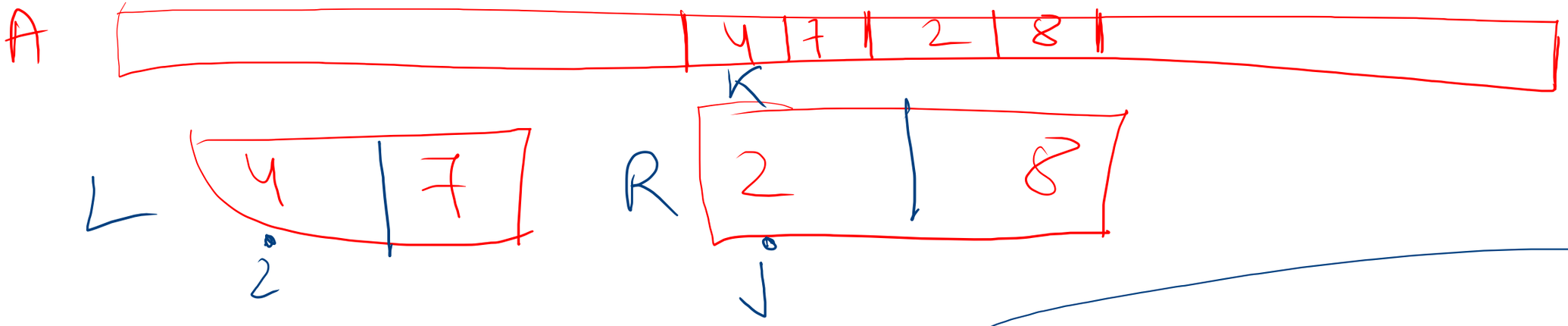
mergesort (A, q+1, r) — $T(\frac{n}{2})$

merge (A, p, q, r) — $\Theta(n)$

Total time: $T(n) = 2T(\frac{n}{2}) + \Theta(n)$

$\Rightarrow T(n) = \Theta(n \log n)$


5 3 9 6 7 4 2 8
5 3 9 6
7 4 2 8
5 3
9 6
7 4
2 8
5
3
9
6
7
4
2
8
3 5
6 9
4 7
2 8
3 5 6 9
2 4 7 8
2 3 4 5 6 7 8 9



if $L[i] \leq R[j]$

$A[k] \leftarrow L[i]$

$k = k+1$

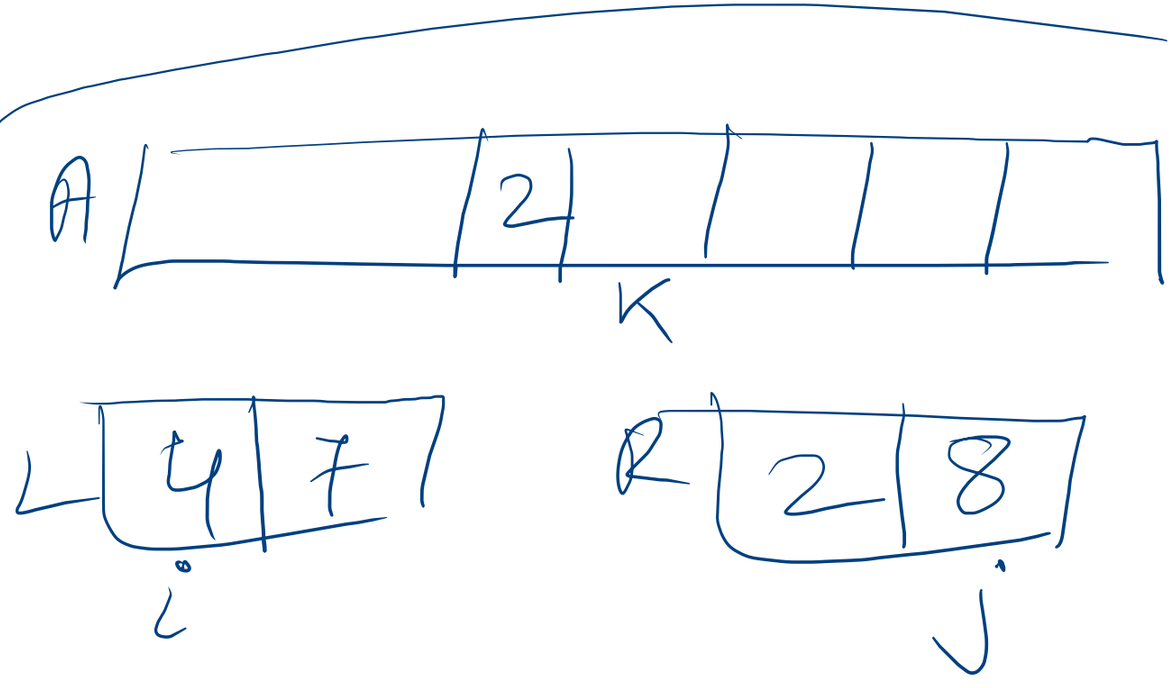
$i = i+1$

else

$A[k] \leftarrow R[j]$

$k = k+1$

$j = j+1$



```
merge(A, p, q, r)
  n1 ← q - p + 1
  n2 ← r - q
  for i = 1 to n1
      L[i] ← A[p + i - 1]
  for j = 1 to n2
      R[j] ← A[q + j]
  L[n1 + 1] ← ∞
  R[n2 + 1] ← ∞
⟹ for k = p to r
      if L[i] ≤ R[j]
          A[k] ← L[i]
          i = i + 1
      else A[k] ← R[j]
          j = j + 1
```

running time :- $O(n)$

At the start of each iteration of the for loop.

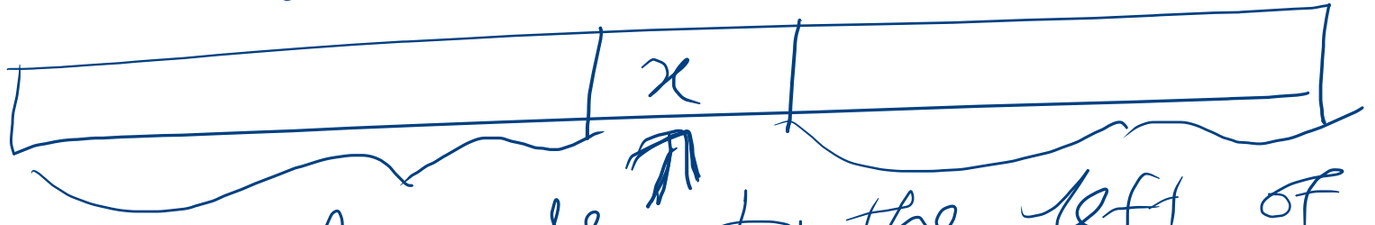
subarray $A[p \ldots k-1]$ contains the $k-p$ sorted elements of L and R

and $L[i]$ and $R[j]$ are the smallest elements of L and L that are yet to copied in A.

Quicksort

high level idea

- we choose a suitable element x
- based on the element x we partition the array into two parts:



- all the elements to the left of x are $\leq x$
- all the elements to the right of x are $> x$

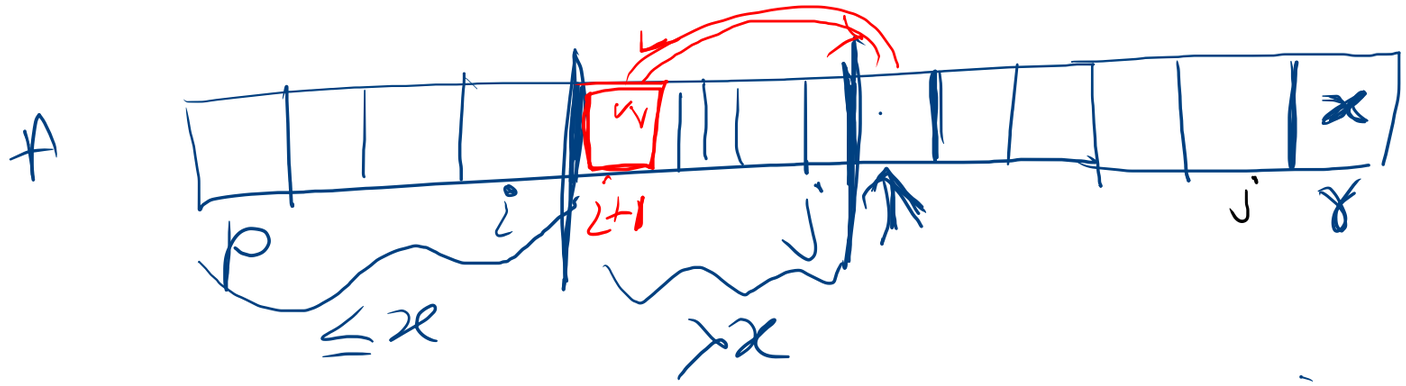
quicksort (A, p, r) ——— T(n)

if p < r ——— θ(1)

q = partition (A, p, r) ——— Θ(n)

quicksort (A, p, q-1) ———

quicksort (A, q+1, r) ———

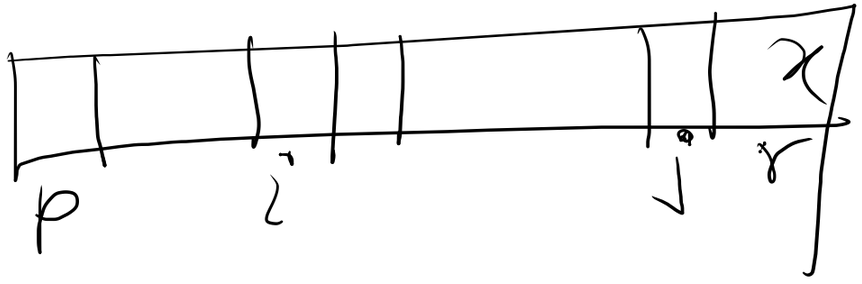


$A[j+1]$ compares with x.

either $A[j+1] \leq x$

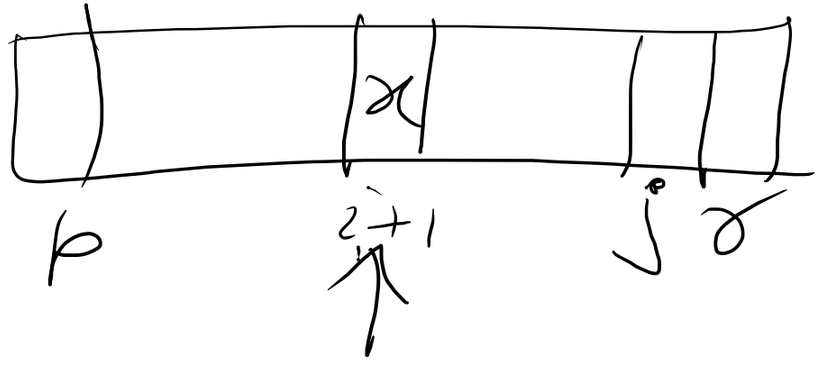
$i = i+1$

swap $A[j+1] \leftrightarrow A[i]$

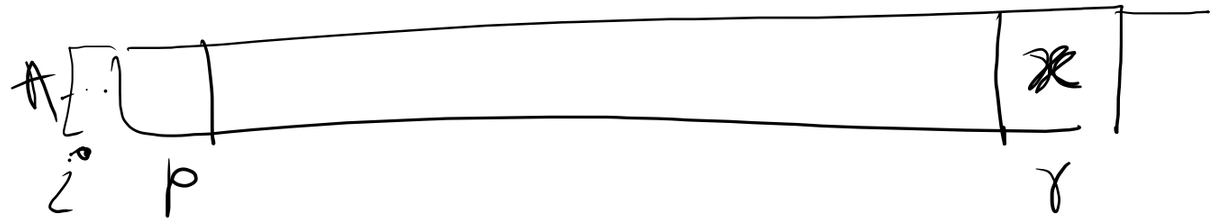


$A[j+1] > x$

$j = j+1$



```
Partition(A, p, r)
  x = A[r]
  i = p - 1
  for j = p to r - 1
      if A[j] ≤ x
          i = i + 1
          swap A[i] ⟷ A[j]
  swap A[i+1] ⟷ A[r]
  return i+1
```

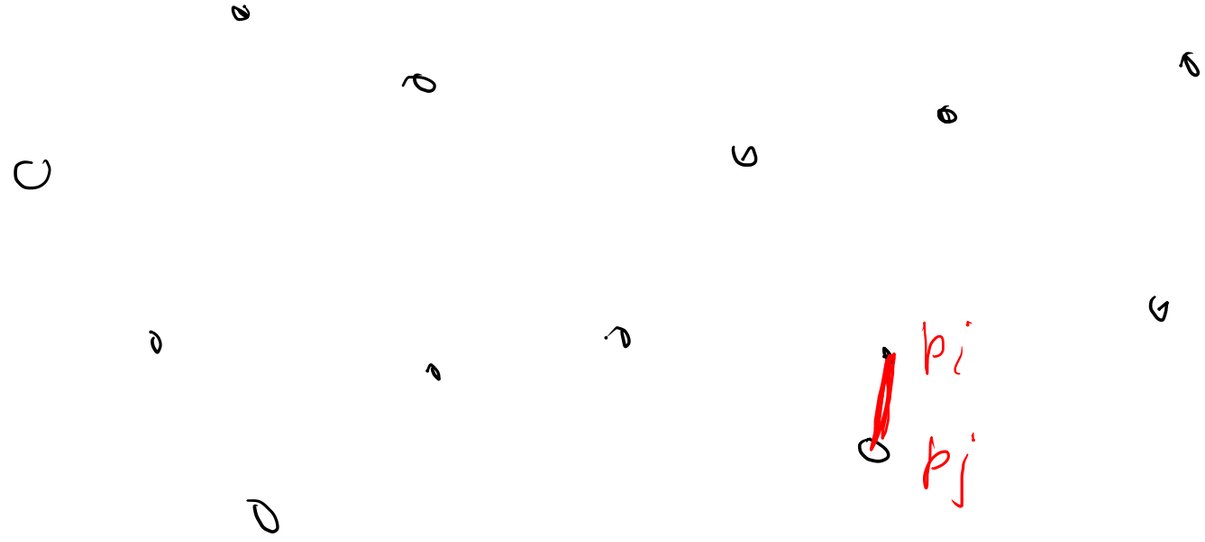


All the elements are same.

closest pair problem

Problem: Input: A set of n points $P = \{p_1, p_2, \ldots, p_n\}$

output: Find a pair (p_i, p_j) such that their distance is minimum.



A naive algorithm

For each pair compute the distance
return the pair with minimum distance.

running time $O(n^2)$

can we do better??

1D-version

points are on a line.

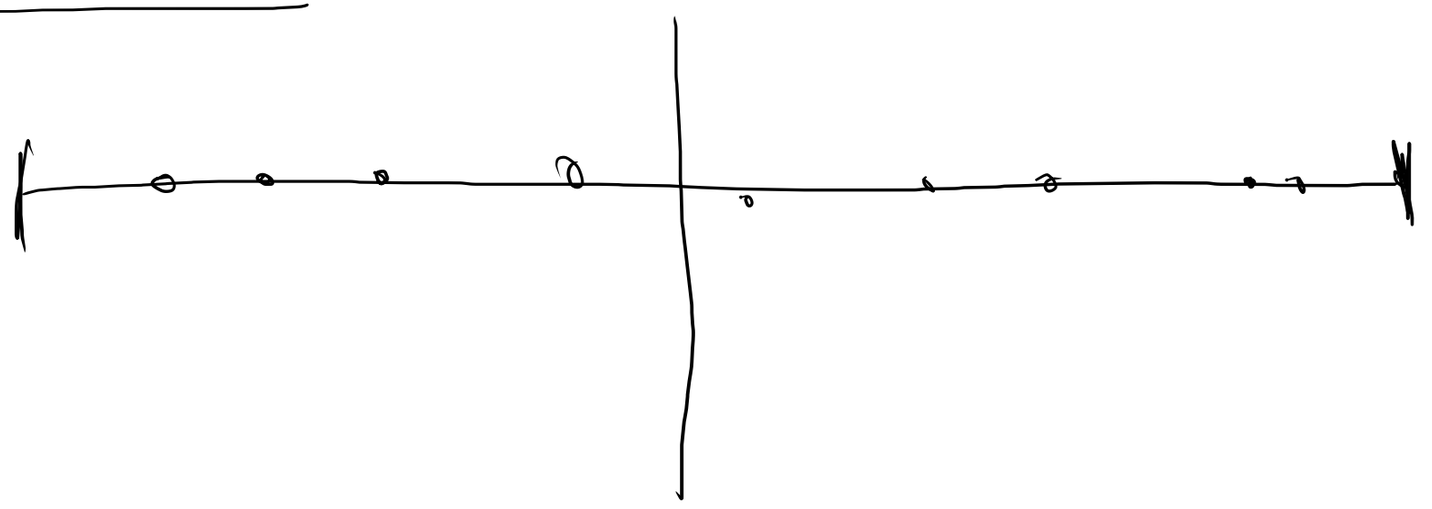
Sort the points.

take distance between consecutive pair.

running time: $O(n \log n) + O(n)$

Applying D & C on 1D version

1 Sort the points



closestpair (P)

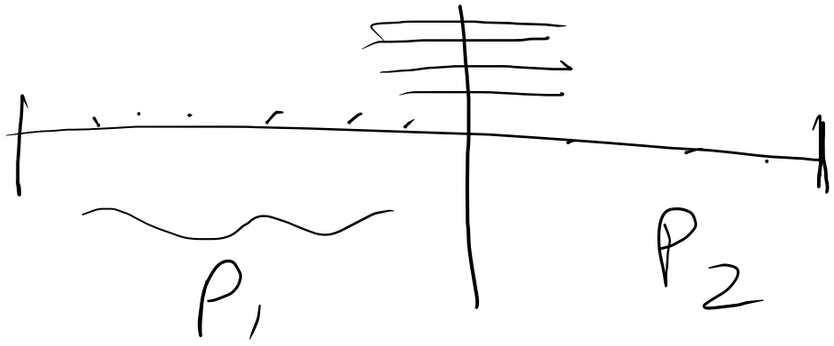
If $|P| = 1$ return $\delta_F = \infty$

If $|P| = 2$ return $\delta_F = |p_2 - p_1|$

otherwise

L = median (P)

Divide P in P_1 and P_2 w.r.t. L



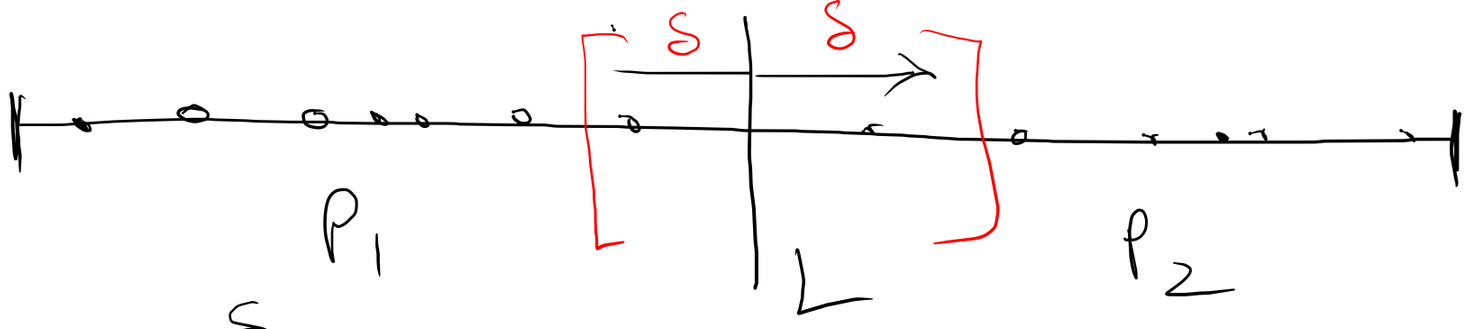
δ_L = closestpair (P_1)

δ_R = closestpair (P_2)

δ_{12} = minimum distance crossing L —— f(n)

return $\delta_F = \min\{\delta_L, \delta_R, \delta_{12}\}$

$T(n) = 2T(n/2) + f(n)$ where $f(n)$



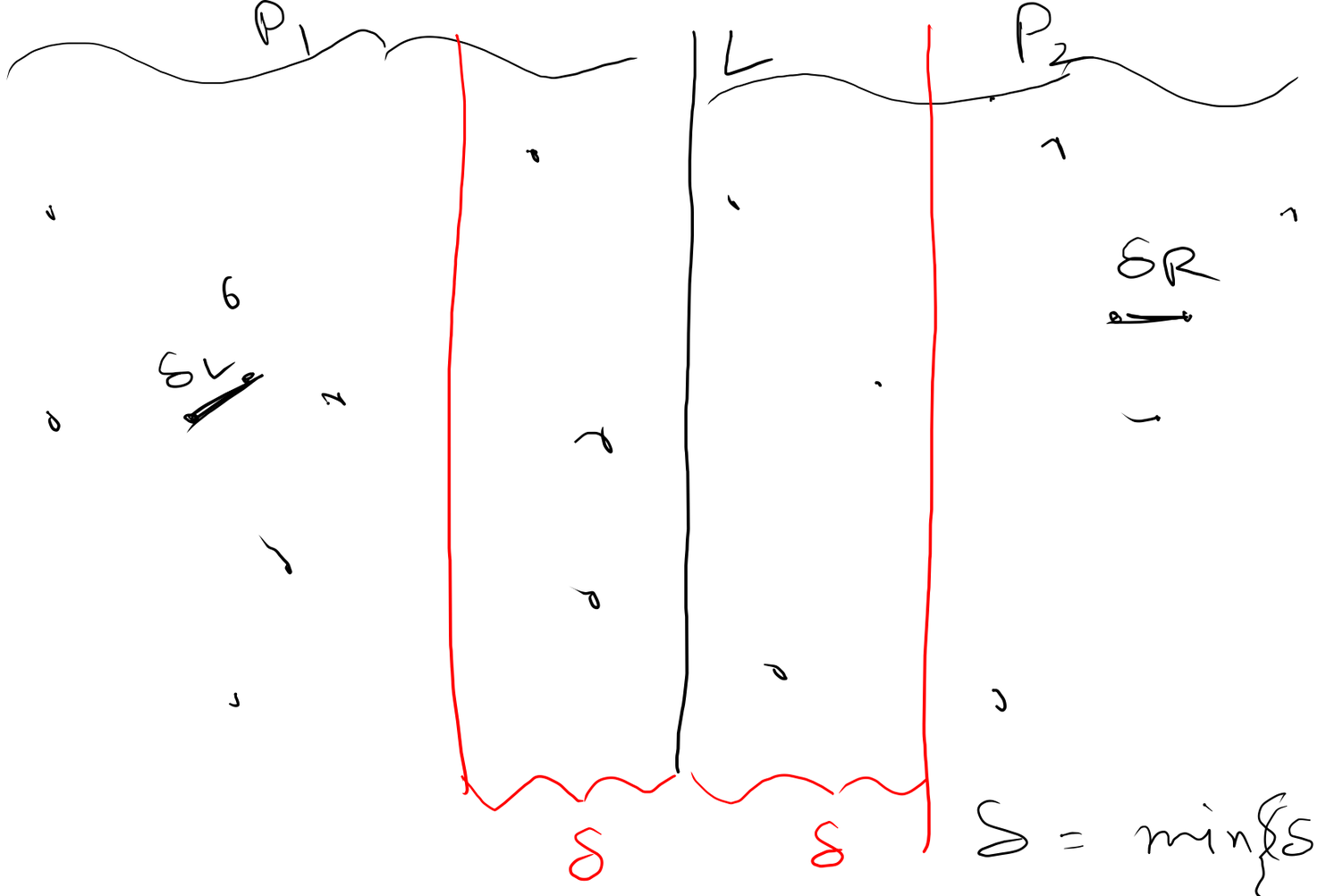
$\delta = \min\{\delta_L, \delta_R\}$

$$T(n) = 2T(n/2) + \theta(n)$$

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

2D - version

closest pair 2D (θ)



$\delta_L =$

$\delta_R =$

for each p in P_1 and for each q in P_2

compute their distances

δ_{12} = minimum of them

$\delta_f = \{\delta_L, \delta_R, \delta_{12}\}$

$\delta = \min\{\delta_L, \delta_R\}$

$T(n) = 2\,T(n/2) + O(n^2)$

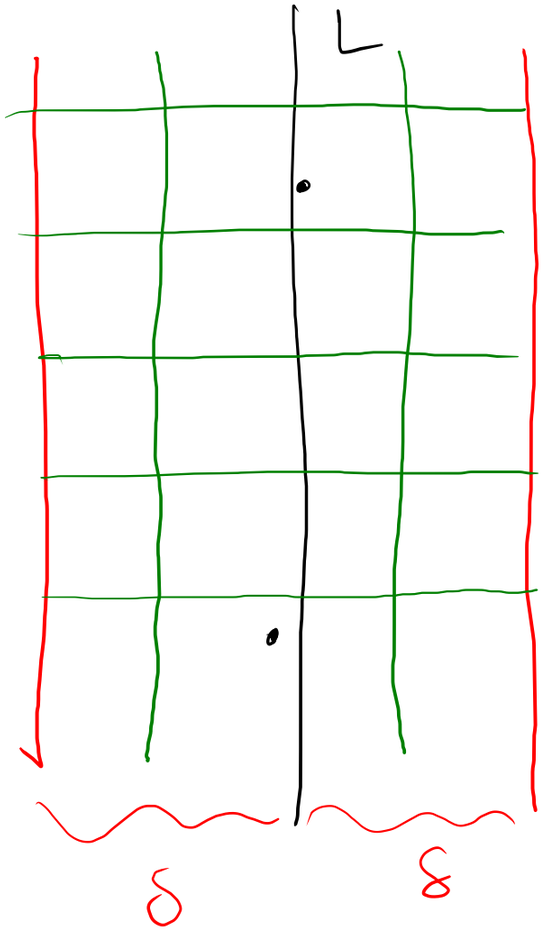
$= O(n^2)$

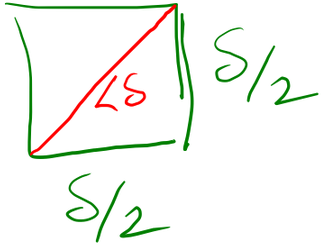
no improvement

Question:

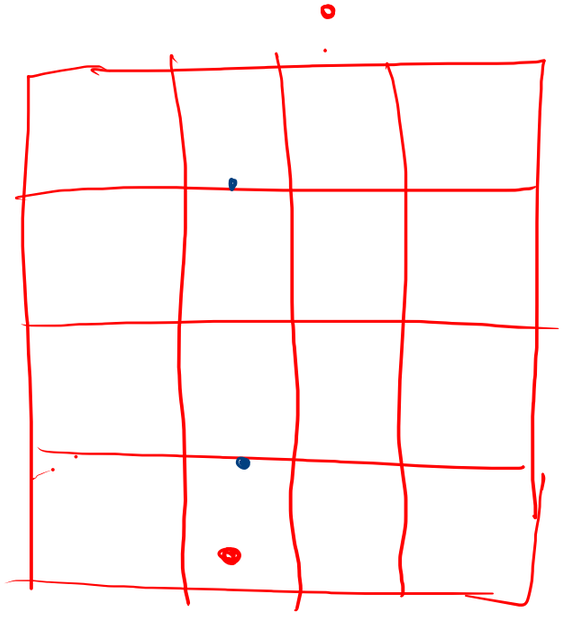
How many points are there in a single box?

Ans: At most 1





$< \delta$



4x4

The final algorithm

P_x: sorted in x order
P_y: " " y order

closestpair2D (P)
construct P_x and P_y — $O(n \log n)$
(p_0^*, p_1^*) = closest-pair-rec (P_x, P_y) — $O(n \log n)$

closest-pair-rec (P_x, P_y) — $T(n)$
= base condition. = $\Theta(1)$

Q: first $n/2$ points in P_x
$R \leftarrow$ remaining points in P_x

Q_x: Q sorted in x direction
Q_y: Q " " y "
R_x: R " " x direction
R_y: R " " y "

construct Q_x, Q_y, R_x, R_y — $O(n)$
(q_0^*, q_1^*) — closestpairrec (Q_x, Q_y) — $T(n/2)$
(r_0^*, r_1^*) — " " " (R_x, R_y) — $T(n/2)$
$\delta = \min \{ d(q_0^*, q_1^*), d(r_0^*, r_1^*) \}$ — $\Theta(1)$
$x^* =$ max x-coordinate of a point in Q — $\Theta(1)$
$L = \{(x, y) \mid x = x^*\}$
$S =$ points in P within δ distance of L — $O(n)$

construct S_y — $O(n)$

for each point $s \in S_y$

compute distances from s to each of the next 15 points in S_y — $O(n)$

let δ_{12} be minimum

$$\delta_{12} = d(q_2^*, r_2^*)$$

If $d(q_1^*, r_1^*) < \delta$ then

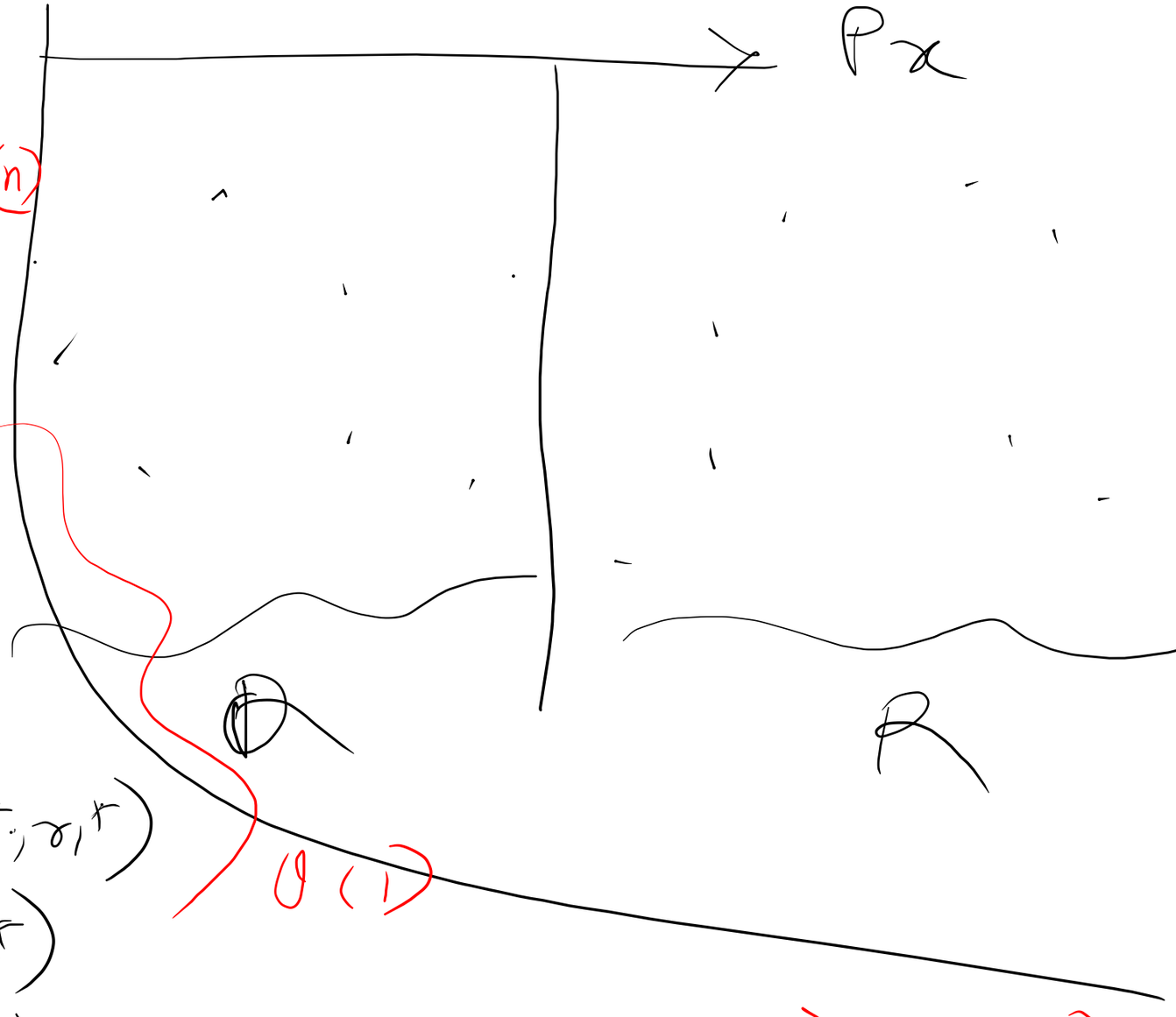
return (q_2^*, r_2^*)

else if $d(q_0^*, q_1^*) < d(r_0^*, r_1^*)$

return (q_0^*, q_1^*)

else

return (r_0^*, r_1^*)



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

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

Dynamic Programming

Divide and conquer:

- Divide the subproblem into independent subproblems.
- solve each subproblem independently
- combine the solutions.

Dynamic Programming

- Divide the subproblem into a series of overlapping subproblems.
- solve them ⟸ need extra care
- combine the solutions.

Dynamic Programming: It solves optimization problems.

Main idea

- compute the solutions to the subproblems once
- Store the solution of the subproblems in a table / dictionary
- They can be reused (repeatedly) in a later stage.

⟹ It trades space for time

Rod cutting problem

Input: A rod of length n unit.

A table of prices p_i for $i = 1, 2, \ldots, n$

where p_i is the price of a rod of length i

Goal: Find the maximum revenue

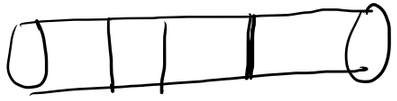
cut the rod into different pieces and sell it.

Ex^m

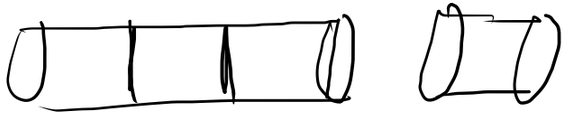
length i	1	2	3	4	5	6	. . . .
price p_i	1	5	8	9	10	17	

The shop owner has a rod of length 4

Solution



9

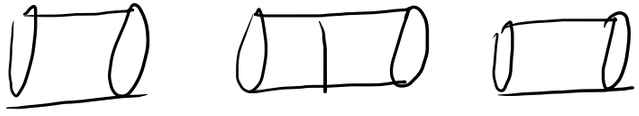


8 + 1

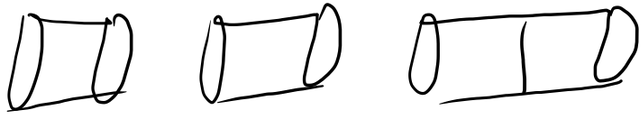
1 + 8

5 + 5

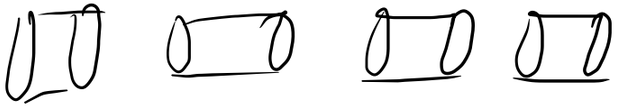
5 + 1 + 1



1 + 5 + 1

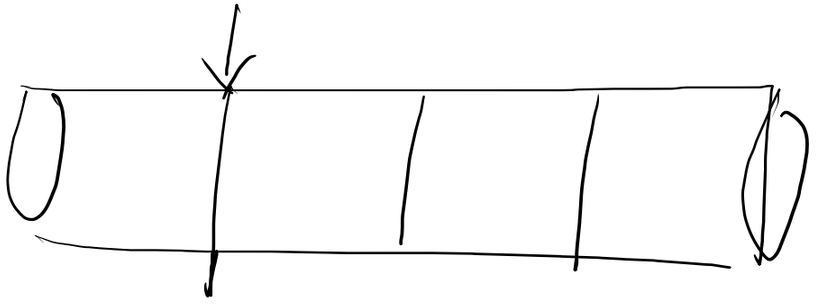


1 + 1 + 5



1 + 1 + 1 + 1

A simple algorithm



- Try all possible cuts of the rod
- Track the best solution.

running time :- $2^{n-1} \approx O(2^n)$

can we do better?

maximum revenue = r_n

$r_i \leftarrow$ maximum revenue for a rod of length i

$$r_n = \max\{p_n, r_1 + r_{n-1}, r_2 + r_{n-2}, \ldots, r_{n-1} + r_1\}$$

In general:

- making an initial cut into two pieces of length i and $n-i$
- optimally cutting these two pieces
- we donot know ahead of time which initial cut gives the optimum revenue.
- we have to consider all possible value for i and pick that with the maximum revenue.

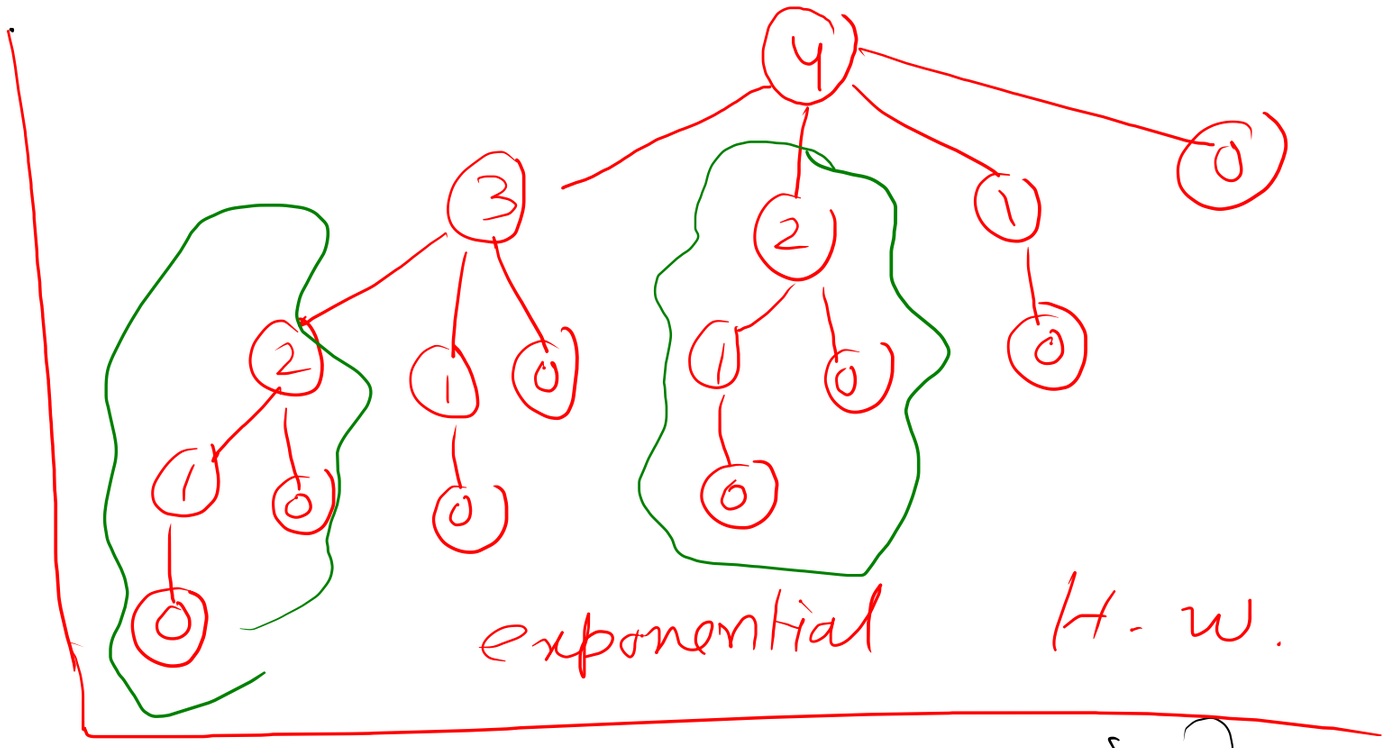
$$r_n = \max \{ p_n, r_1 + r_{n-1}, r_2 + r_{n-2}, \ldots, r_{n-1} + r_1 \}$$

Question:
Do we really need two subproblems?

$$r_n = \max_{1 \le i \le n} \{ p_i + r_{n-i} \}$$

Algorith rod cutting

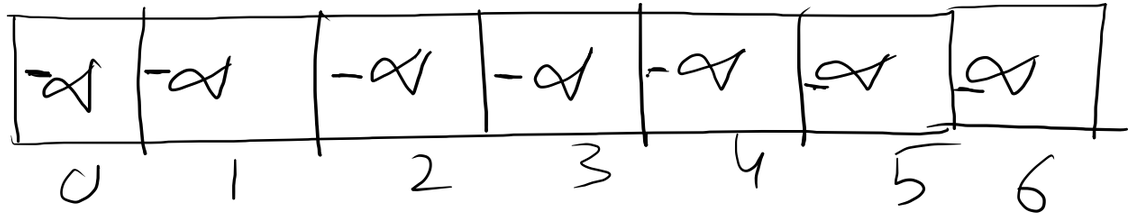
```
rod-cut (P, n)
  if  n == 0
      return 0

  q = -∞
  for i = 1 to n
      q = max { q, P[i] + rod-cut (P, n-i) }

  return q
```



Problem: several subproblems are called many times.

Top-down approach

r




```
memoized-rod-cut(P, n)
  let r[0,..,n] be a new array
  for i = 1 to n
      r[i] ← -∞
  return memoized-rod-cut-aux(P, n)
```

```
memoized-rod-cut-aux(P, n)
  if r[n] ≥ 0
      return r[n]
  if n == 0
      q = 0
  else
      q = -∞
      for i = 1 to n
          q = max{ q, P[i] + memoized-cut-rod-aux(P, n) }
  r[n] = q
  return q
```

running time

# of independent subproblems

× time taken without recursive call

Two ways to solve the problem

1. Top-down with memoization
2. Bottom up with tabulation

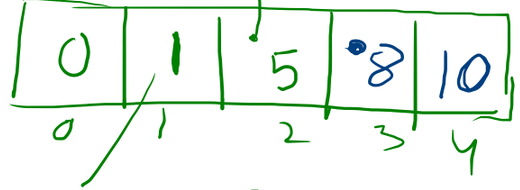
Rod cutting problem Bottom-up approach.

Idea: It solves the subproblems from 0 to n iteratively and store them in a table / dictionary / hash table.

```
Bottom_up_rod_cut(p, n)
let r[0,...,n] be a new array
r[0] = 0
for j = 1 to n
    q = -∞
    q = max_{1≤i≤j} { q, p[i] + r[j-i] }
    s[j] = i // ← this is the i which gives the maximum q
    r[j] = q
return r[n]
```

i	1	2	3	4
p_i	1	5	8	9

$n = 4$



$p[1] + r[0] = 1$

$p[1] + r[1] = 2$

$p[2] + r[0] = 5 \Leftarrow$

$p[3] + r[0] = 8$

$j = 4$ for $i = 2$

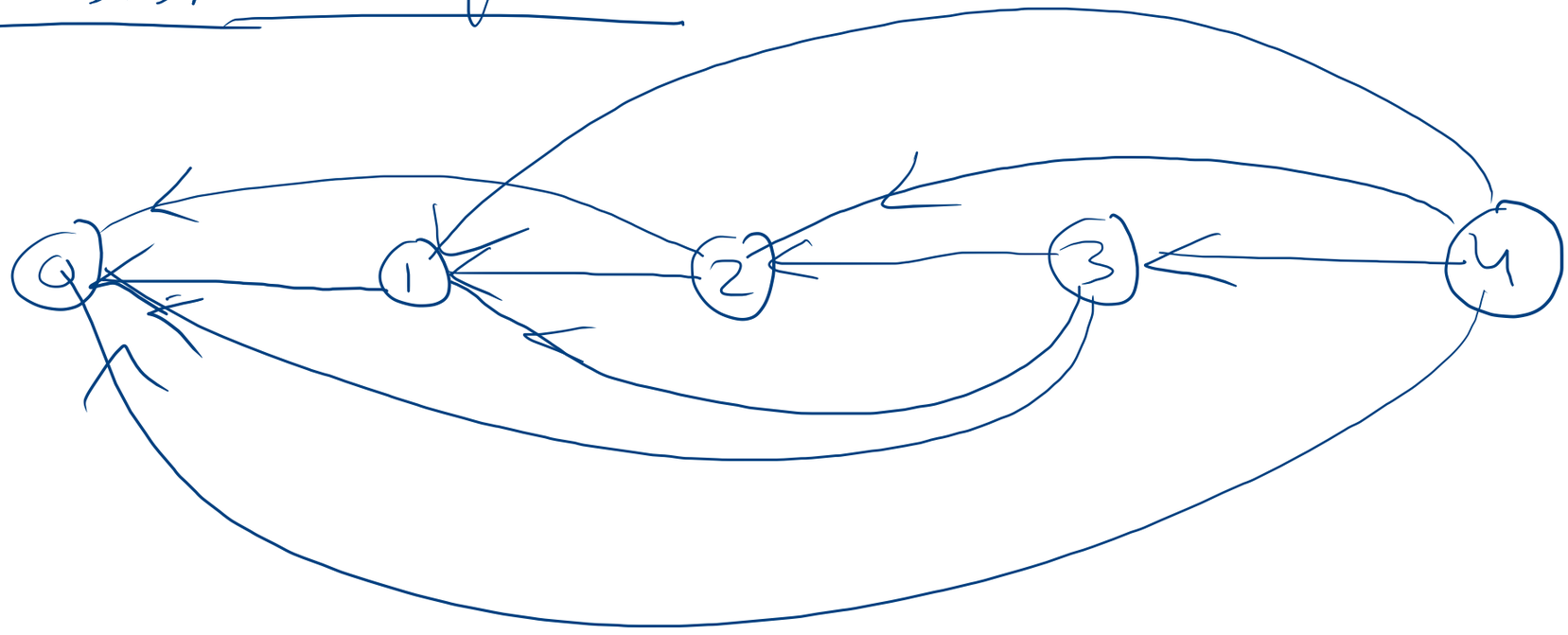
$j = 3$ for $i = 3$

$j = 2$ for $i = 2$ max

s: | 0 | 1 | 2 | 3 | 2 |

Running time: $O(n^2)$ — two for loops

The subproblem graph



construction of a solution

```
Print_rod_cut (P, n)
(r, s) = Bottom-up-rod-cut (P, n)
while n > 0
        Print s[n]
        n = n - s[n]
```

For $n = 4$,

Print gives the solution as 2, 2

General outline of a DP problem

Step 1 :- Structure

Characterize the structure of an optimum solution.
by showing that it can be decomposed into optimum subproblems.

Step 2 Recursive

Recursively define the value of an optimum solution by expressing it in terms of optimum solution for smaller subproblems.

Step 3: Optimum value computation

Two approaches

i) Top-down with memoization

ii) Bottom-up with tabulation.

Step 4: optimum solution computation

Step 4 only requires when one ask for finding an optimum solution.

Some time additional information is maintained during steps 1–3 to easily construct an optimum solution.

Fibonacci number

1, 2, 3, 5, 8, 13, 21, . . .

Step 1 If optimally compute previous 2 terms then you can optimally compute that number. by summing the previous two numbers.

Step 2.

$$F_n = \begin{cases} 1, & \text{if } n = 1 \\ 2 & \text{if } n = 2 \\ F_{n-1} + F_{n-2} & \text{if } n \geq 3 \end{cases}$$

```
fibonacci (n)
let F be an array.
if n = 1
    return 1
if n = 2
    return 2
for i = 3 to n
    F[n] = F[n-1] + F[n-2]
return F[n]
```

```
fib (n)
  if n = 1
      return 1
  if n = 2
      return 2
  for i = 3 to n
      return fib(n-1) + fib(n-2)
```

Logest common subsequence (LCS)

Subsequence:

A B B C B A B

then B C B B is a subsequence

- A sequence whose order is same as in the given sequence.
- They may not be consecutive.

Common subsequence:

X = B A A B C B A B C

Y = A B B C B A C

A B B B C

A B C B A C

longest.

A sequence that is subsequence to both x and y.

ABC is a common subsequence.

Logest: A common subsequence whose length is largest possible.

A simple algorithm

X, Y $\quad |Y| < |X| \quad |Y| = n$, $|X| = m$

consider all possible subsequences of Y

compare with X whether any of the subsequence is common to X

return the largest one.

running time : $O(m \cdot 2^n)$

$X = x_1 x_2 \cdots x_m$

$Y = y_1 y_2 \cdots y_n$

$X_i = x_1 x_2 \cdots x_i$

$Y_j = y_1 y_1 \cdots y_j$

Z be a LCS of X and Y

$Z_K = z_1 z_2 \cdots z_K$

$x_m = y_n$

z_K is a member of LCS of X and Y

Z_{K-1} is a LCS of X_{m-1} and Y_{n-1}

$x_m \neq y_n$

$z_K \neq x_m$

Z_K is a LCS of X_{m-1} and Y_n

$z_K \neq y_n$

Z_K is a LCS of X_m and Y_{n-1}

Recursive definition

$c[i\ j] \leftarrow$ optimum length of an LCS for X_i and Y_j

$$c[i,j] = \begin{cases} 0 & \text{when } i = 0 \text{ or } j = 0 \\ c[i-1, j-1] + 1 & \text{if } i, j > 0 \text{ and } x_i = y_j \\ \max\{c[i-1, j], c[i, j-1]\} & \text{if } i, j > 0 \text{ and } x_i \neq y_j \end{cases}$$

Compute the value of the optimum solution

```
LCS-length (X, Y)
m ← length(X) , n ← length(Y)
let C[0..m, 0...n] be a new table
let B[0..m, 0..n] be a new table.
for i = 1 to m
        C[i,0] = 0
for j = 1 to n
        C[0,j] = 0
for i = 1 to m
    for j = 1 to n
        if x_i = y_j
            C[i,j] = C[i-1,j-1] + 1
            b[i,j] = "↖"
        else if C[i-1, j] ≥ C[i, j-1]
            C[i,j] = C[i-1, j]
            b[i,j] = "↑"
        else
            C[i, j] = C[i, j-1]
            b[i, j] = "←"
return C, b
```

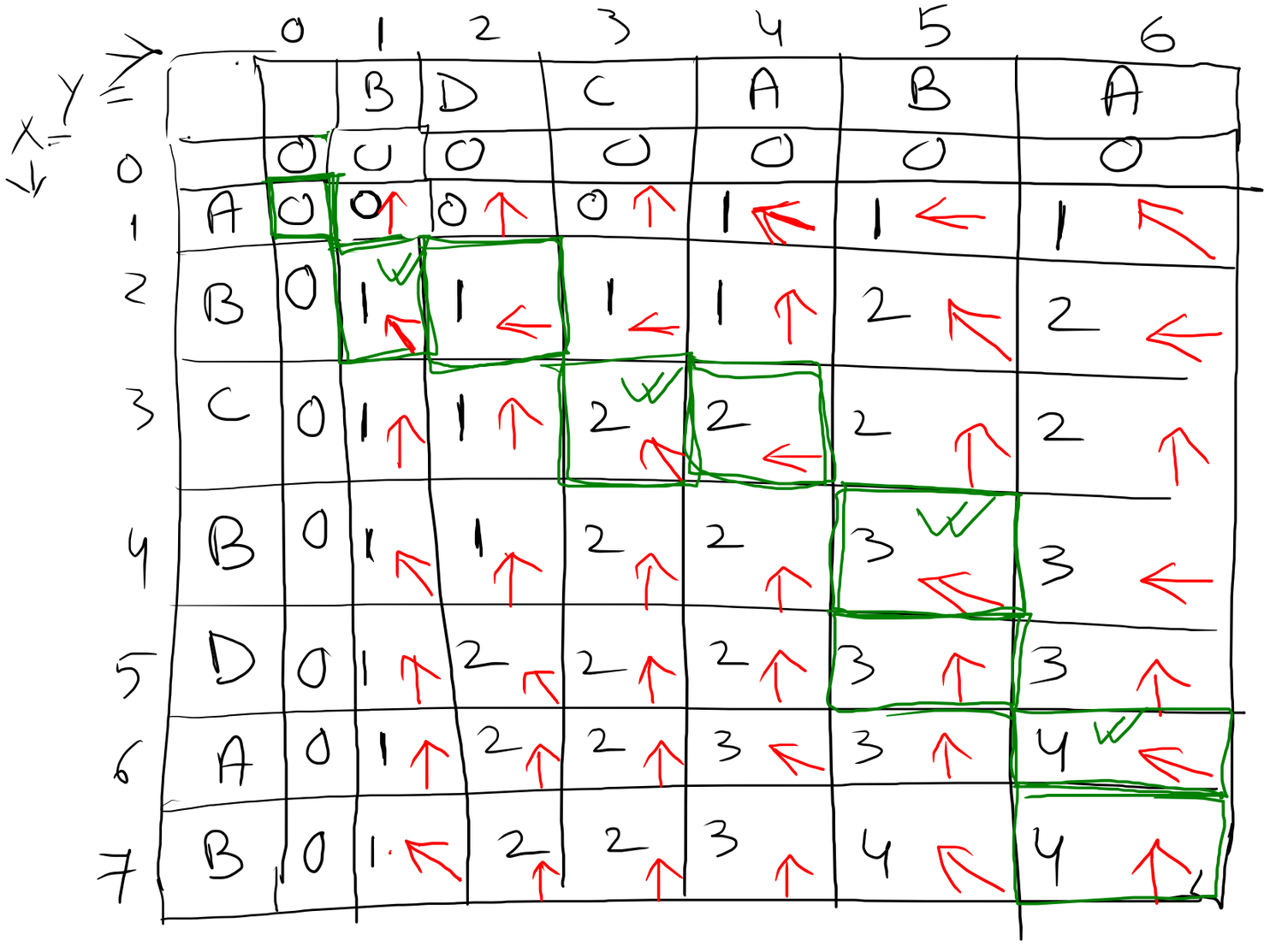
Running time:

$O(mn)$

Ex^m

X = A B C B D A B

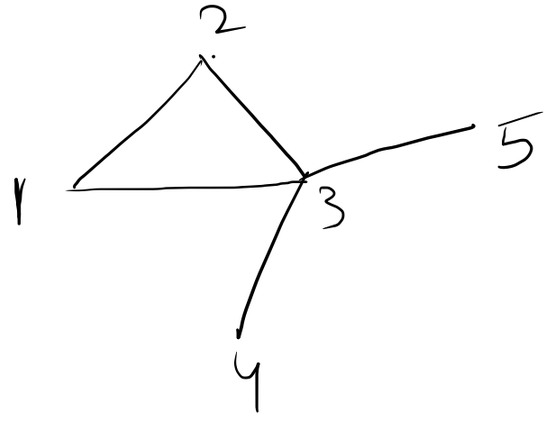
Y = B D C A B A

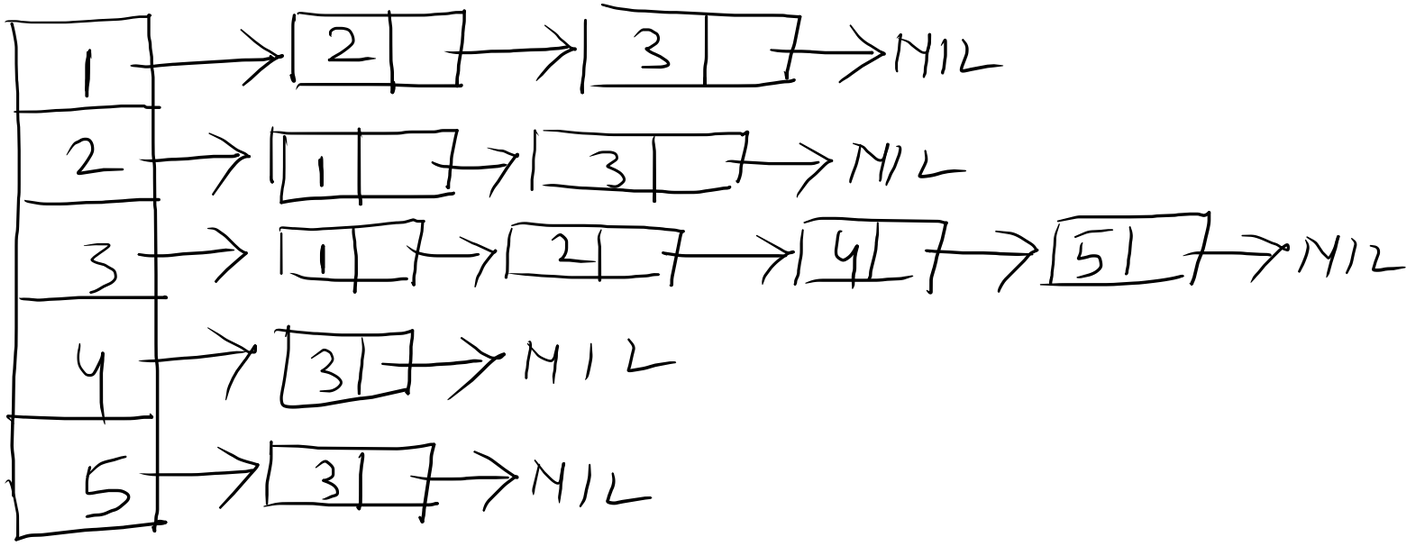


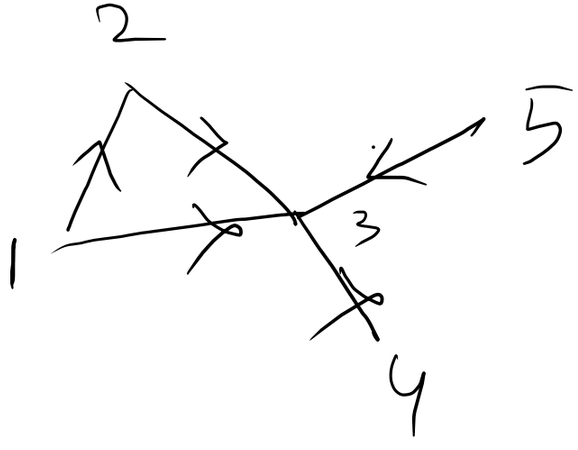
BCBA

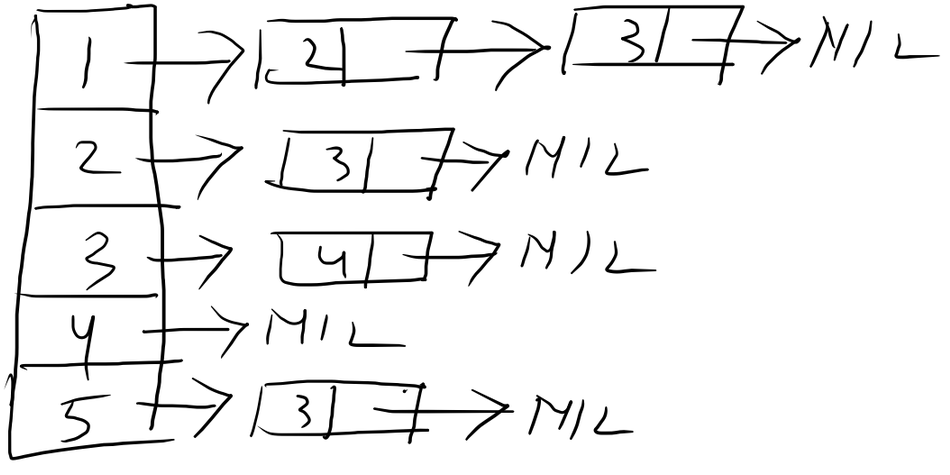
Representations of graphs

Adjacency - List









Storage

$O(|V| + |E|)$

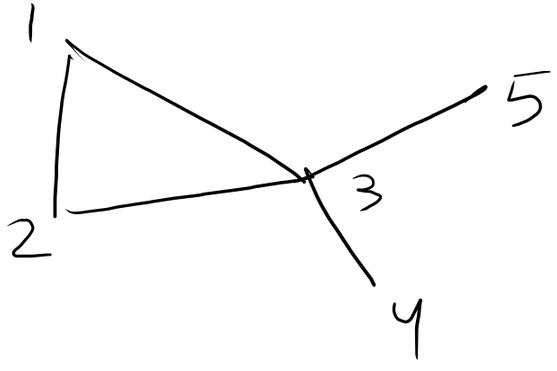
Adjacency matrix

storage: $O(|V|^2)$

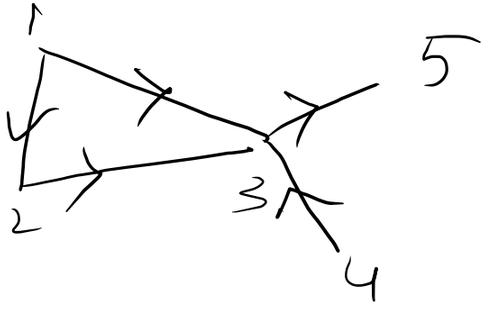
$v_1, v_2, \ldots, v_n$.

$A_{n \times n}$

$$a_{ij} = \begin{cases} 1 & \text{if } v_i \text{ is connected with } v_j \\ 0 & \end{cases}$$



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

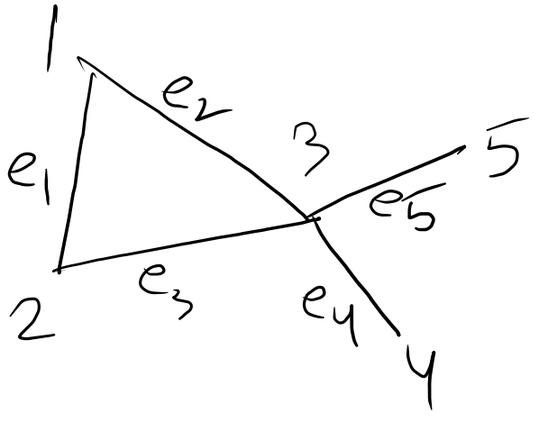


	1	2	3	4	5
1	0	1	1	0	0
2	0	0	1	0	0
3	0	0	0	0	1
4	0	0	1	0	0
5	0	0	0	0	0

Incidence matrix

$A_{n \times m}$

$$a_{ij} = \begin{cases} 1 & e_i \text{ is incident on } j\text{-th vertex} \\ 0 & \text{otherwise} \end{cases}$$



	e_1	e_2	e_3	e_4	e_5
1	1	1	0	0	0
2	1	0	1	0	0
3	0	1	1	1	1
4	0	0	0	1	0
5	0	0	0	0	1

storage:

$O(|V||E|)$

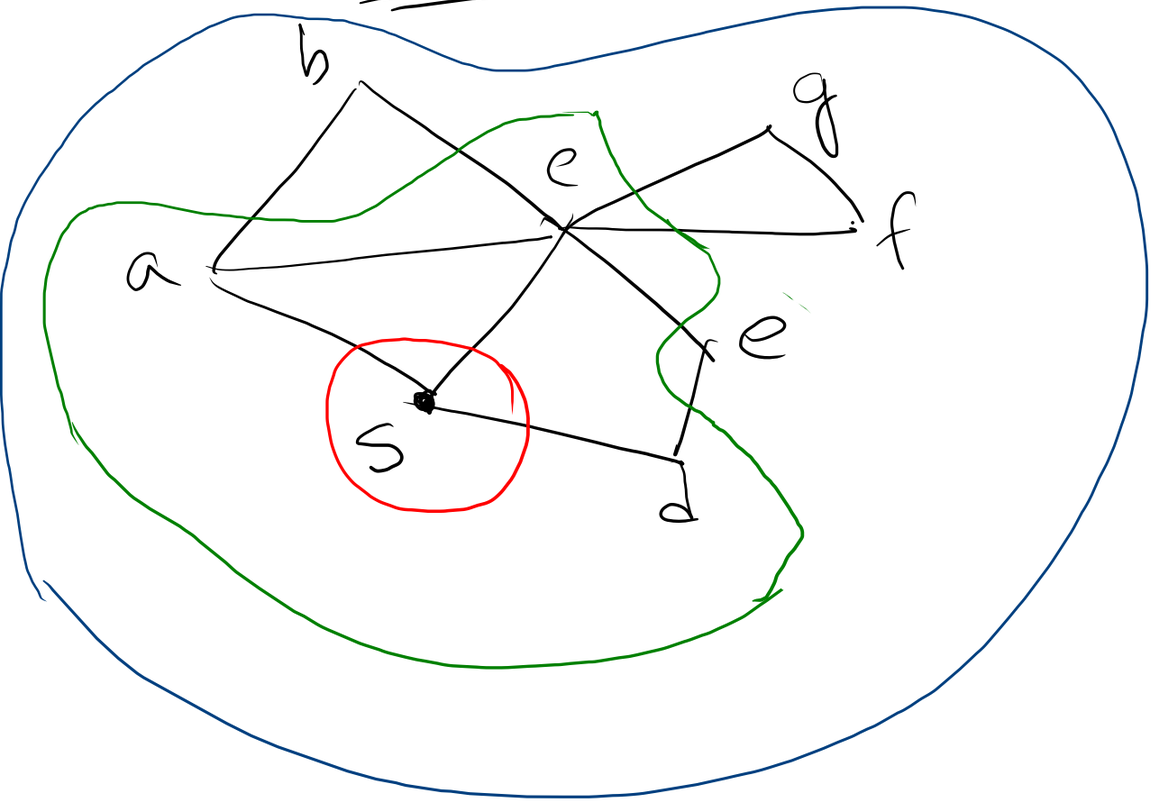
Graph searching algorithms

- systematic searching of each edge or vertices of the graph.
- For directed or undirected graph.
- Applications.
  - maze search.
  - connected compond.

Two popular algorithms.

i) BFS
ii) DFS

BFS



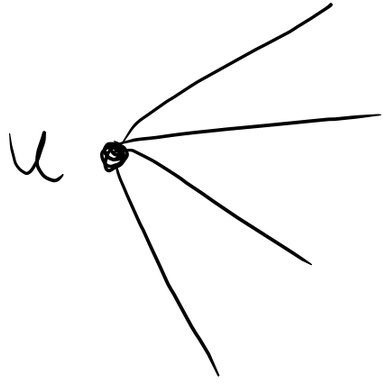
White: This vertex is not yet discovered.

Gray: It is discovered. but not all its neighbours are discovered.

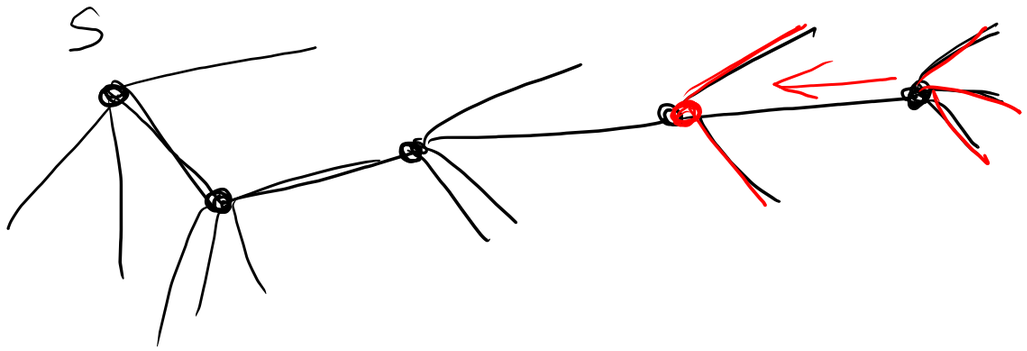
Black: Already discovered and all its neighbours are discovered.

```
BFS (G, s)
for each u ∈ G.V
        u.color = white
        u.dist  = ∞
        u.pred  = NIL
s.color = gray
s.dist = 0
Q = new queue
Q.enqueue(s)
while Q is not empty.
        u = Q.dequeue()
        for v ∈ u.adj
                if v.color = white
                        v.color = gray
                        v.dist = u.dist + 1
                        v.pred = u
                        Q.enqueue(v)
        u.color = black.
```

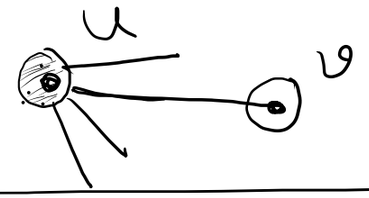
Running time: $O(|V| + |E|)$

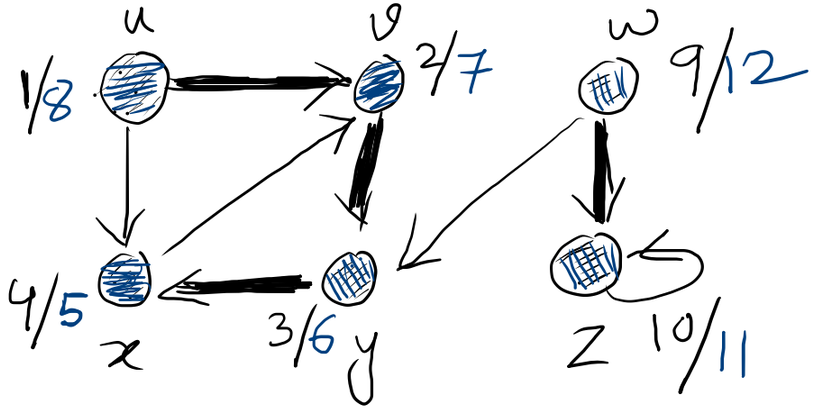


Depth First Search (DFS)



```
DFS(G)
  for each vertex u ∈ G[V]
        u.color = white
        u.Pred = NIL
  time = 0
  for each vertex u ∈ G[V]
        if u.color = white
              DFS-visit(u)

DFS-visit(u)
  u.color = gray
  time = time + 1
  u.starttime = time
  for v ∈ Adj[u]
        if v.color = white
              v.pred = u
              DFS-visit(v)

  u.color = black
  time = time + 1
  u.endtime = time
```





Total time: $O(|V| + |E|)$

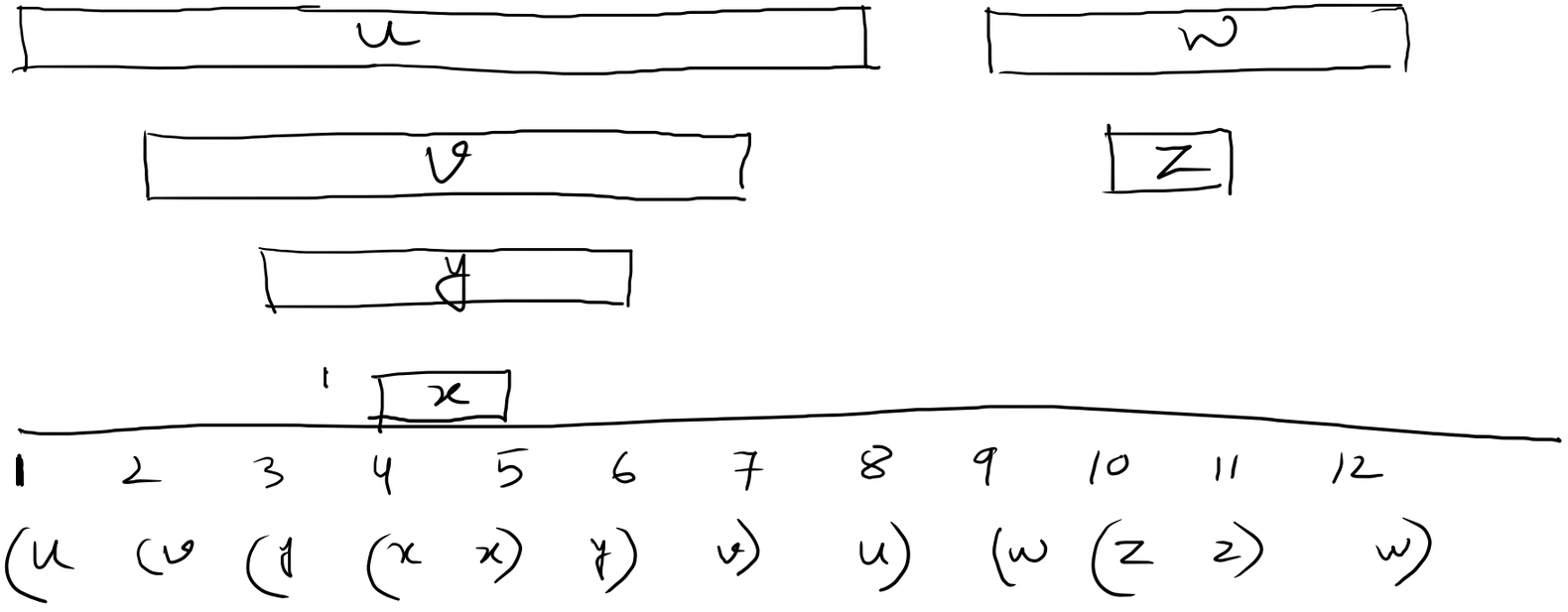
Properties

Parenthesis theorem

(( )) X

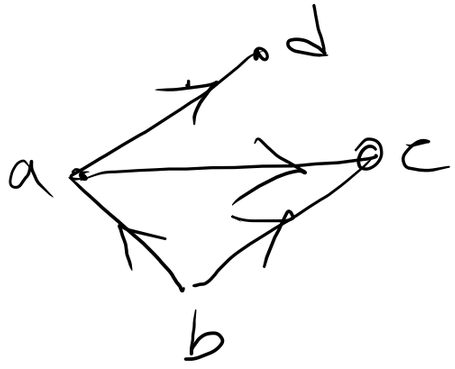
( ) ( ) (( ))

In previous example

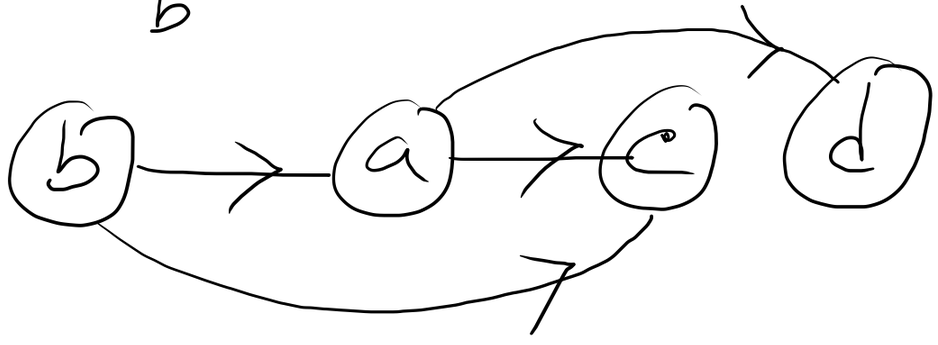


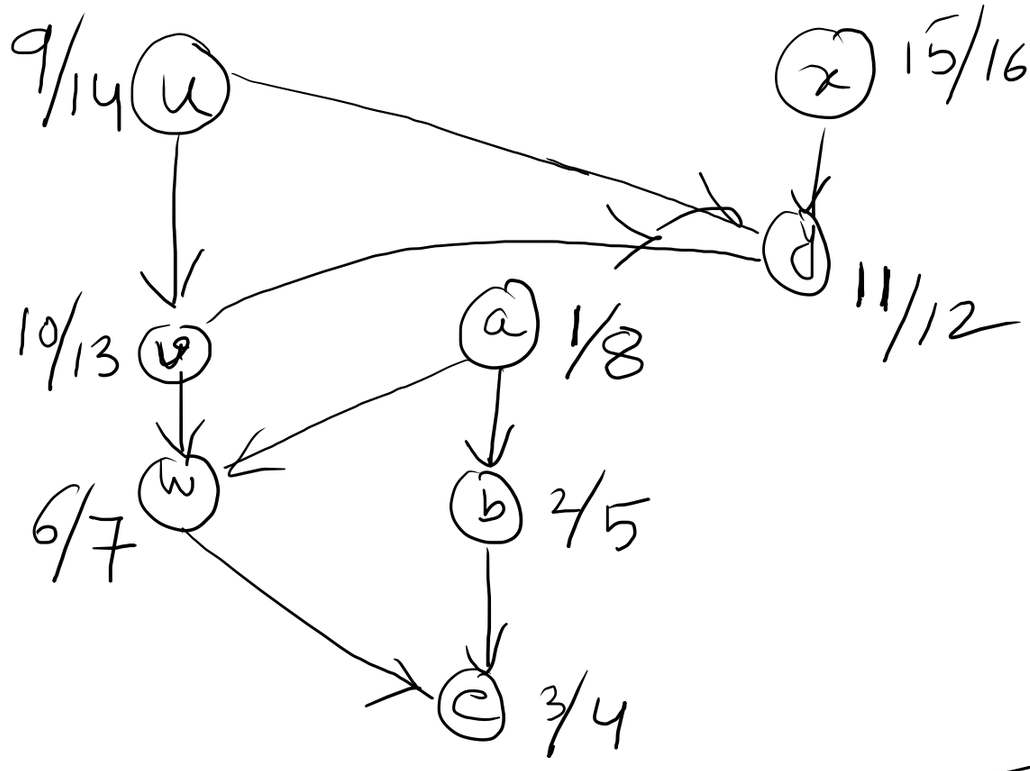
Topological sorting for DAG Directed Acyclic Graph.

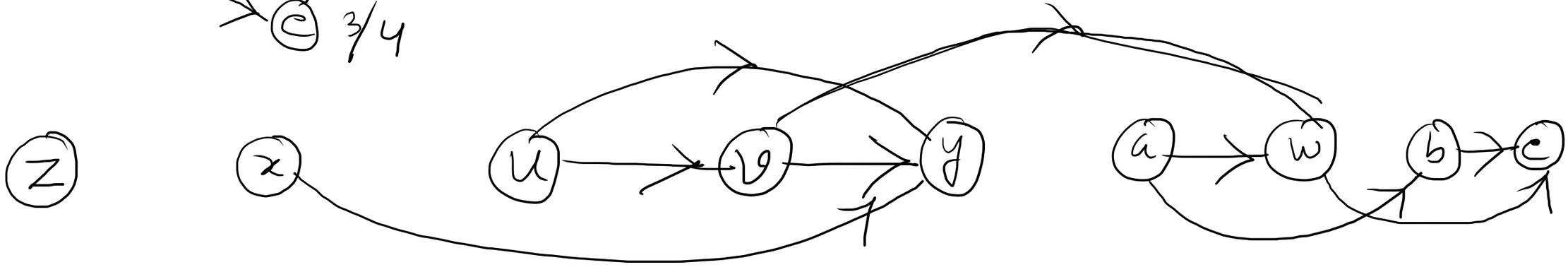
A topological sorting of a DAG $G(V,E)$ is a linear order of all its vertices such that if (u,v) be an edge in G then u appears before v in the order.



Topological-sort(G)
- Run DFS(G)
- As each vertex finish, insert it in a front of a queue
- return the queue.




9/14
u
x
15/16
z
17/18
y
11/12
10/13
v
a
1/8
w
6/7
b
2/5
c
3/4


z
x
u
v
y
a
w
b
c

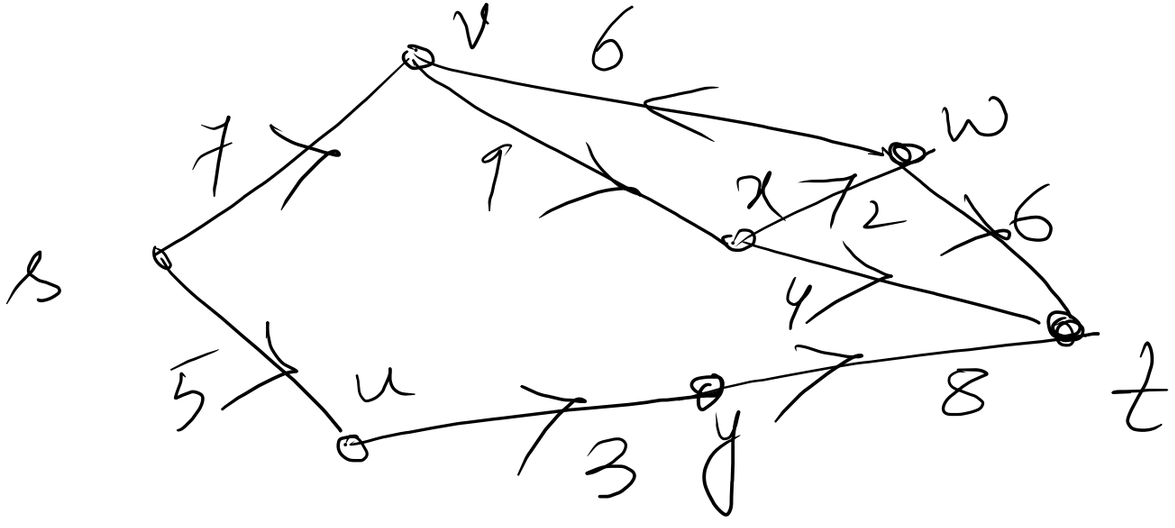
Network-Flow Problem

Flow network : Input: $G = (V, E)$, s, t, $c : E \to \mathbb{R}^+$

A directed graph G

s : source t : sink

For each edge $e \in E$ $c(e) \geq 0$ called the capacity of the edge.



Maximum flow problem

An $s-t$ flow f that satifies the following two conditions / constraints.

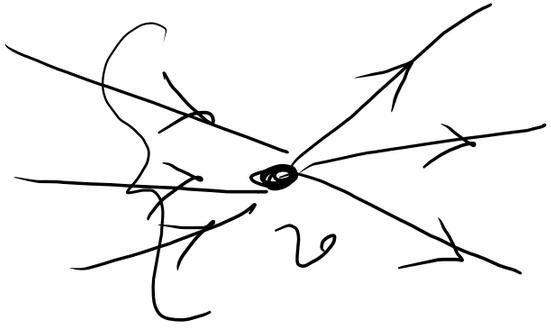
① capacity constraint:

for each edge $e \in E$, $0 \le f(e) \le c(e)$

② flow conservation constraint

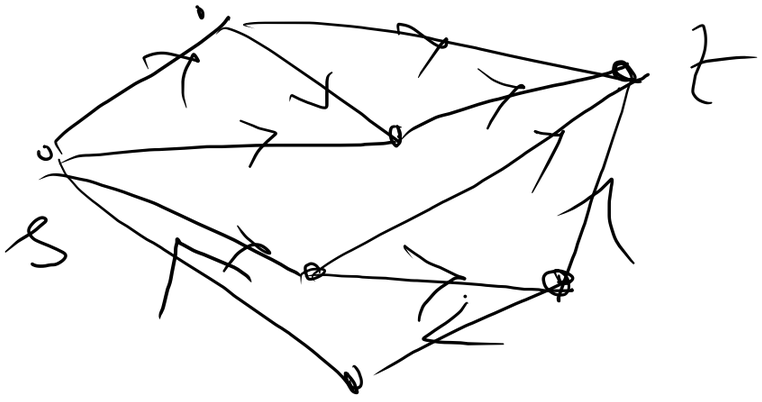
for each vertex $v \in V \setminus \{s, t\}$

$$\sum_{\substack{e \text{ is incident} \\ \text{towards } v}} f(e) = \sum_{\substack{e \text{ is incident} \\ \text{outward } v}} f(e)$$

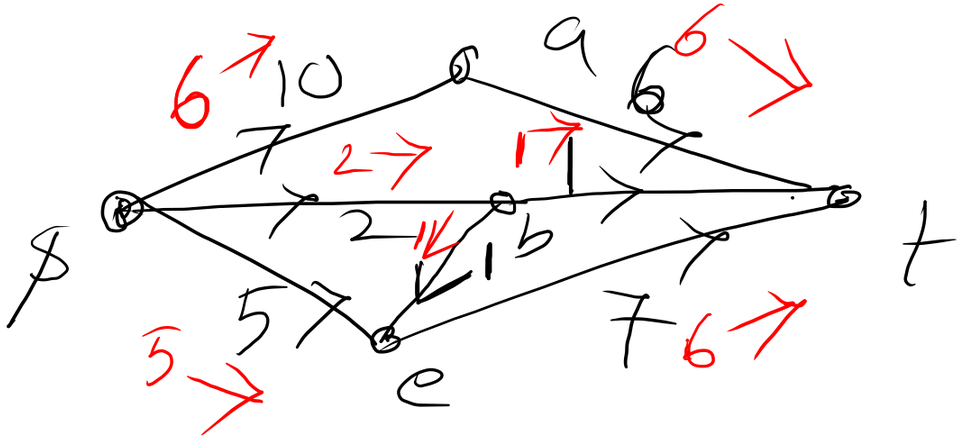


The value of the flow

$$val(f) = \sum_{\substack{e \text{ is going} \\ \text{out of } s}} f(e) - \sum_{\substack{e \text{ is going} \\ \text{inside } s}} f(e)$$

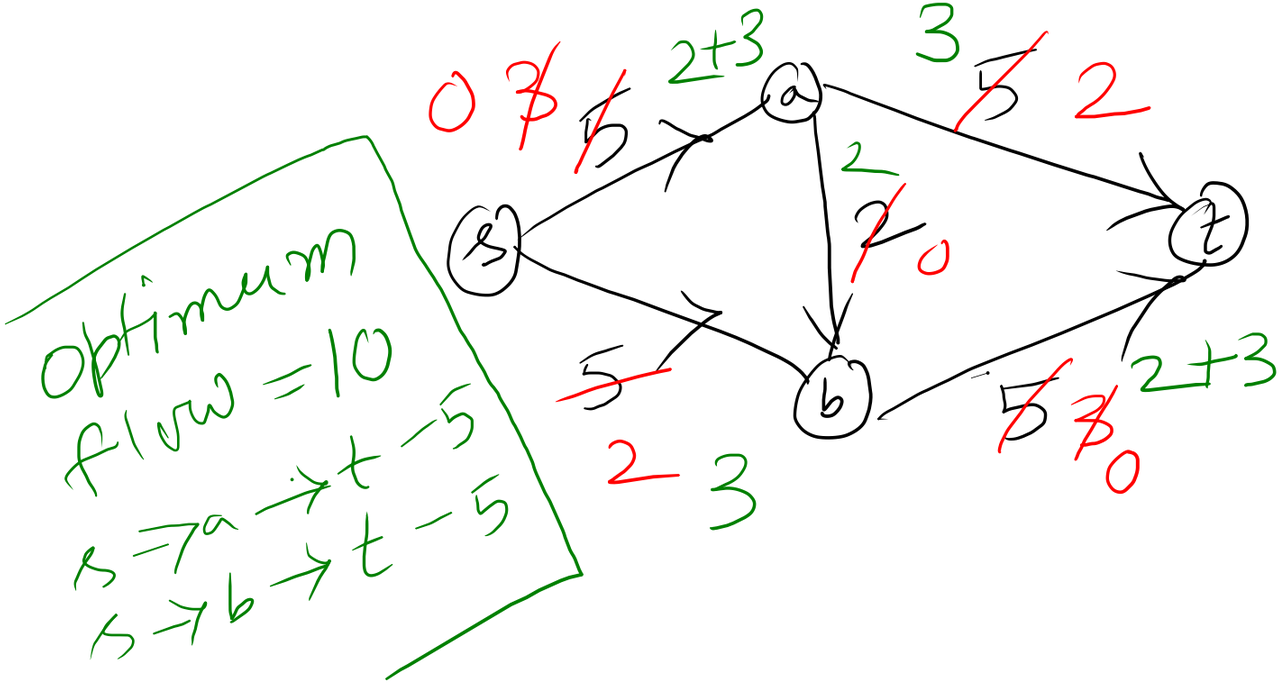


Objective: Find a flow of maximum value.



An algorithm

- for each edge flow is 0 ie $f(e) = 0$
- if there is a $s \to t$ path where $f(e) < c(e)$
- augment flow along the $s \to t$ path
- Repeat until no $s \to t$ path exist.



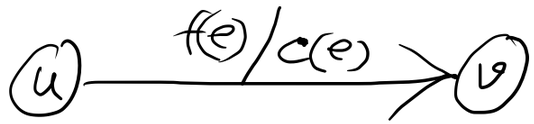
$s \to a \to b \to t \to 2$

$s \to a \to t \quad - 3$

$s \to b \to t \quad - 3$

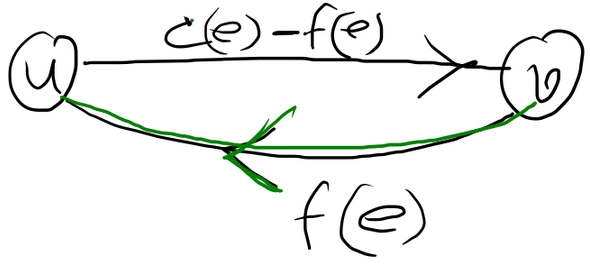
Total flow = 8

Residual network



Residual capacity

$$c_f(e) = \begin{cases} c(e) - f(e) & \text{if } e \in E \\ f(e^{reverse}) & \text{if } e^{reverse} \in E \end{cases}$$



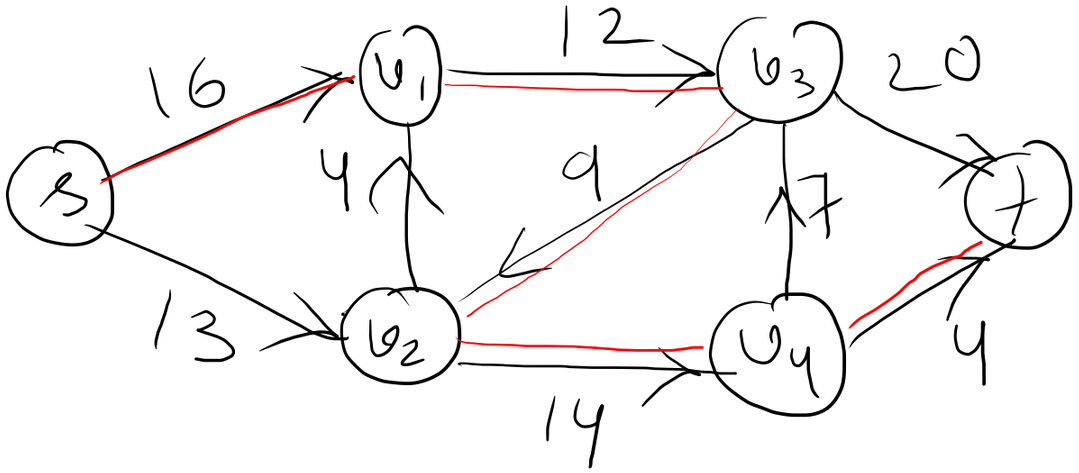
Residual network: $G_f(V, E_f)$, s, t, c_f is residual capacity function.

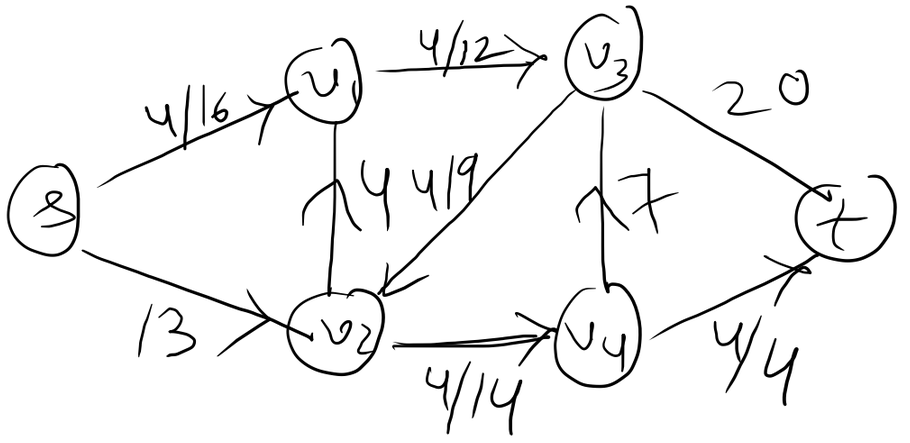
$$E_f = \{ e : f(e) < c(e) \} \cup \{ e : f(e^{reverse}) > 0 \}$$

Ford-Fulkerson algorithm

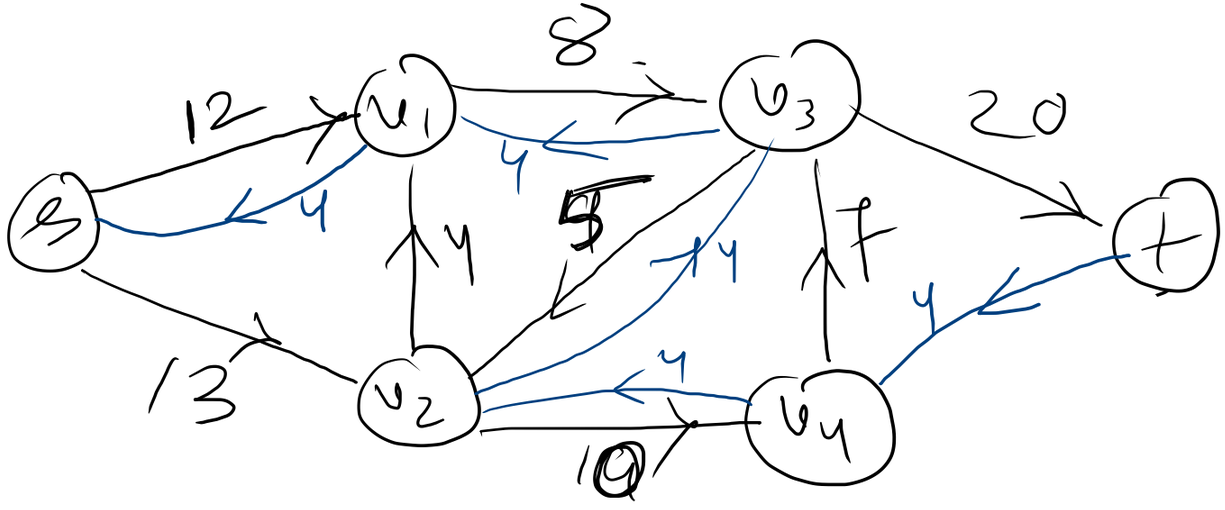
```
Ford-Fulkerson(G)
    for each edge e ∈ E
        f(e) = 0
    G_f ← residual network of G w.r.t. f
    while there is an s ⇝ t path P in G_f
        f ← augment(G, P, c)
        update G_f
    return f.
```

```
augment(G, P, c)
    δ ← bottleneck capacity in P
    for each edge e in P
        if e ∈ E
            f(e) ← f(e) + δ
        else
            f(e^reverse) = f(e^reverse) − δ
    Return f.
```





$s \to v_1 \to v_3 \to v_2 \to v_4 \to t$



Running time of Ford-Fulkerson

initialization — $O(|E|)$

Find residual path $O(|V|+|E|)$

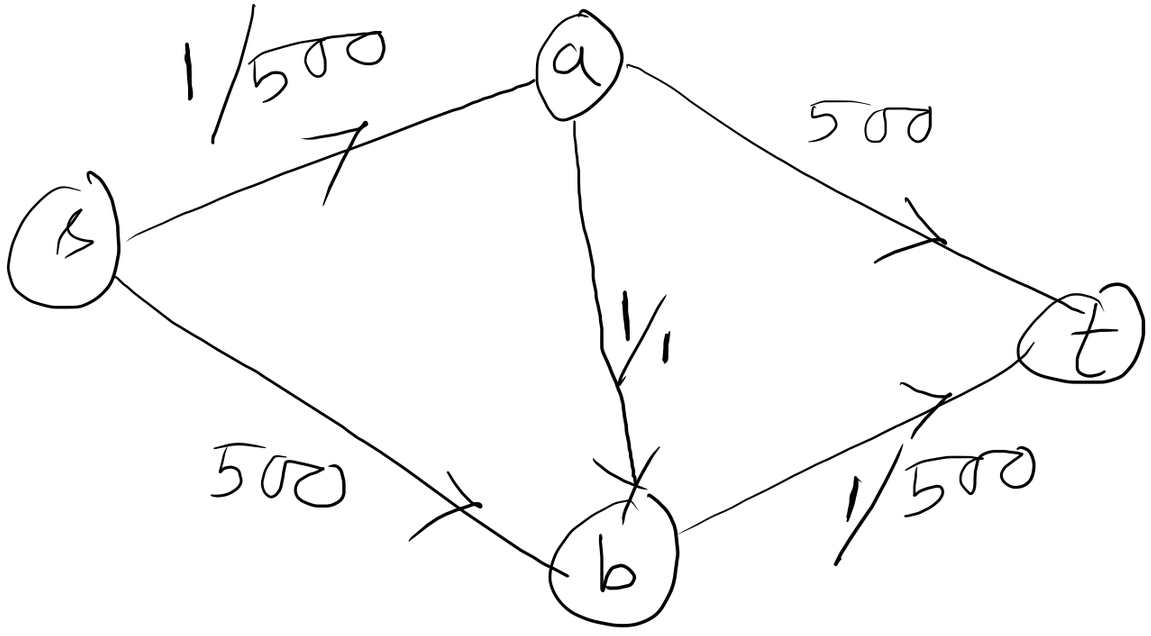
Bottleneck - capacity : $O(|E|)$

update the flow : $O(|E|)$

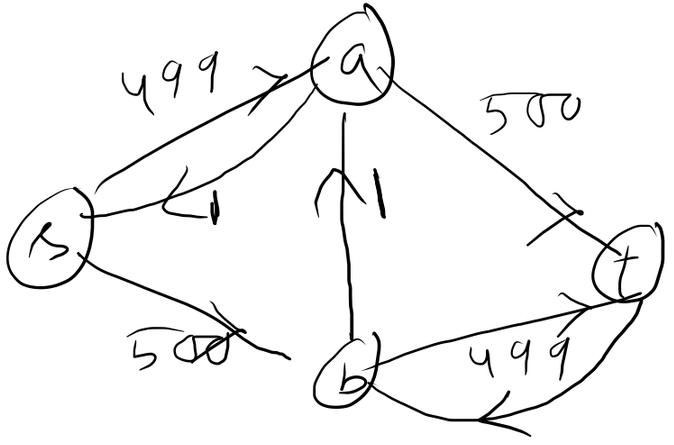
update residual graph : $O(|E|)$

Let # Augment operations is C

Total time : $O(C(|V|+|E|))$



$s \to a \to b \to t$



$s \to b \to a \to t$

Here c is $|f^*|$

- integer array $A[1 \ldots n]$
- Find indices i and j, $i < j$
  $A[i] - A[j]$ minimum.

Brute force

- consider each pair i, j such that $i < j$.
- Track the minimum of $A[i] - A[j]$.

$O(n^2)$

$A[1 \ldots n]$

A 5 2 9 6 3 1 4

create a new array B such that

$B[n] = A[n]$

for $i = n-1$ down to 1

$B[i] = \max(A[i], B[i+1])$

B

9	9	9	6	4	4	4

$min = -7$

$i = 2$

$K = 2$

$l = 3$

$min = \infty$

for $i = 1$ to $n-1$

$t = A[i] - B[i+1]$

if $t < min$ then

$min = t$

$K = i$

for $l = K+1$ to n

If $A[K] - A[l] == min$

return the pair (K, l)

A is a m×n matrix

1> element sorted rowwise

2> " " columnwise

Given x,

Find x in A.

5	9	16	20	25
6	12	18	25	32
9	13	25	29	35
13	29	36	41	45

Trivial: $O(mn)$

- Search all element one by one

Better Binary search each row: $O(m \log n)$

OR

" " column: $O(n \log m)$

$K == A[1][n]$

$K > A[1][n]$

Search $(A[2 \ldots m][1 \ldots n], K)$

$K < A[1][n]$

Search $(A[1 \ldots m][1 \ldots n-1], K)$

Running time : $O(m+n)$

1) Divide and conquer
2) Greedy
3) Dynamic Programming.

} Problems on these paradigms.

All studied algorithm takes $O(n^c)$ time. for some constants.

These problems have efficient algorithms.

Polynomial time.

Question: What happens when one cannot find an efficient algorithm for a problem?

→ Showing a problem has an efficient algorithm is relatively easier.

- one needs to design one algorithm.

→ Proving that no efficient algorithm exists for a particular problem is difficult.

Question: How can we prove the non-existance of something?

Two categories

Solvable

Some algorithm exists.

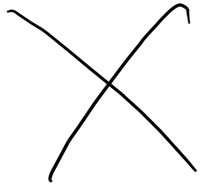
✓

$O(n^c)$

$O(2^n)$

Not solvable

No algorithm possible.



Halting problem.

NP- complete problem

- A thousands of problems for which
- It is not known whether the problems have efficient solutions or not.
- It is known that if any one of the NP- complete problems has an efficient solution that all of them have efficient solution
- There is a large number of tools exist to prove a new problem to be NP- complete.
- The problem of finding an efficient solution to an NP- complete problem is known as $P \neq NP$?

Million dollar question.

claymath.org

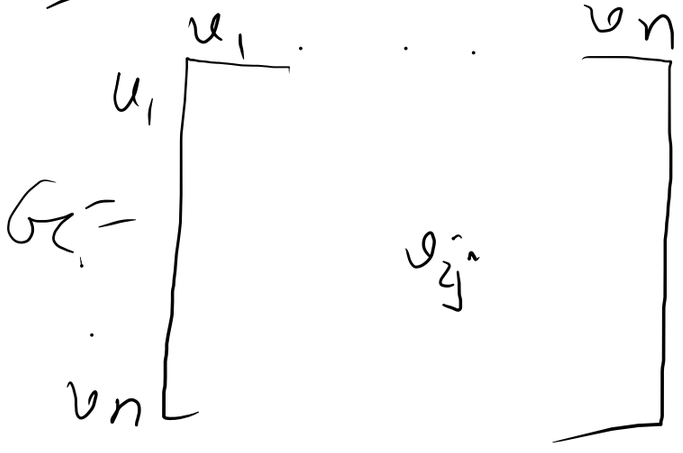
Input to a problem

n be the length/size of the input.

$f(n)$ its time complexity.

Encoding of the input:

Ex^m How a graph is encoded ? Adjacency matrix.



$a_{ij} \leftarrow$ binary string of v_{ij}

G_c can be encoded as.

$a_{11}\ a_{12} \ldots a_{1n}\ a_{21}\ a_{22} \ldots \ldots a_{nn}$

length of the string $n^2 \cdot b$ where $b = \max_{ij} |a_{ij}|$

In general: the input of any problem can be encoded as a binary string.

Input size: minimum number of bits $\{0,1\}$ needed to encode the input of the problem.

Exm Sorting problem

what is the input size.?

Problem a sequence of numbers $a_1, a_2 \ldots, a_n$

Rearrange to make these nondecreasing.

Input size: $b_i \leftarrow$ binary encoding of a_i:

$$k = \max_i |b_i|$$

Input size: $k \cdot n$

Integer multiplication

a, b $\quad a \times b$

Input size $\leq 2 \cdot n$ $\quad n = \max\{b_1, b_2\}$

Decision problems

Defn problems that have yes or no answer.

Optimization problems:

certain configurations need to be optimize

minimize maximize

Ex^m MST

optimization	Decision
• Given an edge weighted graph G	• G and an a number t
• Find a tree T that spans all the vertices of G	• - - - -
• Weight of T is minimum	• Decide whether the weight of the tree is at most t or not

H.W Find the maximum of 10 numbers.

Almost all optimisation problems can be converted to its corresponding decision problems.

Q:

An efficient algorithm is there for an optimization problem.

What about the efficiency of its corresponding decision problem.?

if optimization can be solved efficiently then decision version can also be solved efficiently.

contrapositive: Decision version not solved efficiently (hard to solve) then optimization version not solved efficiently (hard to solve)

yes input / instance
no input / instance

Ex^{n} Is $a+b=c$ for $a,b,c \in \mathbb{N}$?

(a,b,c)

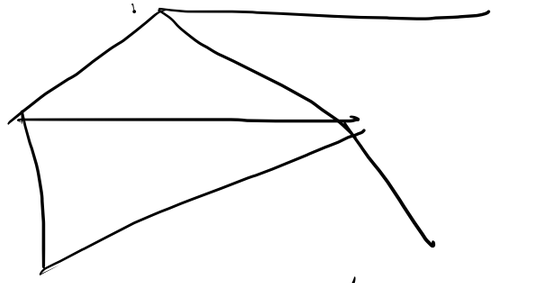
$(1,2,3)$ $\quad 1+2=3$ yes input

$(5\ 6\ 9)$ $\quad 5+6=9$ ✗ no input.

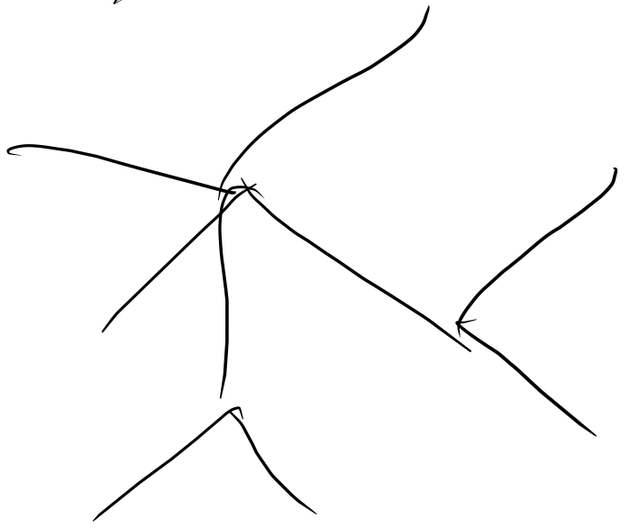
Defn An instance of a decision problem is called an yes instance if the answer to the instance is yes.

Otherwise if the answer is no it is a no instance.

Ex^m Does an undirected graph G contains a cycle?

F 

yes instance.



No instance

complementary problems

Let L be a decision problem then $\overline{L}$ is the decision problem such that yes-input of $\overline{L}$ are exactly the no-input of L.

Ex^m

composite: Is a given positive integer n is composite?

$$n = ab \quad \text{for} \quad 2 \leq a \leq b < n$$

Prime: Is a given number n is prime?

$\overline{\text{composite}} = \text{prime}$.

$\overline{\text{prime}} = \text{composite}$.

Property:

$$\overline{\overline{L}} = L$$

Polynomial-time algorithms

If an algorithm runs in $O(n^k)$ time where k is a constant independent of n.

n: input size

Ex^m matrix multiplication : $O(n^3)$

Remark: n or n^c or cn as input size for c: constant

$O(n^k)$ ≡ $O((n^c)^k) \equiv O(n^{ck})$

Ex^m MST : $O(m \lg n)$

Non-polynomial time algorithm.

running time is not $O(n^k)$

Exm Prime: Decide whether a positive integer I is a prime or not?

Algo:

for $i = 2$ to $\sqrt{I}$

check whether i devides I or not.

running time: $O(I^{1/2})$

Is this polynomial?

Input: I

Input size $n = \log I$

$\Rightarrow I = 2^n$

running time: $O((2^n)^{1/2})$

Polynomial v non-polynomial

running time of an algorithm is $O(2^n)$

but $n = 100$

A computer performs 10^{12} operations per second.

Time taken: $\frac{2^{100}}{10^{12}} \approx 10^{18.1}$ seconds.

$\approx 4 \cdot 10^{10}$ years.

Remark: for polynomial time algorithm large exponent is also impractical.

Polynomial-time algorithm $\Longrightarrow$ tractable.

The class P

class of all decision problems that are solvable in polynomial time.

Q: How to prove a decision problem is in P?

A: by designing a polynomial time algorithm.

Q: How to prove it is not in P?

No polynomial time algorithm exists.

certificate

Decision Problem

Is there an object that satisfying some condition?

- A certificate is a specif object corresponding to a yes-input such that it can be used to show the validity of that yes-input.

only yes-input needs a certificate.

Verifying a certificate

Given a yes-input and its corresponding certificate, by making use of this certificate one verify that the input is actually a yes-input.

The class NP

The class of all problems that can be verified in polynomial time.

NP :- Nondeterministic Polynomial

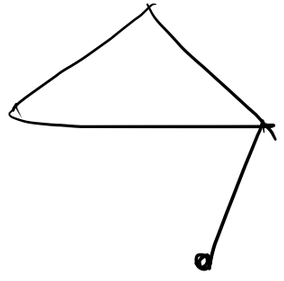
Exm Hamiltonian cycle problem (HC)

Input: An undirected graph $G(V, E)$

Output: Find a cycle that contains each vertex exactly once.

Decision version: (HC-D)

Does G contains a Hamiltonial cycle?



no Hamiltonial cycle exists.

no-input.

Show that HC-D is in NP.

certificate: An ordering of the vertices (corresponding to the ordering along a Hamiltonian cycle)

$$v_{i_1}, v_{i_2}, \ldots\ldots, v_{i_n}$$

verification:

check $v_{i_j} \neq v_{i_l}$ for $j \neq l$

check $(v_{i_j}, v_{i_{j+1}})$ is an edge in the graph

check (v_{i_n}, v_{i_1}) is an edge in " "

verification takes polynomial time

So HC-D is in NP.

Note: certificate is not unique.

Exm Vertex cover problem is in NP

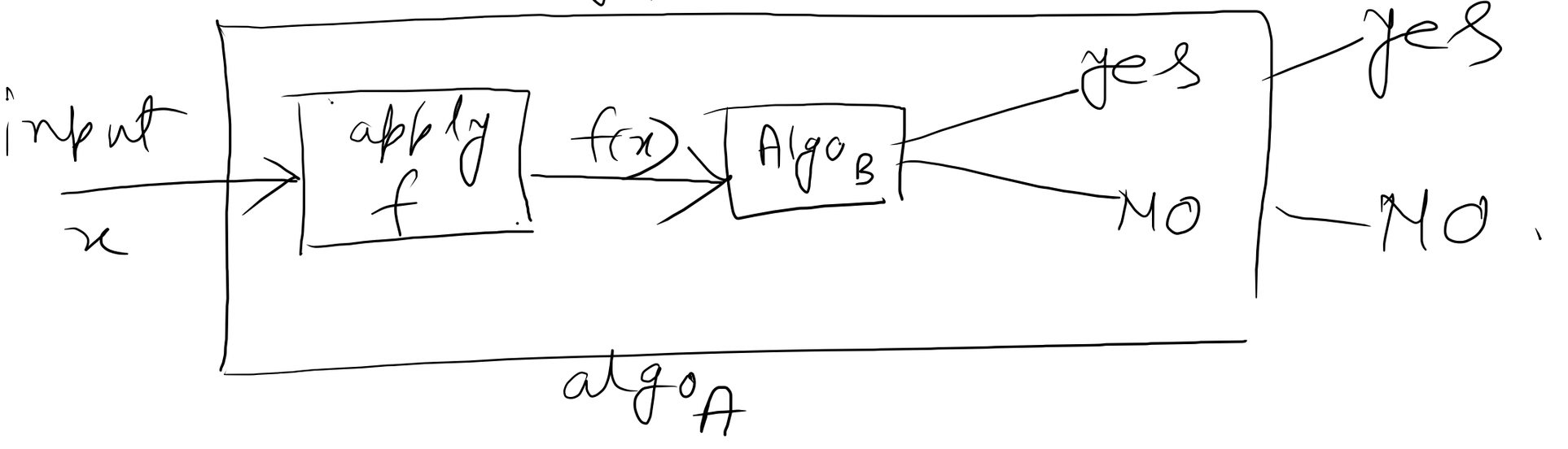
H.W.

Polonial time reduction

What is a reduction?

Let A and B be two decision problems.

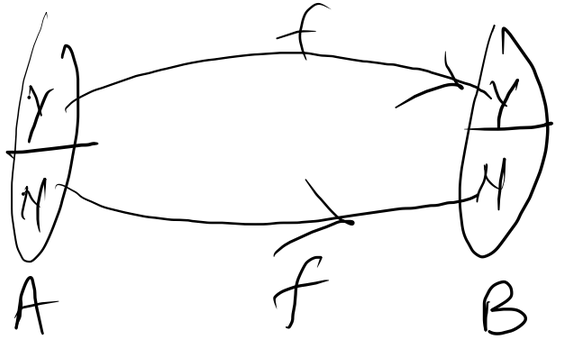
In reduction, we find a transformation f from A to B so that there will be algorithms $algo_A$ for solving A and $Algo_B$ for solving B and the algorithm $Algo_B$ can be a part of $Algo_A$ to solve A.



Polynomial time reduction

A polynomial time reduction from A to B is a transformation f such that:

- f transforms x of A into an instance f(x) of B and x is an yes-instance iff f(x) is an yes-instance.

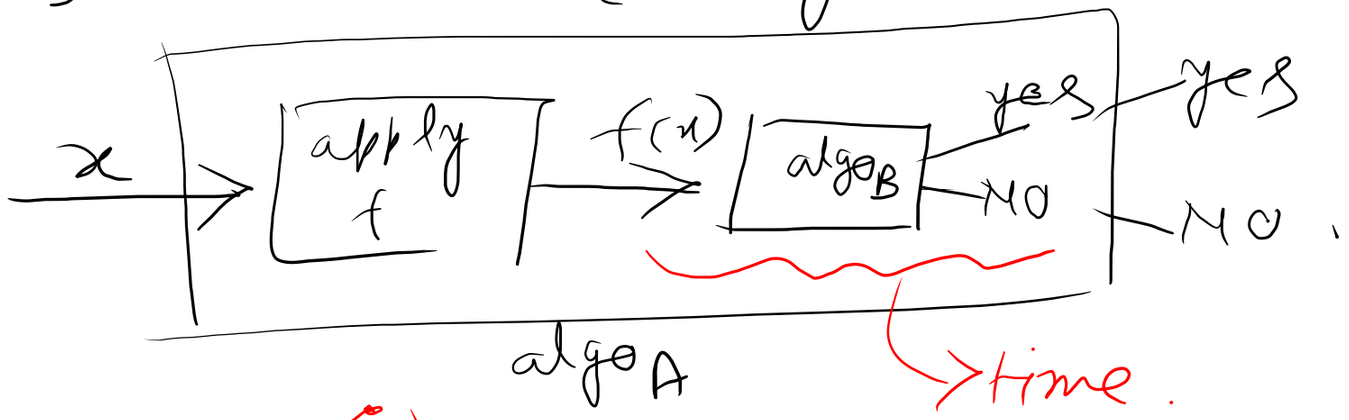


- f(x) is computable in polynomial time (in size of x)

A is polynomial time reducible to B and is denoted by $A \leq_p B$

Th^m $A \leq_p B$ and if B is solvable in polynomial time then A is solvable in polynomial time.

Pictorially



Algo$_B$ takes $O(|f(x)|^c)$ time.

$x \to f(x)$ time: $O(|x|^K)$

total time: $O(|x|^K + |f(x)|^c)$

relation between $|x|$ and $|f(x)|$

$|f(x)|$ outputsize $|x|^K$ running time $\Big\}$ $|f(x)| \leq |x|^K$

Polynomial time reduction

$A \leq_p B$

Thm: $A \leq_p B$ and B is in P then A is in P.

Contrapositive :- $A \leq_p B$, if A is hard then B is hard.

Transitivity: If $A \leq_p B$, $B \leq_p C$ then $A \leq_p C$

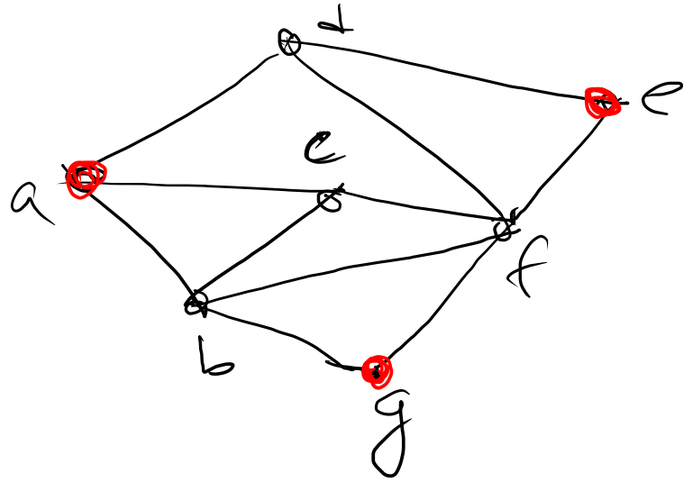
H.W.

Exm

Independent set problem:

Input: A graph $G(V, E)$, find a set $V' \subseteq V$ of maximum size such that no two vertices in V' are adjacent.

Exm



$\{b, d\}$

$\{g, a, e\}$

Does $|V'| \geq K$ or not?

Vertex cover problem

Given a graph $G(V, E)$ find a set $V' \subseteq V$ of minimum size such that at least one end-point of each edge must belongs to V'.

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

Does $|V'| \leq K$ or not?

Show that $IS_D \leq_p VC_D$

Two thing we need to show:

(i) $x \xrightarrow{f} f(x)$

x is a yes-instance of A iff $f(x)$ is a yes instance of B

(ii) $f(x)$ is computed in polynomial time.

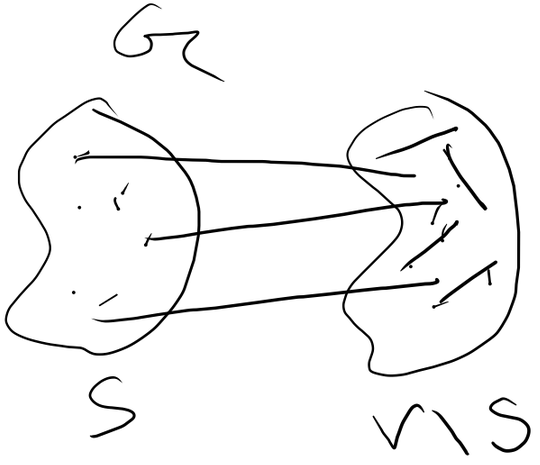
(i) $x \rightarrow f(x)$

- we are given the IS_D instance $G(V, E)$
- we take the same graph $G(V, E)$ as an instance of VC_D

we now prove the following.

Thm Let G be a graph. Let S be an independent set of size at least K iff $\{V \setminus S\}$ is a vertex cover of G of size at most $(n-K)$.

Proof ($\Rightarrow$) Assume S is an independent set.
We need to prove that $\{V \setminus S\}$ is a vertex cover.



($\Leftarrow$)

(ii) Trivial as we take the same graph.

Exm

Set cover problem

Given a universe $U = \{a_1, a_2 \ldots, a_n\}$ and a collection of subsets of U ie, $C = \{S_1, S_2, \ldots, S_m\}$

Find a subcollection $C' \subseteq C$ of minimum size such that each element in U belongs to at least one set in C'.

Exm

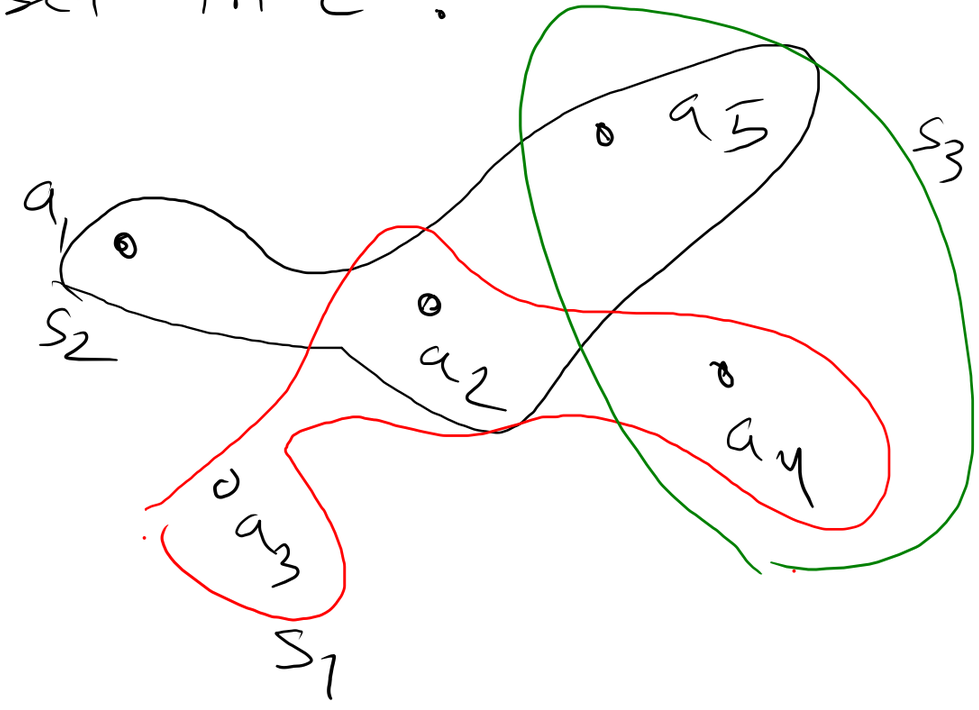
$$U = \{a_1, a_2, a_3, a_4, a_5\}$$

$$C = \{S_1, S_2, S_3\}$$

$$S_1 = \{a_2, a_3, a_5\}$$

$$S_2 = \{a_1, a_2, a_4\}$$

$$S_3 = \{a_4, a_5\}$$



solution $= \{S_1, S_2\}$

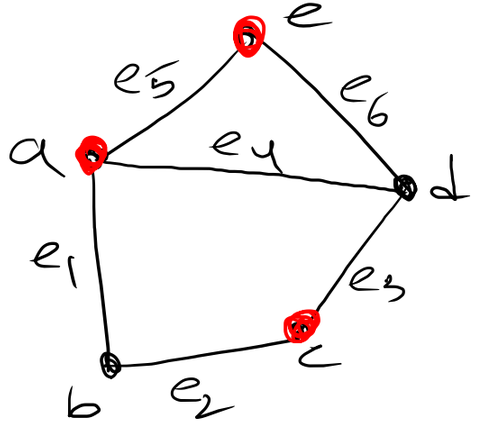
Show that $VC_D \leq_p SC_D$

We are given a VC_D problem instance.

A graph is given $G(V, E)$

$$G \xrightarrow{f} I_G(U, C)$$

instance of SC_D depends on G.



$E \Leftrightarrow U$

$U = \{ e_1, e_2, e_3, e_4, e_5, e_6 \}$

For each vertex $v \in V$ take a set S_v in C.

$C = \{ S_a, S_b, S_c, S_d, S_e \}$

where $S_a = \{ e_1, e_4, e_5 \}$

$S_b = \{ e_1, e_2 \}$

$S_c = \{ e_2, e_3 \}$

$S_d = \{ e_3, e_4, e_6 \}$

$S_e = \{ e_5, e_6 \}$

$x \xrightarrow{f} f(x)$

For each edge e_i take an element in U
For each vertex $v \in G$ take a set S_v in C.
Where S_v contains all elements whose corresponding edges are incident on v.

In: G has a vertex cover of size at most K iff $I_G(U, C)$ has a set cover of size at most K.

Further the reduction takes polynomial time. Why?

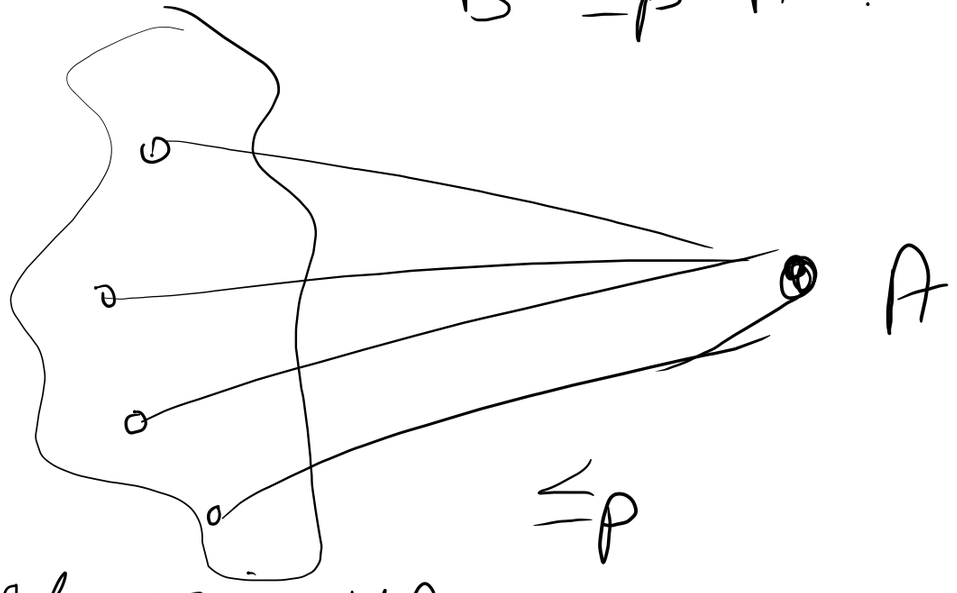
class P
class NP
} polynomial time reduction.

class NP-hard

A decision problem A is in class NP-hard if for all problems B in NP

$B \leq_p A$.

Pictorially



NP-complete

A decision problem A is in class NP-complete if

i) $A \in NP$

ii) A is NP-hard. (all problems $B \in NP$ $B \leq_p A$)

Ex^m satisfiability or circuit satisfiability. (SAT)

1971 → cook and Levin

They proved every problem in NP is polynomial time reducible to SAT.

SAT: ϕ is a formula in CNF form with n variables $x_1, x_2, \ldots, x_n$ and m clauses $C_1, C_2, \ldots, C_m$.

Decide whether ϕ is satisfiable or not.

Assigning 0/1 values to the variables and evaluate ϕ.

Ex: $\phi = C_1 \wedge C_2 \wedge C_3 \wedge \cdots \wedge C_m$

where each $C_i = (x_{i_1} \vee x_{i_2} \vee \cdots \vee x_{i_k})$

$$\varphi = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_4)$$

$$x_1 = 1, \quad x_2 = 1, \quad x_3 = 0, \quad x_4 = 1$$

Thm A is a decision problem such that $B \leq_p A$, for some NP-complete problem B, then A is NP-hard.

Proof B is NP-complete.

For all problems C is in NP.

$$C \leq_p B \quad \text{---------- (1)}$$

we also have $B \leq_p A$, ---- (2)

Transitivity (1) & (2)

$$C \leq_p A.$$

that means all problems in NP is polynomial time reducible to A. $\Rightarrow$ A is NP-hard.

Alternative definition of NP complete

A decision problem A is in class NP-complete if

i) A is in NP

ii) $\exists$ an NP-complete problem B such that $B \leq_p A$.

} NP-hard.

Methods to prove a problem A is NP-complete

1) Prove $A \in NP$.

2) Select a known suitable NP-complete problem B

3) Describe an algorithm that computes a function f that maps each instance x of B to an instance $f(x)$ of A.

4) Prove that the function satisfies $x \in B$ iff $f(x) \in A \quad \forall x \in B$

5) Prove that f can be computed in polynomial time.

Exⁿ Prove that 3-SAT is NP-complete.

3-SAT: $\phi = (\bar{x}_1 \vee x_2 \vee \bar{x}_3) \wedge (x_2 \vee \bar{x}_3 \vee x_4) \wedge (x_1 \vee \bar{x}_2 \vee x_4)$

Each clause contains exactly 3 literals.

1) 3-SAT $\in$ NP.

consider a certificate: Given an assignment to the variables. $x_1 = 0$, $x_2 = 1$, $x_3 = 0$, $x_4 = 1$

In ϕ, use this assignment, evaluat ϕ.

It takes poly-time (in n and m).

2) choose a suitable NP-complete problem say SAT.

$$SAT \leq_p 3\text{-}SAT$$

3) ϕ be an instance of SAT, F_ϕ be an instance of 3SAT

&

4)

$$\phi \xrightarrow{f.} F_\phi$$

$$\phi = C_1 \wedge C_2 \wedge C_3 \wedge \ldots \wedge C_m$$

C_i's have arbitrary sizes.

$$F_\phi = C_1' \wedge C_2' \wedge \ldots \wedge C_{m'}'$$

C_i''s are exactly size-3.

consider a clause C_i: it has literals.

Assume $C_i = x$

replace C_i by 4 clauses as follows.

$$F_{C_i} = (x \vee z_1 \vee z_2) \wedge (x \vee z_1 \vee \bar{z}_2) \wedge (x \vee \bar{z}_1 \vee z_2) \wedge (x \vee \bar{z}_1 \vee \bar{z}_2)$$

C_i is evaluate to 1 then take any value of z_1 and z_2

then f_{C_i} is satisfiable.

$C_i = (x \vee y)$

replace by $F_{C_i} = (x \vee y \vee z) \wedge (x \vee y \vee \bar{z})$

C_i is evaluate to 1 then any value of z makes F_{C_i} satisfiable.

$C_i = (x \vee y \vee z)$

not doing anything

$c_i = (x \vee y \vee z \vee w)$

replace c_i by

$f_{c_i} = (x \vee y \vee t) \wedge (z \vee w \vee \bar{t})$

if c_i evaluates to 1 then (if x or y evaluate to 1
then take $t = 0$)

→ else if z or w evaluate to 1
then take $t = 1$)

$$C_i = (x_1 \vee x_2 \vee x_3 \vee \cdots \vee x_K)$$

$$F_{C_i} = (x_1 \vee x_2 \vee z_1) \wedge (\bar{z}_1 \vee x_3 \vee z_2) \wedge (\bar{z}_2 \vee x_4 \vee z_3) \wedge \cdots$$

$$\cdots \wedge (\bar{z}_{K-3} \vee x_{K-1} \vee x_K)$$

Assume C_i is satisfiable, but x_t be 1

we consider $z_1, z_2, \cdots, z_{t-2} = 1$

$$z_{t-1}, z_t, \cdots, z_{K-3} = 0$$

5> Polynomial time

F_ϕ contains polynomial in $(n \& m)$ number of clauses and variables.

3SAT is NP-complete.

We have seen $IS_D \leq_p VC_D$

Also we have seen VC_D is in NP.

We know that IS_D is NP-complete (somehow we know)

Then we conclude VC_D is also NP-complete.

An alternative proof of VC_D is NP-complete.

by giving a reduction from 3-SAT problem.

poly-time.

$3SAT \leq_p VC$

$\phi \xrightarrow{f} G_\phi (V, E)$

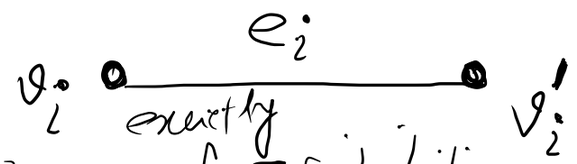
We show that ϕ is satisfiable iff G_ϕ has a vertex cover of size $\leq k$.

Gadget reduction

The graph G_ϕ contains gadgets that mimics the variables and clauses of ϕ.

variable gadget

For each variable x_i, we take a graph as,



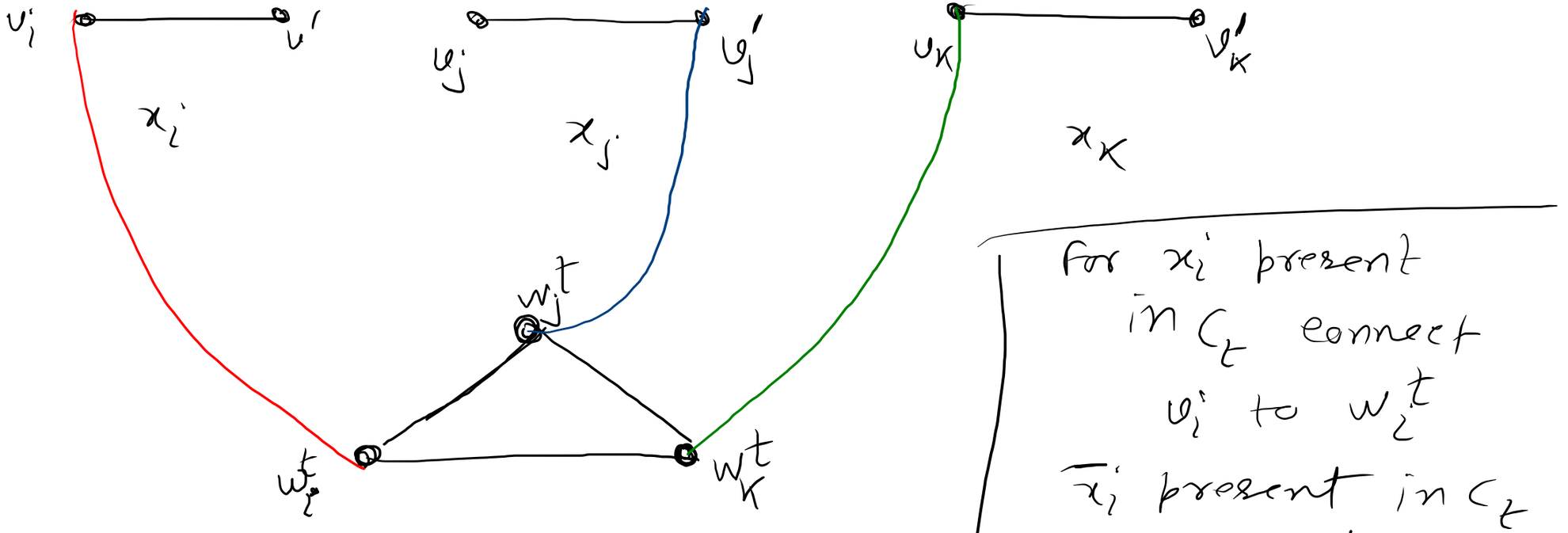
There are two possibilities of minimum vertex cover.

We pick in the vertex cover v_i → corresponding to literal x_i

" " " " " " v_i'' → " " " " $\overline{x_i}$

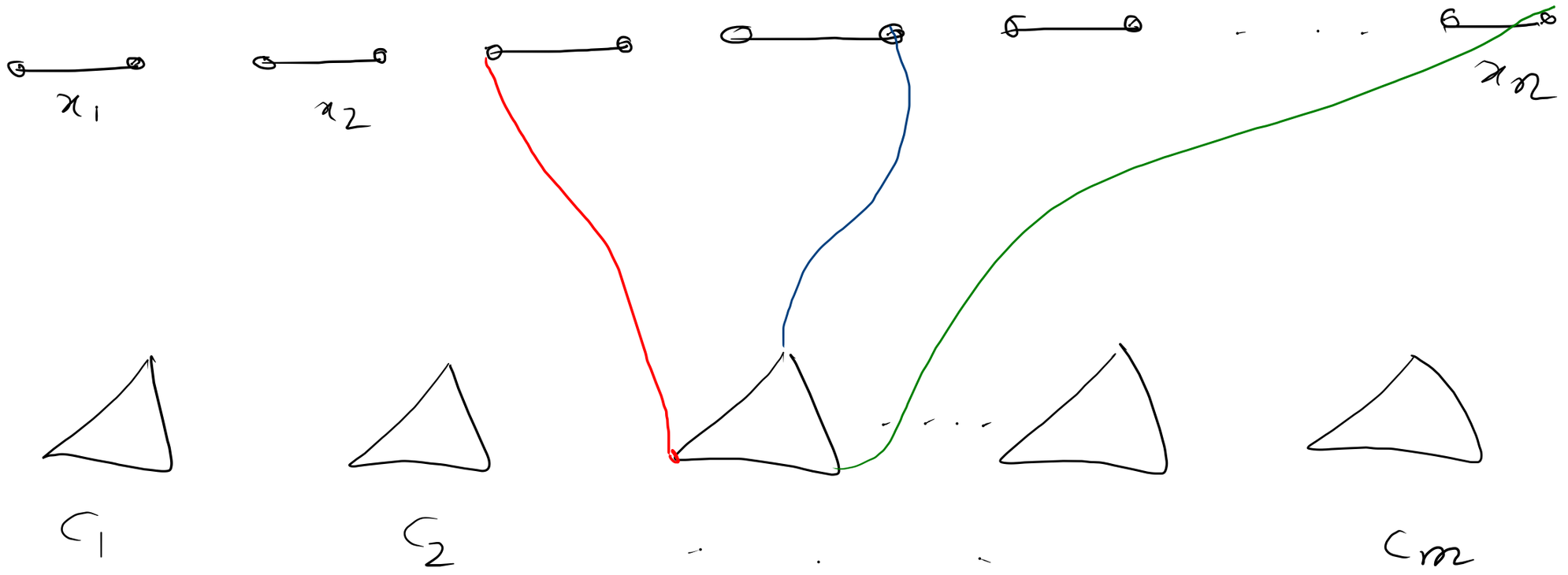
clause gadget $C_t = (x_i \vee \bar{x}_j \vee x_k)$ (w_t^i, w_t^j, w_t^k)

For a clause take 3 vertices and 3 edges that makes a triangle.



For x_i present in C_t connect v_i to w_i^t

$\bar{x}_i$ present in C_t connect v_i' to w_j^t



We now prove ϕ is satisfiable iff G_ϕ has a vertex cover of size $n+2m$

Assume ϕ is satisfiable

It has a satisfying assignment ϕ assign to variables that evaluates ϕ to be 1.

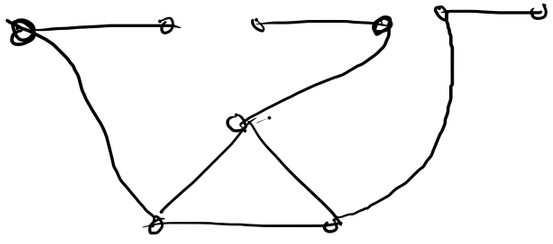
$$T : \{x_1 \dots x_n\} \longrightarrow \{0, 1\}$$

$T(x_i) = 1$ then take v_i in the solution

$T(x_i) = 0$ " " v_i' " " "

So we select a total of n vertices.

So we can pick at most $2m$ vertices covering the remaining edges.



for each clause $c_t = (x_i \vee \overline{x_j} \vee x_k)$

we consider a true literal and then select the other two vertices from clause gadget in the vertex cover.

Total we select $n + 2m$ vertices.

Otherside

suppose there is a ~~vertex~~ cover of size at most $n+2m$.

For each variable ∧ gadget at least one ~~vertex~~ is required to cover the edge

For each clause gadget at least 2 vertices are required.

⇒ at least $n+2m$ vertexes are required.

⇒ we need exactly $n+2m$ vertices.

⇒ exactly n vertices from variable gadget
" $2m$ " " clause "

each variable and clause gadgets are independent

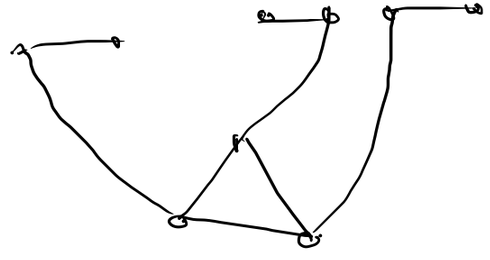
=> Each variable gadget exactly 1 vertex is required
" clause " " 2 vertices are "

We now consider the assignment as follows.

we take x_i to be 1 if v_i is picked
x_i to be 0 if v_i " "

Now we prove that each clause is satisfiable.

$$C_t = (x_i \vee \overline{x_{ij}} \vee x_k)$$



since exactly 2 vertices are picked.
one of the three cross edges must be covered by variable vertex.

That vertex is corresponding to a true literal.

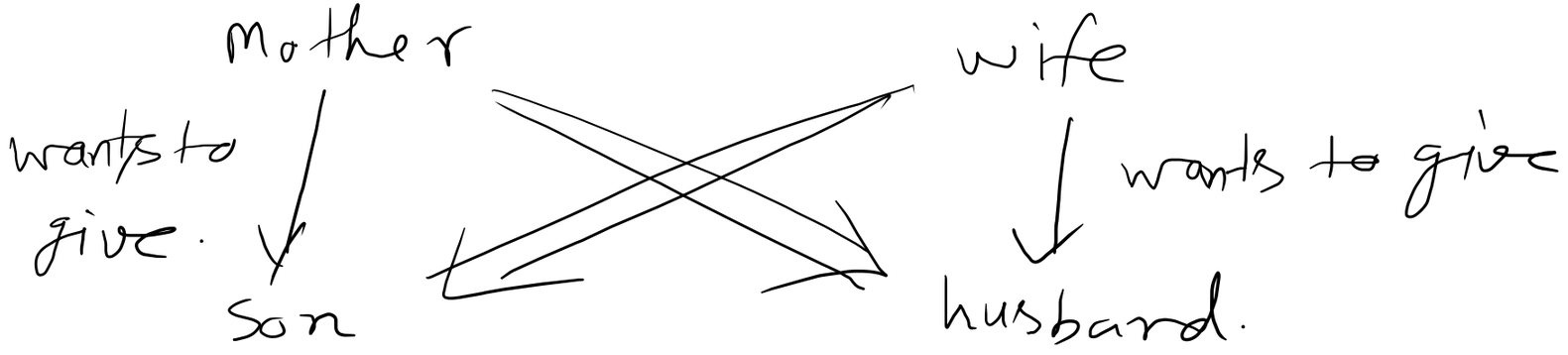
makes the clause satisfiable.

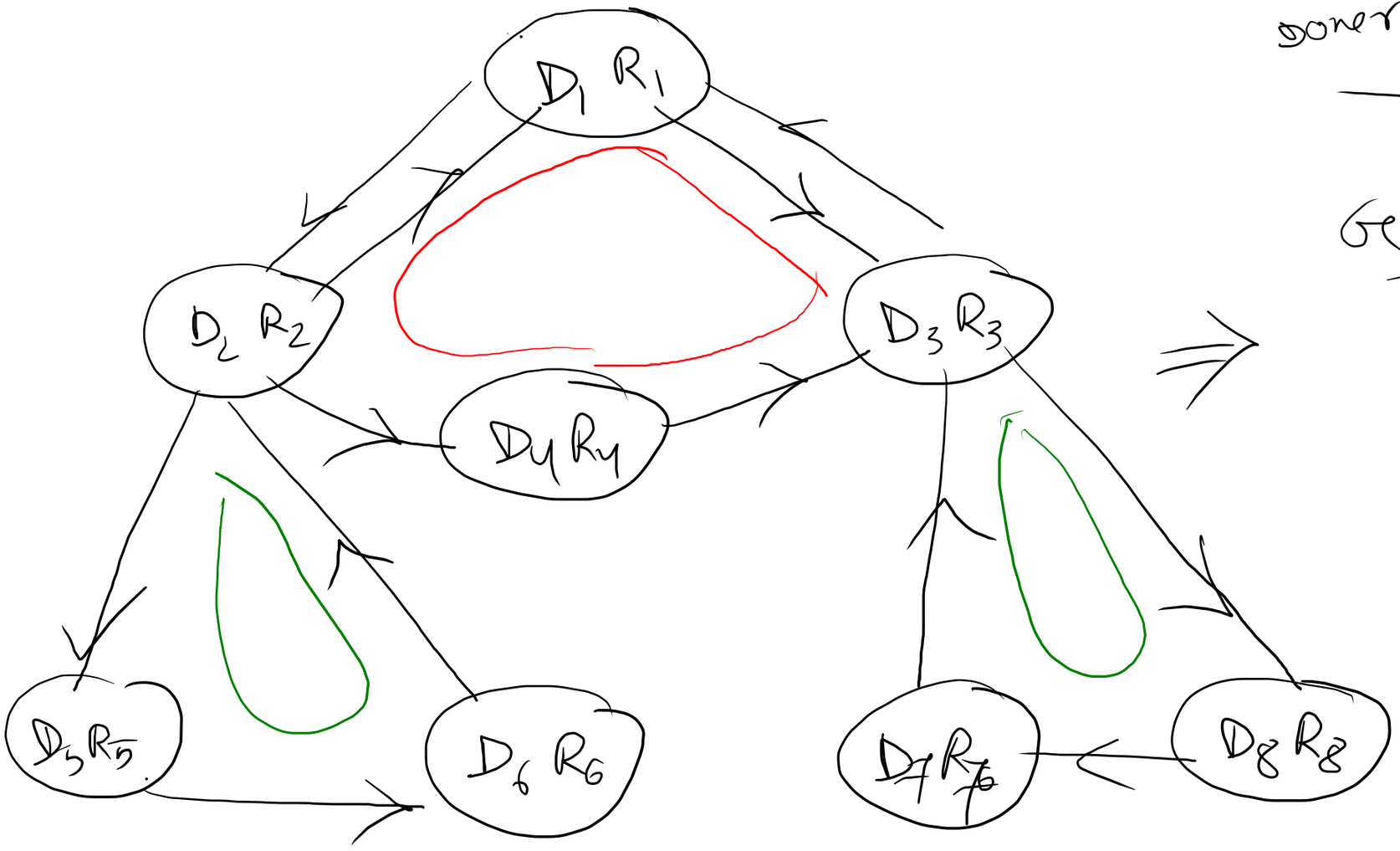
	vertices	edges
variable gadget	$2n$	n
clause gadget	$3m$	$3m$
	$3m+2n$	$3m+n$.

Kidney exchange problem

Basic facts:

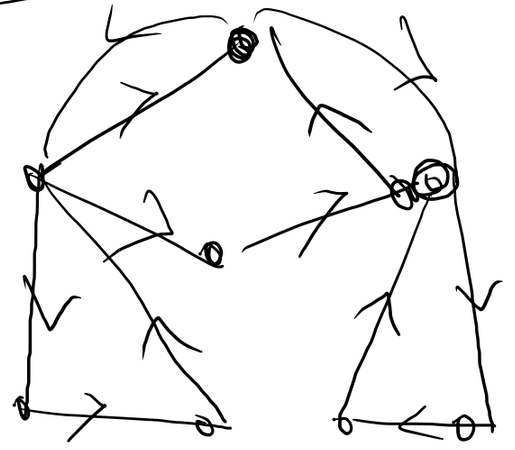
- People can survive with one kidney only.
- Thousands of patients need only one kidney.
- Thousands of them die because of unavailability of kidney
- compatibility issue.





donor$_i$ → receiver$_i$

Graph problem



- Given a directed graph
- Find a set of disjoint cycles that cover maximum vertices.

Disjoint cycle cover problem:

It is NP-complete.

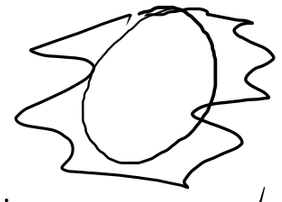
Cope with NP-complete problems

Optimization problems

- They are everywhere.
- They are incredibly hard to solve.
- But we need to solve them. They are important.
- Many of them are NP-complete.

coping methods

- Special cases — (general problem is NP-complete by a special case may be solved in poly time).
  Ex^m: vertex cover problem in bipartite graph can be solved in poly time.
- Approximation algorithms →
- Heuristics → difficult to measure the solution.



In polynomial time find near optimum solution.

- Exponential time algorithm →
- Parameterized algorithms. → running time is polynomial on the input size and the given parameter.

Approximation algorithms

- It is a polynomial time algorithms.
- It gives a solution as close to the optimum.

- A be a minimization problem.
  - Opt ← optimum solution.
  - algo ← algorithm "

$$\alpha = \frac{algo}{Opt.}$$ is called the approximation for the minimization problem.

$$\alpha > 1$$

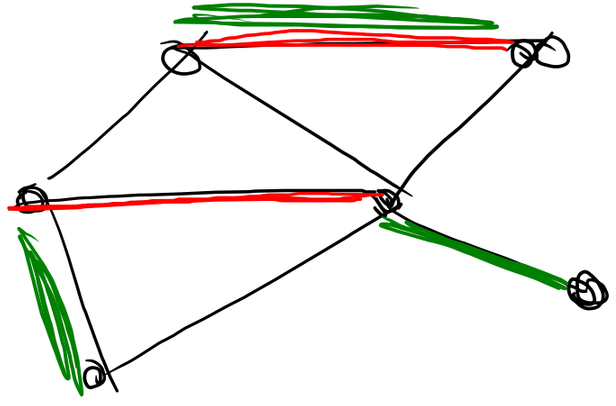
Vertex cover problem

Input: $G_c(V, E)$

output: $V' \subseteq V$ of minimum cardinality that cover all edges.

Approximation algorithm

maximal matching : $F \subseteq E$ such that no two edges are adjacent.



maximum: $|F|$ is maximum

maximal: can not add one extra edge in F.

Approx Algo:

1. Find a maximal / maximum matching $M \subseteq E$

2. Return the set C of end-point of each edge in M as a vertex cover.

we need to prove:

i) C is a vertex cover.

ii) Algo takes poly time

iii) Approximation factor : 2.

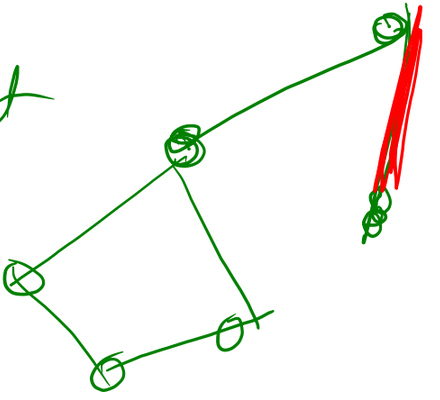
i) C is a vertex cover.

but C is not a vertex cover

- ∃ an edge e whose both end point not in C.
- add e to M.

makes increment in size of M.

$\Rightarrow : \Leftarrow$



ii) Algo takes poly time.

straightforward.

iii) Approximation factor: (size)

opt ← optimum vertex cover.

$opt \geq |M|$ How they related.

$$|C| = 2|M| \leq 2 \cdot opt$$

$$\frac{|C|}{opt} = 2$$

Number theory

Study of numbers

integers

positive integers

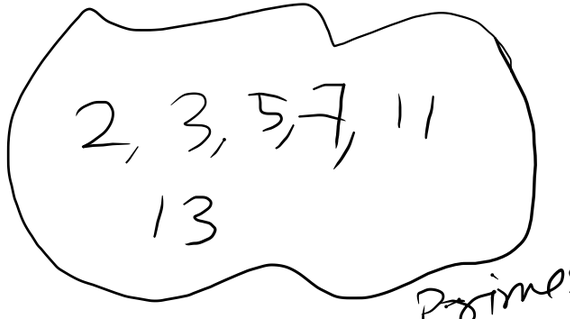
$$\mathbb{Z} = \{-\infty, \ldots, -1, 0, 1, 2, \ldots \infty\}$$

$$\mathbb{Z}^+ = \{1, 2, \ldots, \infty\}$$

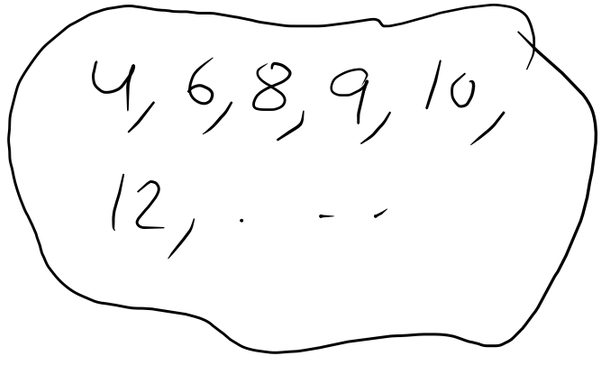
Divisibility Theory

positive integers classes.

Unit



primes



composites.

Division

Let a, b be integers with $a \neq 0$ then a divides b $(a \mid b)$ if $\exists$ an integer c such that

$$b = a \cdot c$$

$a \leftarrow$ factor / divisor

$b \leftarrow$ multiple of a.

Ex^{m} $9 \mid 27$, $7 \mid 49$.

$a \nmid b \leftarrow$ a does not divides b.

Properties: Let a, b, c be integers $a \neq 0$ then

a) if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$

b) If $a \mid b$, then $a \mid bc$ for all integers c.

c) If $a \mid b$ and $b \mid c$ then $a \mid c$

d) $a \mid b$ and $a \mid c$ then

$$a \mid (mb + nc)$$ m, n are integers.

Division theorem

Let a and d be two integers with $d > 0$
then $\exists$ integers q and r such that

$$a = qd + r \quad \text{where} \quad 0 \leq r < d$$

$d \leftarrow$ divisor
$a \leftarrow$ divident
$q \leftarrow$ quotient
$r \leftarrow$ remainder

Ex^{m}

$$34 = 8 \cdot 4 + 2$$
$$a \quad q \quad d \quad r$$

congruence relation

Let a and b be integers and m be a positive integer, then a is congruent to b modulo m if $m \mid (a-b)$

notation : $a \equiv b \bmod m$.

$a \not\equiv b \bmod m$: a is not congruent to b modulo m.

$5 \equiv 1 \bmod 2$

modulo 3.

0, 3, 6, 9, 12, . . . $\equiv 0 \mod 3$

1, 4, 7, 10, 13 . . . $\equiv 1 \mod 3$

2, 5, 8, 11, 14, ... $\equiv 2 \mod 3$

Properties: Let m be a positive integer, The integers a, and b where a is b congruent modulo m iff there is an integer k such that $a = b + km$

Proof

$$a \equiv b \bmod m$$

$$\Rightarrow m \mid (a-b)$$

$$\Rightarrow a - b = m \cdot k$$

$$\Rightarrow a = b + km.$$

- Let m be a positive integer. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then
  - $\rightarrow (a+c) \equiv b+d \bmod m$
  - $\rightarrow ac \equiv bd \bmod m$.

H.W.

- If $a \equiv b \bmod m$ then
  - $\rightarrow ca \equiv cb \bmod m$
  - $\rightarrow c+a \equiv c+b \bmod m$

where c is an integer.

– Let m be a positive integer and a, b are integers

then

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m.$$

$$ab \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m.$$

Primes: A positive integer > 1 is a prime if it is divisible by 1 and the number itself.

otherwise it is a composite.

The fundamental theorem of arithmatic

Every integer can be written as the the product of primes.

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Where p_i's are k distinct primes and

e_i's are integers with $e_i > 0$

Greatest common divisor (gcd)

It is the positive divisor of both a and b

i.e, $gcd(a, b) = d$ means.

$d \mid a$ and $d \mid b$.

Exm $gcd(12, 33) = 3$ as $3 \mid 12$ and $3 \mid 33$

Relatively prime

Two integers a and b are relatively prime.
if gcd (a, b) = 1

Ex^m

12, 31 gcd (12, 31) = 1

8, 9 ← relatively prime.

Finding gcd

gcd (a, b)

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_K^{e_K} \qquad e_i \geq 0$$

$$b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_K^{f_K} \qquad f_i \geq 0.$$

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} \cdot p_2^{\min(e_2,f_2)} \cdots p_K^{\min(e_K,f_K)}$$

This method is not efficient.

as prime factorization is not efficient.

Least common multiple (lcm)

$lcm(a,b) = l$ means $a \mid l$ and $b \mid l$

l is the smallest integer.

Finding lcm

$$lcm(a,b) = p_1^{\max\{e_1,f_1\}} \; p_2^{\max\{e_2,f_2\}} \cdots p_x^{\max\{e_x,f_x\}}$$

Let a, b be integers, then

$$ab = gcd(a,b) \times lcm(a,b)$$

Properties of gcd

$$gcd(a,b) = gcd(b,a)$$

$$gcd(a,a) = a$$

$$gcd(a,b) = gcd(a-b,b)$$

$$gcd(a,0) = a$$

Euclid's algorithm for finding gcd

Input: two integers a, b

output: $\gcd(a, b)$

Ex^m $\gcd(138, 256)$

$\gcd(256, 138)$

```
Euclid (a, b)
while b ≠ 0
    r ← a mod b
    a ← b
    b ← r
return a
```

$\equiv a = bq + r$

$b = 138$

$\begin{cases} r \leftarrow 118 \\ a = 138 \\ b = 118 \end{cases}$

$\begin{cases} r \leftarrow 20 \\ a \leftarrow 118 \\ b \leftarrow 20 \end{cases}$

$\begin{cases} r \leftarrow 18 \\ a \leftarrow 20 \\ b \leftarrow 18 \end{cases}$

$\begin{cases} r \leftarrow 2 \\ a \leftarrow 18 \\ b \leftarrow 2 \end{cases}$

$\begin{cases} r \leftarrow 0 \\ a \leftarrow 2 \\ b \leftarrow 0 \end{cases}$

$\boxed{\gcd(256, 138) = 2}$

correctness

~~let~~ $a = bq + r$ where a, b, q, r are integers with $r \geq 0$ then

$$\gcd(a, b) = \gcd(b, r).$$

Proof $d = \gcd(a, b) \Rightarrow d \mid a$ and $d \mid b$

also $a = bq + r$

$\Rightarrow a - bq = r$

if $d \mid a$ and $d \mid b \Rightarrow d \mid a - bq$

$\Rightarrow d \mid r$.

Exm gcd (1244, 324)

$= \gcd(324, 272)$

$= \gcd(272, 52)$

$= \gcd(52, 12)$

$= \gcd(12, 4)$

$= \gcd(4, 0)$

$= 4.$

Linear congruences

A congruence is of the form.

$$ax \equiv b \mod m$$

where m is a positive integer and a, b are integers
x is an integer variable.

The solution of this congruence are all integers that satisfy this equation.

Multiplicative inverse

$\bar{a}$ is a multiplicative inverse of a modulo m if

$$a\,\bar{a} \equiv 1 \bmod m.$$

How this is used to solve linear congruence?

$$ax \equiv b \bmod m.$$

$$\Rightarrow \bar{a}\,a\,x \equiv \bar{a}\,b \bmod m.$$

$$\Rightarrow x \equiv \bar{a}\,b \bmod m.$$

Ex^n find multiplicative inverse of 5 mod 9

Sol^n need to find $\bar{a}$ s.t

$$5 \cdot \bar{a} \equiv 1 \bmod 9.$$

$$5 \cdot 1 \equiv 5 \bmod 9.$$

$$5 \cdot 2 = 10 \equiv 1 \bmod 9.$$

multiplicative inverse is 2.

Exm Find multiplicative inverse of
7 mod 11

Sol^n Find. $\bar{a}$ s.t. $7 \cdot \bar{a} \equiv 1 \bmod 11$

$7 \cdot 1 = 7 \equiv 7 \bmod 11$

$7 \cdot 2 = 14 \equiv 3 \bmod 11$

$7 \cdot 3 = 21 \equiv 10 \bmod 11$

$7 \cdot 4 = 28 \equiv 6 \bmod 11$

$7 \cdot 5$

$7 \cdot 8 = 56 \equiv 1 \bmod 11$

Ex.^m Find multiplicative inverse of

3 mod 6

Soln

$3 \cdot 1 = 3 \equiv 3$

$3 \cdot 2 = 6 \equiv 0$

$3 \cdot 3 = 9 \equiv 3$

$3 \cdot 4 = 12 \equiv 0$

If a and m are relatively prime and $m > 1$ then a multiplicative modulo m exists. Further this inverse is unique.

Ex^n Find x such that $3x \equiv 7 \pmod{10}$

Sol^n

$$3x \equiv 7 \pmod{10}$$

$$\Rightarrow x \equiv \bar{3}\,7 \pmod{10}$$

$$\Rightarrow x \equiv 7 \cdot 7 \pmod{10}$$

$$\Rightarrow x \equiv 49 \pmod{10}$$

$$\Rightarrow x \equiv 9 \pmod{10}$$

$$3 \cdot 7 \equiv 1 \pmod{10}$$

$$3^{-1} = 7$$

The chinese remainder theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers then the system.

$$x_1 \equiv a_1 \bmod m_1$$
$$x_2 \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x_n \equiv a_n \bmod m_n$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \cdots \cdot m_n$

Proof $p_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n$

$\gcd(p_i, m_i) = 1 \Rightarrow \exists$ two integers s_i and t_i s.t. $\gcd(p_i, m_i) \equiv s_i p_i + t_i m_i$

$\Rightarrow s_i b_i + t_i m_i = 1$

$\Rightarrow s_i b_i + t_i m_i \equiv 1 \mod m_i$

$\Rightarrow s_i b_i \equiv 1 \mod m_i$

Now assume a solution x as,

$$x = a_1 s_1 b_1 + a_2 s_2 b_2 + \cdots + a_n s_n b_n$$

If $j \neq i$, $m_i \mid b_j$ so take mod m_i we get,

$$x \equiv a_i s_i b_i \mod m_i$$

$$\Rightarrow x \equiv a_i \mod m_i$$

x is a unique solution

Assuming there are at least 2 solutions x and y.
modulo m.

$x \equiv a_1 \bmod m_1$ $\quad$ $y \equiv a_1 \bmod y_1$

$x = a_i \equiv y \bmod m_i$ $\quad$ so, $x - y \equiv 0 \bmod m_i$

$\Rightarrow m_i \mid x-y$

$lcm(m_1, m_2, \ldots, m_n) \mid x-y$

$\Rightarrow m_1 \cdot m_2 \cdots m_n \mid x-y \Rightarrow x \equiv y \bmod (m_1 m_2 \cdots m_n)$

Ex^m Solve: $x \equiv 2 \bmod 7$

$x \equiv 3 \bmod 8$

Sol^n

Solution is $x \equiv a_1 s_1 b_1 + a_2 s_2 b_2 \pmod{m_1 m_2}$

$b_1 = 8$ so $s_1 = 1$

$b_2 = 7$ $s_2 = 7$

$s_i b_i \equiv 1 \bmod m_i$

$s_1 8 \equiv 1 \bmod 7$

$s_1 \equiv 8^{-1} \bmod 7$

$= 1$

$x \equiv 2 \cdot 1 \cdot 8 + 3 \cdot 7 \cdot 7 \pmod{7 \cdot 8}$

$\equiv 16 + 147 \pmod{56}$

$\equiv 163 \pmod{56}$

$\equiv 51$

Ex^m

$$x \equiv 2 \mod 3$$
$$x \equiv 5 \mod 7$$
$$x \equiv 4 \mod 5$$
$$x \equiv 3 \mod 4$$

sol^n

$$x = a_1 p_1 s_1 + a_2 r_2 p_2 + a_3 s_3 p_3 + a_4 s_4 p_4 \mod m$$

HW

Fermat's little theorem

If p is a prime then,

$$a^{p-1} \equiv 1 \bmod p \quad \text{if } p \nmid a$$

$$a^{p} \equiv a \bmod p \quad \text{for every integer } a.$$

Ex^m $7^{222} \bmod 11$

Here $11 \nmid 7$ then by Fermat's little theorem.

$$7^{10} \equiv 1 \bmod 11$$

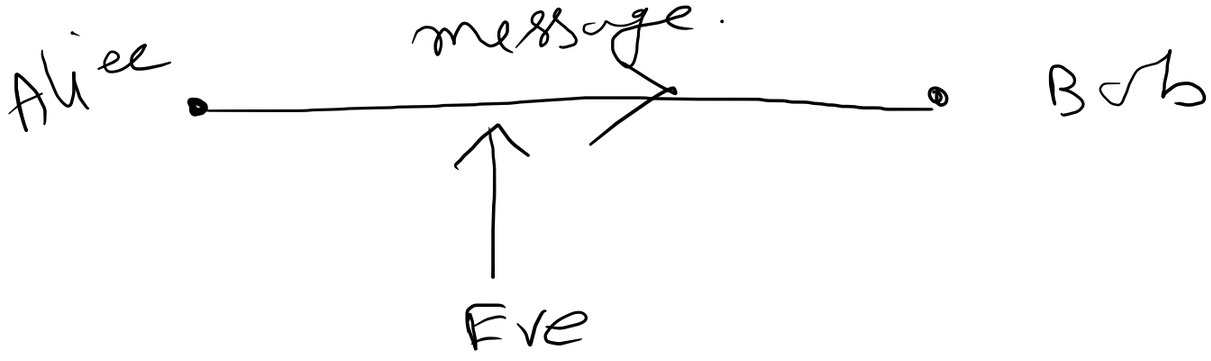
$$7^{222} \equiv \left(7^{10}\right)^{22} \cdot 7^{2} \mod 11$$

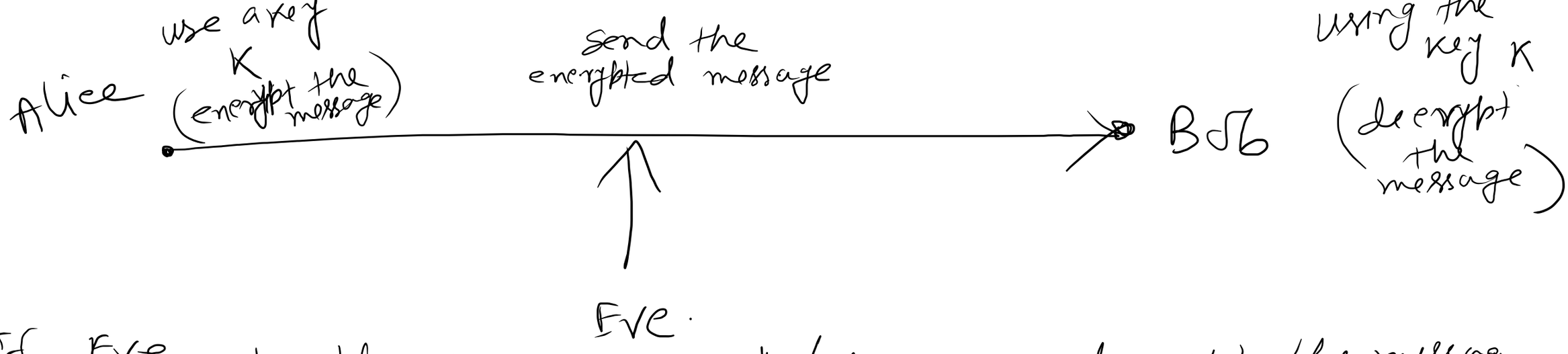
$$\equiv 1 \cdot 7^{2} \mod 11$$

$$\equiv 49 \mod 11$$

$$\equiv 5 \mod 11$$

Cryptography





If Eve gets the key K. then he/she can decrypt the message

Private key cryptosystem

Public key cryptosystem

Public keys.

send some keys.

Alice

Bob. (generates some keys) (send some of the keys to Alice)

uses Bob's public key.
to encrypt the message and send

- upon receiving the encrypted message uses its private key to decrypt the message.

cryptography:- It is encoding and decoding of messages.

plain text: The message that needs to be encoded.

cipher text: The encoded message.

Encryption: Process of encoding the message (plain to cipher)

Decryption: Process of decoding the message. (cipher to plain)

The caesar cipher

A	B	C	D	. . . .	Z
0	1	2	3	. . . .	25

Encoding some message.

$$c = x + 17 \mod 26$$

'HELLO' is the message.

H → 7 so $7 + 17 \mod 26 \equiv 24 \mod 26$ → Y

E → 4 $\equiv 21$ → V

C

C

F

HELLO ⟷ YVCCF

Decryption:

$$C \equiv x + 17 \mod 26.$$

$$x \equiv C - 17 \mod 26$$

YVCCF

Y → 24 $\quad 24 - 17 \mod 26 \equiv 7 \mod 26 \rightarrow$ H

V E

C L

C L

F O

RSA cryptosystem

It is a public key cryptosystem.

In RSA there are two phases.

Phase 1: key generation.

- choose two large primes p and q. (secret)
- compute $n = pq$ and $K = (p-1)(q-1)$
- choose e such that $\gcd(e, K) = 1$
- choose $d \equiv e^{-1} \bmod K$

n and e are public keys.
d is the private key.

Phase 2: Encryption and decryption.

Encryption

- A message M needs to send $\quad m < n$
- compute $C \equiv M^e \bmod n$
- send C to Bob.

Decryption

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

Exm $p = 5$, $q = 11$

$n = pq = 5 \times 11 = 55$ $\quad k = 4 \times 10 = 40$

choose e such that $\gcd(e, k) = 1$

let us take e as 3

compute $d \equiv e^{-1} \bmod k$ $\quad d \equiv 3^{-1} \bmod 40$

$\Rightarrow d = 27$

(n, e) are public keys ie, $(55, 3)$

d is private key ie, 27

Ex^{m} $p = 5$ $q = 11$

Key generation

Public keys: n, e 55 and 3

Private key d 27

Encoding:

A	B	C	D	. . .	Z
0	1	2	3	. . .	25

HELLO

H $\rightarrow$ 7

Encoding for H.

$$C \equiv m^e \bmod n$$

$$C \equiv 7^3 \bmod 55$$

$$\equiv 13 \bmod 55$$

encrypted message is $13 \rightarrow N$

Decryption: Bob received N $\longrightarrow$ 13

$13^2 \bmod 55 \qquad 169$

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

$$\equiv 13^{27} \bmod 55$$

$$\equiv \underbrace{13^2 \cdot 13^2 \cdots 13^2}_{13} \cdot 13$$

$$\equiv 4 \cdot 4 \cdots 4 \cdot 13$$

$$\equiv 64 \cdot 64 \cdot 64 \cdot 64 \cdot 4 \cdot 13$$

$$\equiv 9 \cdot 9 \cdot 9 \cdot 9 \cdot 4 \cdot 13$$

$$\equiv 7 \bmod 55$$

$7 \rightarrow H.$

Why RSA algorithm is correct?

we need to show that $c^d \bmod n$ is M.

$$c^d \equiv (M^e)^d \bmod n$$
$$\equiv M^{ed} \bmod n.$$

we have, $ed \equiv 1 \bmod K$

$$\Rightarrow ed = tK + 1$$

where t is any integer.

$$c^d \equiv M^{ed} \bmod n$$
$$\equiv M^{tK+1} \bmod n$$
$$\equiv M^{t(k-1)(q-1)} \bmod n$$

$$c^d \equiv m^{t(p-1)(q-1)+1} \mod pq$$

$$\equiv m \cdot m^{t(p-1)(q-1)} \mod pq$$

$$\equiv m \cdot \left(m^{(p-1)}\right)^{t(q-1)} \mod pq$$

$$m \cdot \left(m^{(q-1)}\right)^{t(p-1)} \mod pq$$

Fermats little theorem.

$$m^{p-1} \equiv 1 \mod p$$

$$m^{q-1} \equiv 1 \mod q.$$

$$c^d \equiv m \cdot \left(m^{p-1}\right)^{t(q-1)} \mod p$$

$$= m$$

$$c^d \equiv m \left(m^{q-1}\right)^{t(p-1)} \mod q$$

$$= m$$

we have,

$$c^d \equiv m \mod p$$

$$c^d \equiv m \mod q$$

By chinese remainder theorem The system has a unique solution mod pq.

$$c^d \equiv m \mod pq$$

Approximation

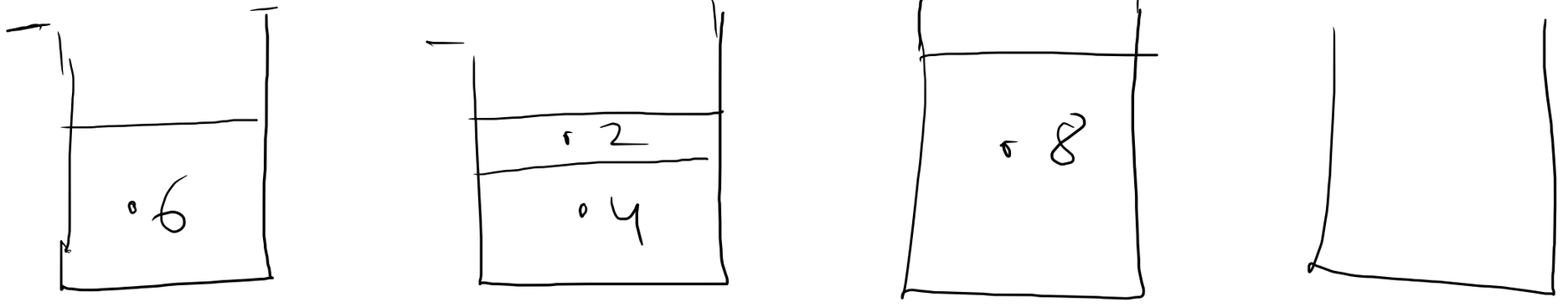
Bin packing problem

Assume there are n items of sizes < 1

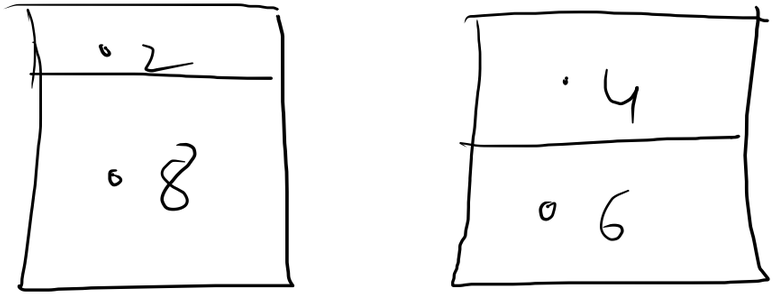
They need to fit in minimum number of unit size boxes.

.4, .6, .2, .8

some packing



optimum



Best-fit

⇒ first-fit

Next-fit

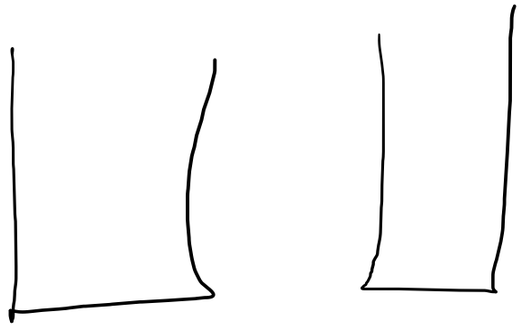
First-fit

- traverse from 1st to last bin.
- if it fits in a bin - place it there
- otherwise open a new bin

Correctness: trivially.

running time: $O(n^2)$

Approximation factor:



can these two bins are both are less than half full.

Not the case here.

If C bins are used by the algorithm.

and C^* be the optimum number of bins can be used.

$$c^* \geq \sum_{i=1}^{n} a_i > \frac{c-1}{2}$$

$$\Rightarrow 2c^* > c-1$$

$$\Rightarrow c < 2c^* - 1$$

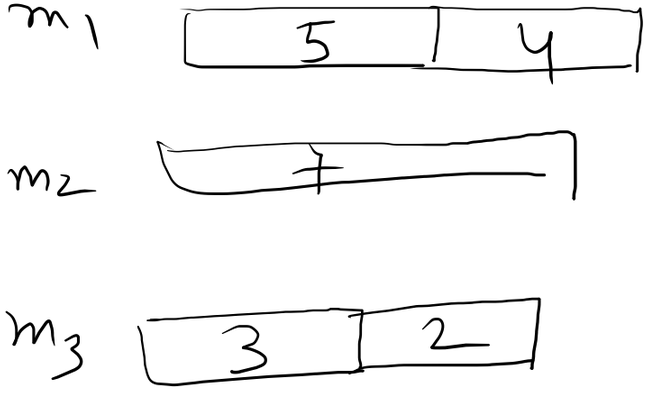
$$\Rightarrow c \leq 2c^* \quad \text{as } c \text{ \& } c^* \text{ are integers.}$$

Minimize makespan

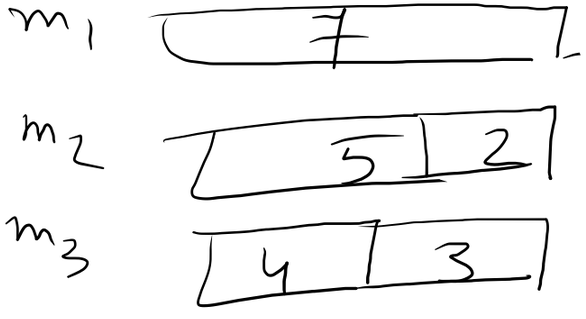
Scheduling jobs on identical parallel machines.

Input: n jobs $j_1, j_2, \ldots, j_n$ each job j_i has processing time t_i. There are m identical machines.

Output: Assign jobs into these machines such that the maximum load to any machine is minimum.



5, 7, 3, 2, 4



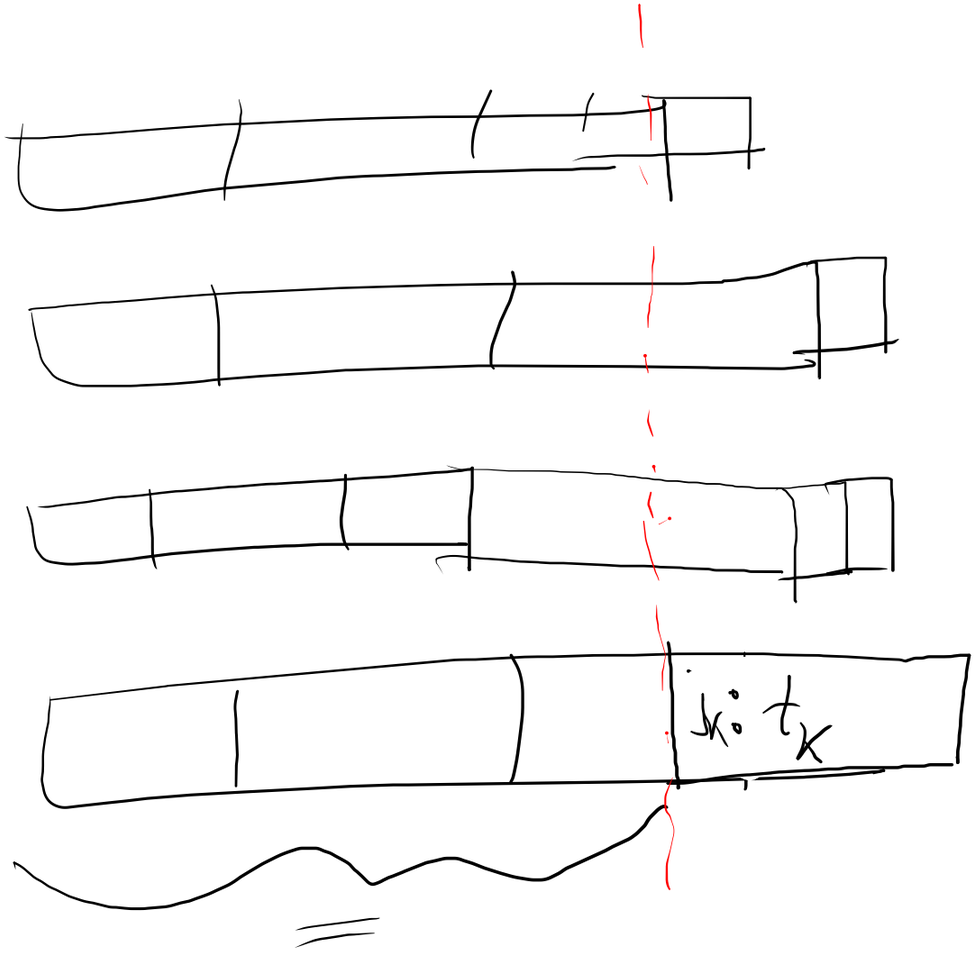
Algo: - Take jobs one-by-one.

= Assign to a machine whose load is minimum so far.

Approx factor:

Opt is the optimum load.

$$opt \geq \frac{\sum t_i}{m} \qquad opt \geq t_{max}$$



d' be the makespan just before adding J_k.

$$d' \leq \frac{\sum_{i=1}^{n} t_i}{m}$$

$$\text{Total makespan} = \frac{\sum_{i=1}^{n} t_i}{m} + t_k$$

$$\leq \text{opt} + \text{opt}$$

$$= 2\,\text{opt}.$$

t_{max}.