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 \( AB \neq C \)

where addition is modulo 2

Compute \( (A(BX)) \) 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 \( X \in \{0,1\}^n \), i.e. \( AB = C \)

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

What if \( X' = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \), \( ABX' = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \), \( CX' = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \)?
Therefore answer is incorrect!

Suppose \( AB = C \), then can it happen that \( ABX \neq CX \)?

\[
\text{No} \quad \quad \Rightarrow \quad \quad \text{Algorithm will return YES which in the correct answer}
\]

Whenever \( ABX \neq CX \), algorithm returns \( \text{NO} \)?

\[
ABX = CX \\
\neq \quad \neq \quad = \quad \Rightarrow \quad \text{Algorithm returns YES}
\]

Algorithm says \( \text{NO} \)

Always covered

Correct??

(Not sure.)

When \( ABX = CX \), let us try again with another \( X' \) to see if \( ABX' = CX' \).
Repeat $K$ times:

Until $ABX \neq CX$ distinct

pick a vector (≠ 0) test $ABX \neq CX$

Return NO

$\begin{bmatrix}
AB - C
\end{bmatrix} x \neq 0$

By choosing a random 0-1 vector $X$, what is the prob of the following event:

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

(2) Given $AB - C \neq 0$ $ABX = CX$ non-zero for a random vector.

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

$\begin{bmatrix}
0 & 0 & 1 & 0 & 0 & 0
\end{bmatrix}$ say it is in row $r_i$
What is the prob that \( \mathbf{r}_i \cdot \mathbf{X}^T = 0 \)? for a random \( \mathbf{X} \)

Claim: The \( \mathbf{r}_i \) good random vectors in \( 2^{n-1} \) for any non-zero row vector \( \mathbf{r}_i \).

\[ \Rightarrow \] With prob at least half the random vectors 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 random algorithm

Las Vegas