Lecture 29

Saturday, 23 October 2021 10:02 AM

Finding Primes efficiently — Universal hashing $[M, 2M]$ / Pattern match $[2, n^4]$

Prime No Thm

$[1, L] - \theta\left(\frac{L}{\log L}\right)$

random x in range $[1, L]$, $Pr(x \text{ is prime}) \overset{?}{=} \frac{1}{\log L}$

$x_1, x_2 \ldots x_{\log L}$ rand nos $[1, L]$, Expected no. of primes $= 1$

$x_1 \ldots x_{\log^2 L}$ rand no $[1, L]$ —

Prob of not getting prime will be $\boxed{\left(1 - \frac{1}{\log L}\right)^{\log^2 L}}$

this is very small

Relation

$\left(1 - \frac{1}{x}\right)^x \in \left[\frac{1}{4}, \frac{1}{e}\right]$

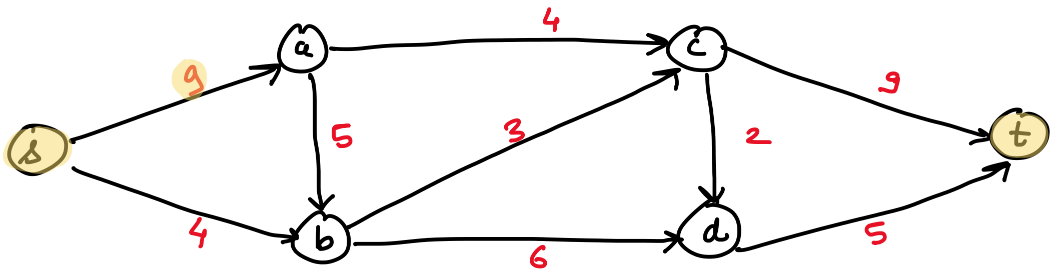
# To check if a no q is prime $\boxed{O(\text{polylog}(q))}$ time

Primes is in P

Max-Flow

Given : • A directed graph $G = (V, E)$, & each eadge e has some capacity $c(e) \geq$

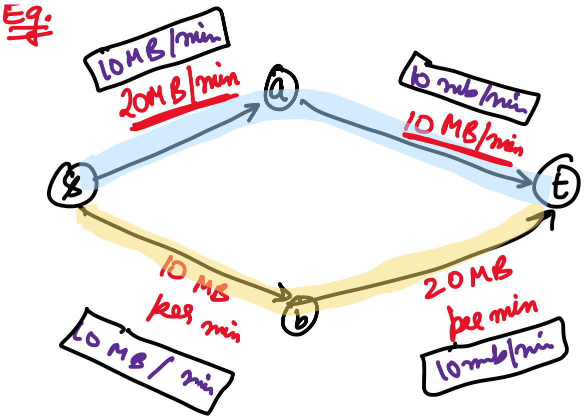
• We have a source s, and sink t.



Capacity

pipe / chanel — max possible rate of flow 9 litre /

Eg.



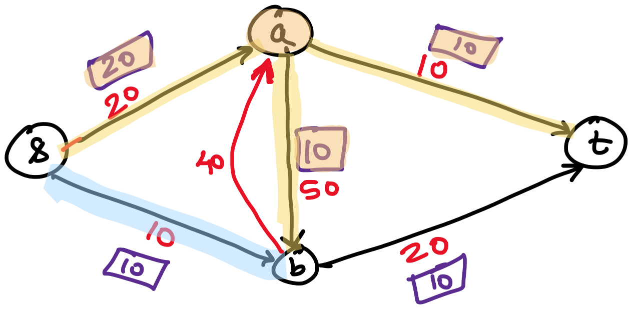
Wires — 45 mb / min
9 MB / min

(30) ×
(10) ×
20 ✓

f : E

f(e)

Eg.



Max - flow 30

Max flow doesn't correspond to edge disjoint p

Sol^n will be a vector of size |E(G)|

NOTATON : c(e) — capacity of edge e
f(e) — flow passing through edge e.

Constraints

① CAPACITY : $\forall e \quad f(e) \in [0, c(e)]$.

② CONSERVATION OF FLOW : $\forall x \neq s, t$ In-flow(x) = Out-fl

$$\sum_{\substack{(y,x)\\ \in \text{IN-EDGES}(x)}} f(y,x) = \sum_{\substack{(x,z)\\ \in \text{OUT-EDGE}}} f$$

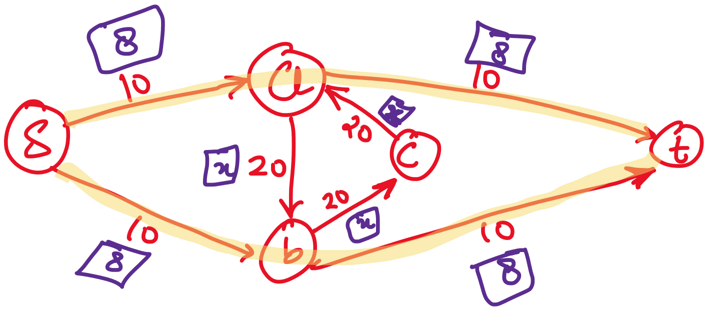
Mathematical Def^n of FLOW f

Value of flow f :

$$\text{val}(f) = \underbrace{\sum_{(s,x)\in E} f(s,x)} \quad \text{or} \quad \underbrace{\sum_{(x,t)\in}}$$

H. W. Prove that they are equal.

Eg.



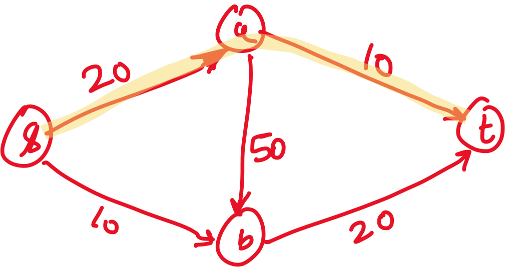
val (f) = 16

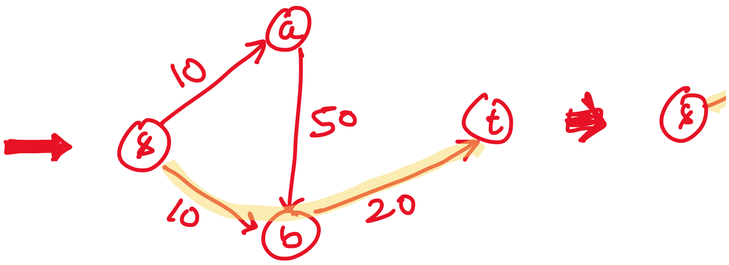
GOAL : Find a s-t flow "f" of max possi

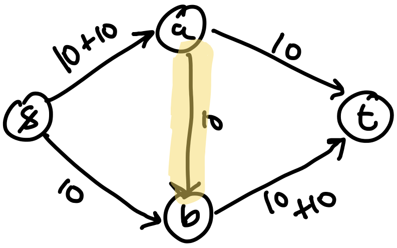
Approach

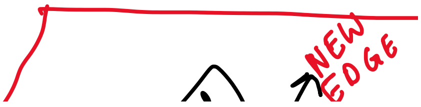
```
① $\forall e \in E$ : $f(e) = 0$
② While $\exists$ (s,t) path in G:
    P ← some (s,t) path
    $\delta$ = MIN $\{c(e) \mid e \in P\}$ ← Max flow that can transfered thr
    For all edges $e \in P$
        $f(e) = f(e) + \delta$ ← Increasing flow value
        $c(e) = c(e) - \delta$ ← Updating capacity
    Remove edges of capacity 0. ← Edge has 0 capacity
③ Return f
```

Run

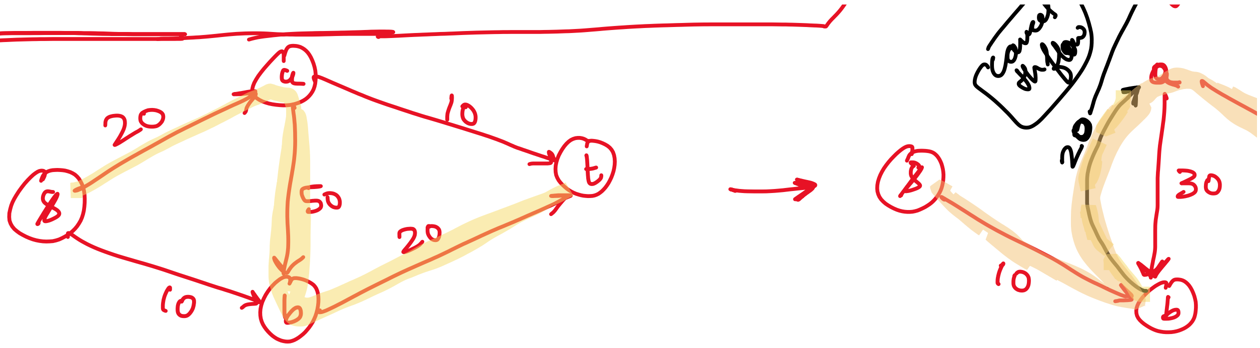


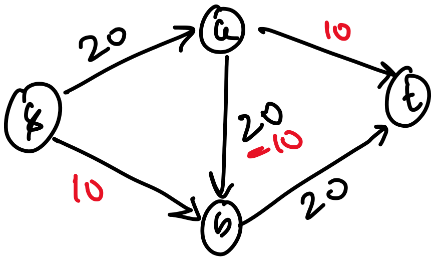






Rem

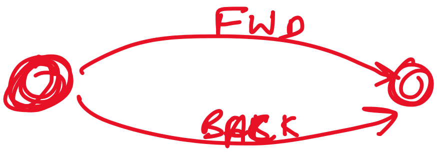




Def^n Residual graph G_f w.r.t. some flo

For each $(x,y) \in E(G)$ with flow

- Include $(x,y) \in G_f$ with $c_r(x,y) = c($
- Include $(y,x) \in G_f$ with $c_r(y,x) =$:



Next class

- Algorithm (approach + G_f)
- correctness