

CSE 6512 RANDOMIZATION
IN COMPUTING
10-12-2023

FACT: IF we have an undirected,
 Connected, & NON-BIPARTITE GRAPH $G(N, E)$
 we can construct a Markov
 Chain M Corr. to G .
 $V \equiv S; \quad P_{ij} = \frac{1}{d_i} \text{ IF } (i, j) \in E.$
 $= 0 \text{ otherwise. } m = |E|.$
 \exists a UNIQUE STATIONARY
 STATE PROB. VECTOR π .
 $\pi_i = \frac{d_i}{2m} \quad \forall i \in S. \quad \pi = \pi P.$

COMMUTE TIME BETWEEN TWO NODES

$$\bar{i} \text{ and } j = h_{ij} + h_{ji}.$$

EX.
 $C_i(\sigma) =$ TIME NEEDED TO VISIT
 EVERY node σ at least
 once starting FROM \bar{i} .

COVER TIME, $C(\sigma) = \max_{i \in V} C_i(\sigma).$

FOR ANY EDGE $(i,j) \in E$,
 $h_{ji} + h_{ij} \leq 2m$.

FROM $G \rightarrow$ CONSTRUCT A DIRECTED G' .

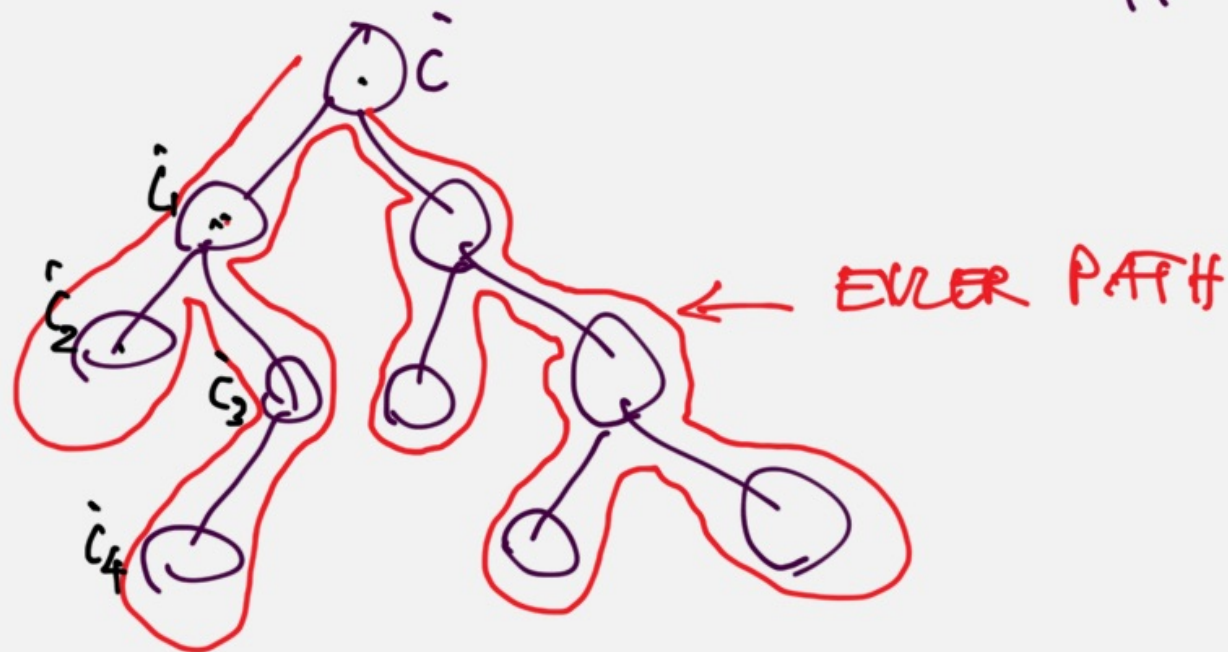
EVERY EDGE OF G' IS A STATE.

$$Q_{(a,b) \rightarrow (c,d)} = \frac{1}{d_b} \quad \# \quad b=c$$

$$= 0 \quad \text{OTHERWISE.}$$

$$\Pi = \left(\frac{1}{2m}, \frac{1}{2m}, \dots, \frac{1}{2m} \right).$$

let S be any SPANNING TREE FOR G .



let the EVLER PATH BE
 $\hat{c}, \hat{i}, \hat{i}_2, \hat{i}_3, \hat{i}_4, \dots, \hat{i}_{2(n-1)}$.

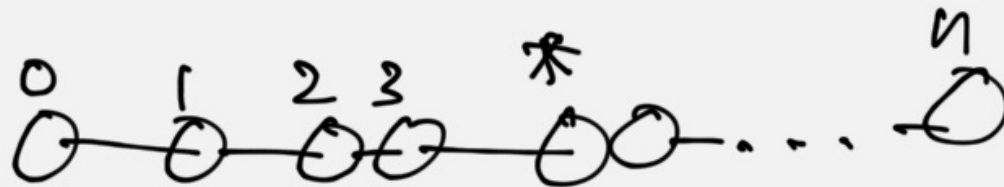
$$C_i(G) \leq h_i c_i + h_i c_{i+1} + h_i c_{i+2} + \dots$$

$$\leq 2(n-i)m$$

$$\Rightarrow C(G) \leq 2(n-1)m.$$

THEOREM: $C(G) \leq 2(n-1)m.$ \square

2SAT:



No. OF CORRECT ASSIGNMENTS \rightarrow

EXPECTED RUN TIME = $O(n^2)$.

FOR A COMPLETE GRAPH $G(V, E)$: $|V| = n$
 $|E| = \binom{n}{2}$
 $C(G) = O(n^3)$.

PROBLEM: INPUT: AN UNDIRECTED
 GRAPH $G(V, E)$.

$a, b \in V$.

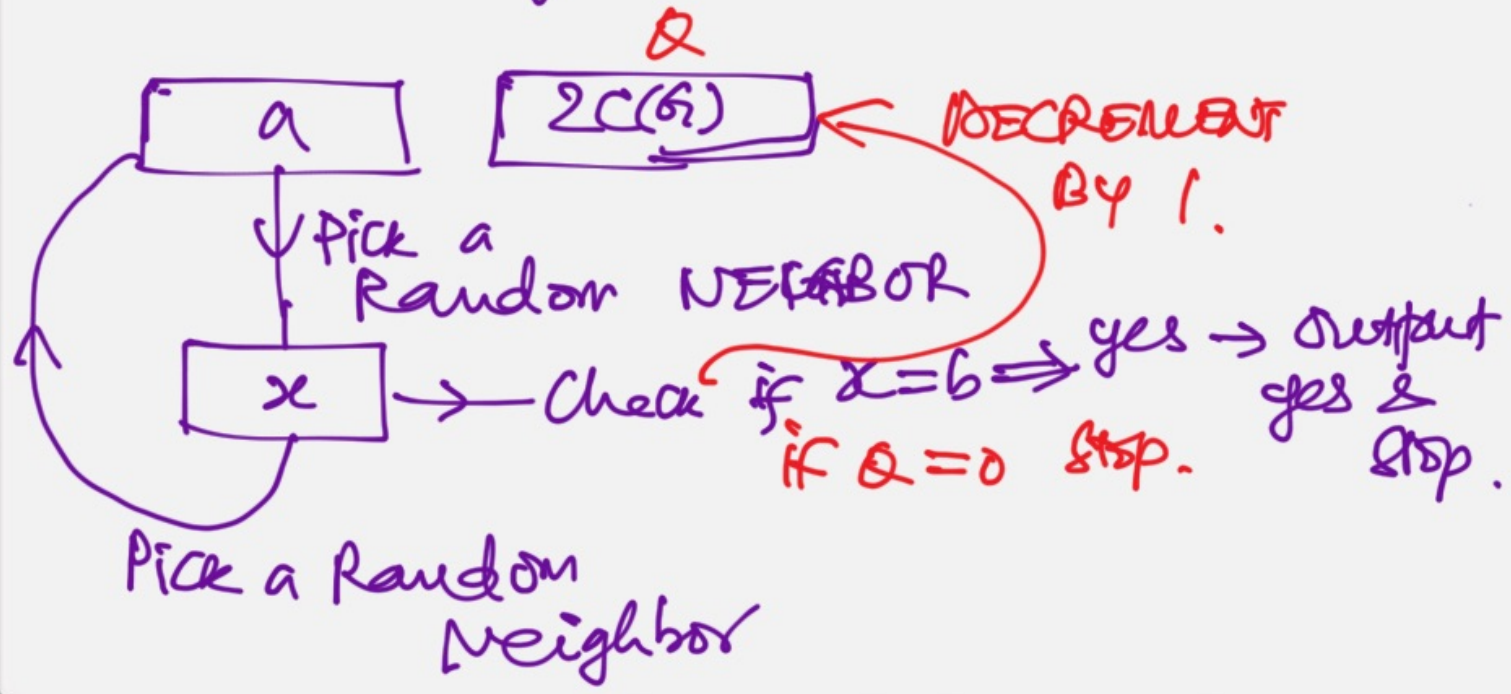
OUTPUT: IS b REACHABLE FROM a ?

DEFN. A PROBLEM $\pi \in RLP$

IF π Can be solved with
 prob. $\geq \frac{1}{2}$ USING A RAND. ALG.
 and LOG-SPACE.

CLAIM! REACHABILITY \in RLP.

IDEA. PERFORM A RANDOM WALK
Starting from a .



IF b IS REACHABLE FROM a ,
PROB. OF NOT VISITING b IN
 $2C(G)$ TIME IS $\leq \frac{1}{2}$.

\Rightarrow PROB. OF AN INCORRECT
ANSWER IS $\leq \frac{1}{2}$.

MATRIX MULTIPLICATION:

INPUT: $A_{n \times n}$ $B_{n \times n}$

Output: $C_{n \times n} = A \cdot B.$

RANDOMIZED APPROXIMATE PRODUCT:

(KANNAN, et al. 2005).

Let $X = K_1, K_2, \dots, K_n.$

Let $S = \sum_{i=1}^n K_i$ - We want to compute $S.$

AN APPROXIMATE ALG.

Pick k elements l_1, l_2, \dots, l_k

RANDOMLY FROM X .

$$\text{Let } Y = \sum_{i=1}^k l_i.$$

Output: $\frac{n}{k} \sum l_i$

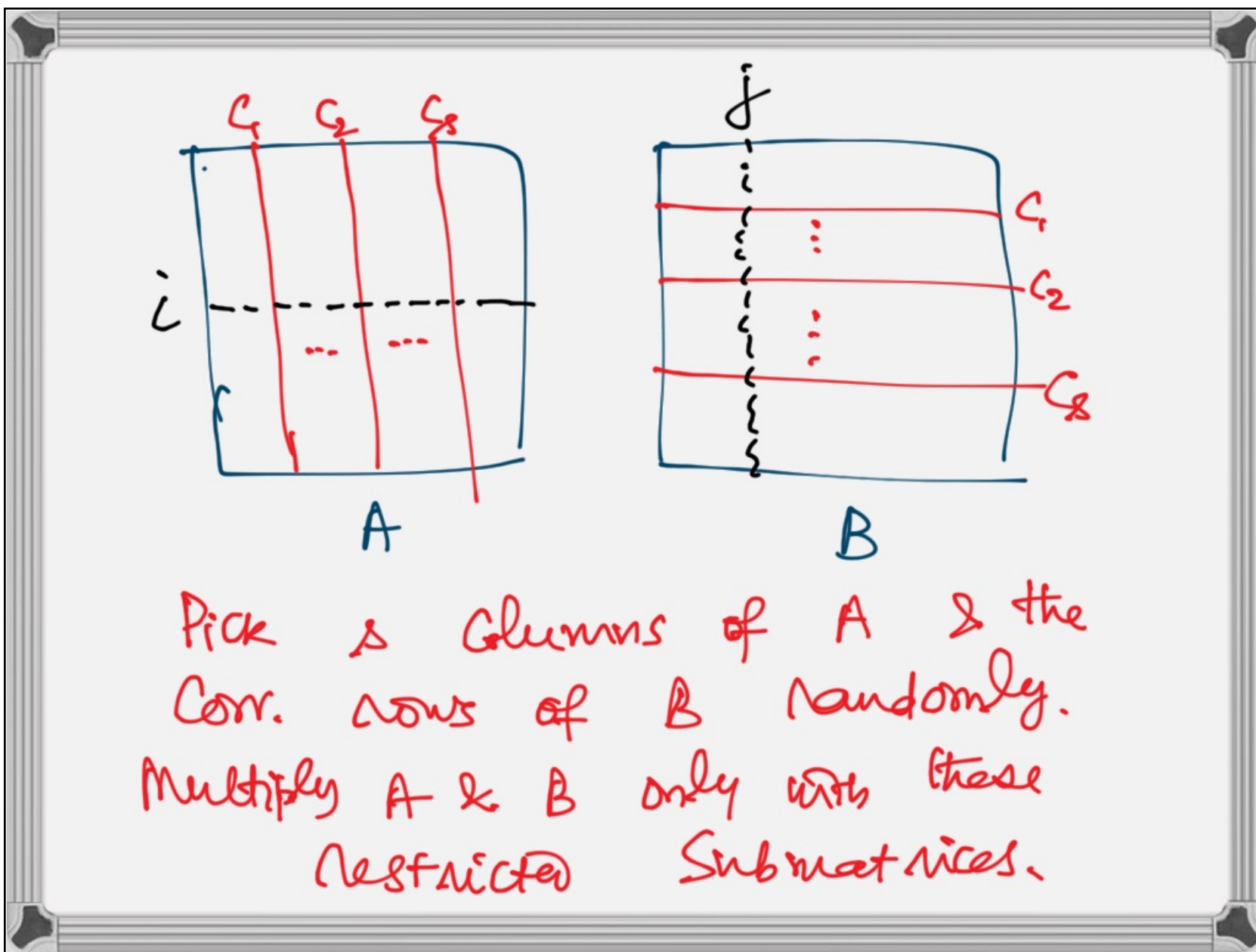
CLAIM! $E\left[\frac{n}{k} Y\right] = S.$

Let x be any sample element.

$$E[x] = \frac{1}{n} \sum_{i=1}^n K_i = \frac{S}{n}.$$

$$\Rightarrow E[y] = \frac{S}{n}.$$

$$\Rightarrow E\left[\frac{n}{s} y\right] = S. \quad \square$$

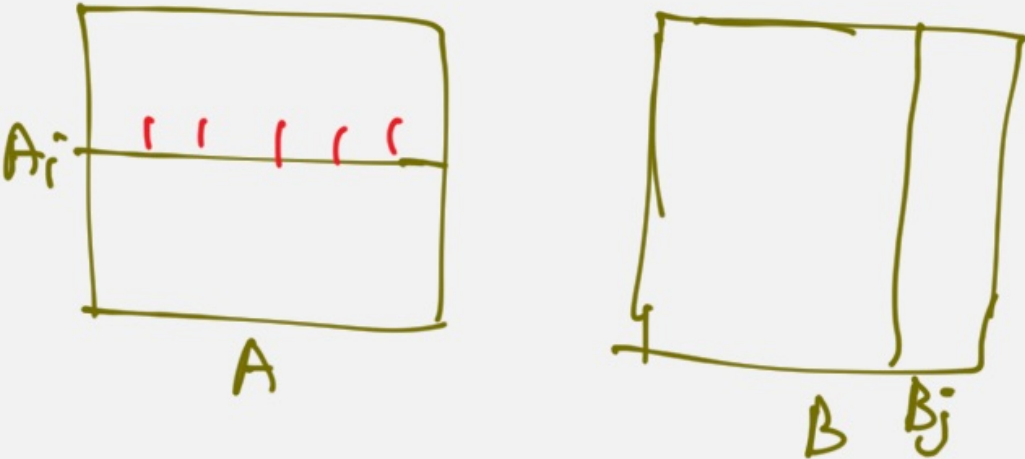


$$C'_{ij} = \sum_{k=1}^s A_{ik} B_{kj} \quad \forall i, j$$

$$\text{RUNTIME} = O(n^2 s)$$

A
SPECIAL CASE:

| | | | | |
|--|---|--|---|--|
| $\begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix}$ | = | $\begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{matrix}$ | = | $\begin{matrix} 2 & 2 & 3 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 1 & 3 & 1 \\ 1 & 2 & 2 & 1 \end{matrix}$ |
| A | | B | | C |



$C_{ij} = \# \text{ of Matching ones}$
 in A_i and $B_j = ?$.

Expected $\# \text{ of MATCHING ones}$
 in the sample $= \frac{1}{n} q$.

Using Chernoff Bounds,
 the # of Matching ones in
 the sample is $\in \left[\frac{2g}{n} \pm c\alpha \sqrt{\frac{2g \log n}{n}} \right]$

\Rightarrow ERROR IN OUR output is w.h.p.

$\pm c\alpha \sqrt{\frac{n}{2} g \log n}$ with prob. $\geq (1 - n^{-\alpha})$.

PROBLEM: PRIMACY TESTING.

INPUT: AN INTEGER n .

OUTPUT: "YES" if n IS PRIME
& "NO" otherwise.

CAN BE solved in $O(\sqrt{n})$ TIME.

MILLER-RABIN'S ALGORITHM:

FERMAT'S THEOREM:

IF p IS PRIME, THEN

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{FOR ANY } a < p.$$

\exists COMPOSITE NUMBERS FOR WHICH
THE ABOVE HOLDS FOR EVERY
 $a < n$.

EX. CARMICHAEL NUMBERS.
eg. 561.

let $(n-1) = b_k b_{k-1} \dots b_1 b_0$ IN BINARY.

$$a^{n-1} = \prod_{i=0}^k b_i 2^i = \prod_{i=0}^k a^{b_i 2^i}$$

$$= \prod_{i=0}^k a^{2^i}$$

$n-1 = 10$
 $= 1010$
 $b_3 b_2 b_1 b_0$

0 1 2 3 4 5 6 7 8 9 10
 $a,$ $a^2,$ $a^4,$ $a^8,$ $a^{16},$ $a^{32},$ $\dots,$ a^{2^k}