COL 702 Lecture 5, Aug 6

Example

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Recall Is $AB \stackrel{?}{=} C$

where addition is modulo 2

Compute $(A\,[B\,X])$ and CX for some non-zero vector X

$X \in \{0,1\}^n$

Suppose $X = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, then $(A\,(BX)) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$CX = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Since $ABX = CX$

the algorithm returns YES, i.e. $AB = C$

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq C$$

What if $X' = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ $ABX' = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ $CX' = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Therefore answer is incorrect !

Suppose $AB = C$, then can it happen that $ABX \neq CX$

NO

$\Rightarrow$ Algorithm will return YES which is the correct answer

Whenever $ABX \neq CX$, algorithm returns NO

$$ABX \stackrel{?}{=} CX$$

$\neq$: Algorithm says NO

Always correct

$=$: Algorithm returns YES

Correct ??
(Not sure !)

When $ABX = CX$, let us try again with another X' to see if $ABX' \stackrel{?}{=} CX'$

Repeat K -times

Until $ABX \neq CX$

pick a vector $(\neq 0)$ distinct

test $ABX \stackrel{?}{=} CX$

random 0-1 vector independently

Return NO

$$(AB - C)X \stackrel{?}{=} 0$$

By choosing a random 0-1 vector as X what is the prob of the following event?

$AB \neq C$ but $ABX = CX$

$\Leftrightarrow$ Given $AB - C \neq 0$ $ABX = CX$

for a nonzero random vector

When $AB - C \neq 0 \Rightarrow$ at least one row $\neq 0$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

say it is i^{th} row r_i

What is the prob that $r_i \cdot X^T = 0$?
for a random X

Claim: The # of good random vectors is 2^{n-1} for any non-zero row vector r_i

$\Rightarrow$ With prob at least half the random vector will give the right answer

The prob of an error after K consecutive YES $\leq \frac{1}{2^K}$

Overall running time is $O(K \cdot n^2)$

Monte Carlo randomized algorithm

Quicksort kind of rand algorithm
Las Vegas