Freivald's Algorithm

Matrix Multiplication Verification : $O(n^2)$

$\Pr(\text{incorrect}) \leq \frac{1}{2}$

$r \in \{0,1\}^n$ $n \times 1$ matrix

$A \times B = C$ $n \times n$ matrice

$x = Br$ ($n \times n$ · $n \times 1$ → $n \times 1$) $y = Ax$ ($n \times n$ · $n \times 1$ → $n \times 1$) $z = Cr$ ($n \times n$ · $n \times 1$ → $n \times 1$)

$\Downarrow$

$y = ABr$ $z = Cr$

$y == z \Longleftrightarrow AB == C$

If $AB = C$, $y = z$

If $AB \neq C$, False Positive

$\Pr(y = z \mid AB \neq C) \leq \frac{1}{2}$

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad C = \begin{bmatrix} 7 & 8 \\ 15 & 22 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \end{bmatrix}$$

$x = Ar$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 2 \\ 4 \end{bmatrix} = \begin{bmatrix} 10 \\ 22 \end{bmatrix}$$

$y = Ax$

$$\begin{bmatrix} 7 & 8 \\ 15 & 22 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 10 \\ 22 \end{bmatrix}$$

$z = Cr \Rightarrow y = z$

Let $D = AB - C$

Assume $AB \neq C$

we know some elements in D is non-zero.

$$D = \begin{bmatrix} \underbrace{d_1, \dots d}_{k} \end{bmatrix} \qquad d^T r = 0$$

$$\sum_{i=1}^{k} d_i r_i = 0$$

设 $d_1 \neq 0$

$\{0,1\}$ flip coin

$$r_1 = \frac{-\sum_{i=2} d_i r_i}{d_1}$$

$$Pr(r = v) \leq \frac{1}{2}$$

A B C

Decrease the probability of error from $\frac{1}{2}$

$\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots$

$(\frac{1}{2})^k$

$O(kn^2)$