Randomized Algorithms
CSCI 432

Matrix Multiplication Verification

5	8	1
3	6	7
4	1	5

A

X

2	4	7
5	1	2
3	6	5

B

=

53	34	56
57	60	68
28	47	55

C

Problem: Given three $n \times n$ matrices A, B, and C, verify that $AB = C$.

Obvious Solution?

Do the multiplication of A and B directly and compare to C.

Running Time?

$O(n^3)$

Freivalds’ Algorithm

Running Time?

$$\underbrace{A}_{O(n^2)}(\underbrace{Br}_{O(n^2)}) = \underbrace{Cr}_{O(n^2)} \quad \Big\} \; O(n^2)$$

$$\underbrace{\underbrace{\begin{bmatrix}5&8&1\\3&6&7\\4&1&5\end{bmatrix}}_{A} \times \underbrace{\left(\underbrace{\begin{bmatrix}2&4&7\\5&1&2\\3&6&5\end{bmatrix}}_{B} \times \underbrace{\begin{bmatrix}1\\0\\1\end{bmatrix}}_{r}\right)}_{\begin{bmatrix}9\\7\\8\end{bmatrix}}}_{\begin{bmatrix}109\\125\\83\end{bmatrix}} = \overbrace{\underbrace{\begin{bmatrix}53&34&56\\57&60&68\\28&47&55\end{bmatrix}}_{C} \times \underbrace{\begin{bmatrix}1\\0\\1\end{bmatrix}}_{r}}^{\begin{bmatrix}109\\125\\83\end{bmatrix}}$$

Freivalds’ Algorithm (on input A, B, C):

1. Generate $n \times 1$ vector r containing random 0 or 1 values.
2. Check if $A(Br) = Cr$.
3. If yes, return **True**. If no, return **False**.

Freivalds' Algorithm

What is the probability of a false negative?

Zero. If $AB = C$, then $(AB)r = Cr$ and $A(B$
Cr.

If $AB = C$, Freivalds' never returns false.

$$\underset{A}{\begin{bmatrix} 5 & 8 & 1 \\ 3 & 6 & 7 \\ 4 & 1 & 5 \end{bmatrix}} \times \left(\underset{B}{\begin{bmatrix} 2 & 4 & 7 \\ 5 & 1 & 2 \\ 3 & 6 & 5 \end{bmatrix}} \times \underset{r}{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}} \right) = \underset{C}{\begin{bmatrix} 53 & 34 & 56 \\ 57 & 60 & 68 \\ 28 & 47 & 55 \end{bmatrix}} \times \underset{r}{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}}$$

Error Types:

1. ~~False Negative. $AB = C$, but Freivalds' says **false**.~~
2. False Positive. $AB \neq C$, but Freivalds' says **true**.

Freivalds' Algorithm (on input A, B, C):

1. Generate $n \times 1$ vector r containing random 0 or 1 values.
2. Check if $A(Br) = Cr$.
3. If yes, return **True**. If no, return **False**.

Freivalds' Algorithm

$$\underbrace{\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}_{A} \times \left(\begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}_{B} \times \begin{bmatrix}1\\1\\1\end{bmatrix}_{r}\right)}_{\begin{bmatrix}1\\0\\0\end{bmatrix}} = \overbrace{\begin{bmatrix}0&0&1\\0&0&0\\0&0&0\end{bmatrix}_{C} \times \begin{bmatrix}1\\1\\1\end{bmatrix}_{r}}^{\begin{bmatrix}1\\0\\0\end{bmatrix}}$$

Error Types:

1. ~~False Negative. $AB = C$, but Freivalds' says **false**.~~
2. False Positive. $AB \neq C$, but Freivalds' says **true**.

Freivalds' Algorithm (on input A, B, C):

1. Generate $n \times 1$ vector r containing random 0 or 1 values.
2. Check if $A(Br) = Cr$.
3. If yes, return **True**. If no, return **False**.

Freivalds' Follies

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

Freivalds' Follies

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

$$\underbrace{\begin{bmatrix} - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{bmatrix}}_{D} \times \underbrace{\begin{bmatrix} {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \end{bmatrix}}_{r} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Freivalds' Follies

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

$$\underbrace{\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boldsymbol{d_j} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{D} \times \underbrace{\begin{bmatrix} {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \end{bmatrix}}_{r} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Freivalds' Follies

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

$$\underset{D}{\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boldsymbol{d_j} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} \times \underset{r}{\begin{bmatrix} {}^{0}/_{1} \\ {}^{0}/_{1} \\ {}^{0}/_{1} \\ 0 \\ {}^{0}/_{1} \end{bmatrix}} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

For D very close to 0, it would not be hard to get $Dr = 0$.

Freivalds' Follies

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

$$\underset{D}{\begin{bmatrix} \boldsymbol{a} & 0 & 0 & 0 & \boldsymbol{b} \\ 0 & 0 & \boldsymbol{c} & 0 & 0 \\ 0 & \boldsymbol{e} & 0 & \boldsymbol{d} & 0 \\ \boldsymbol{h} & 0 & 0 & \boldsymbol{f} & \boldsymbol{g} \\ 0 & 0 & \boldsymbol{i} & 0 & 0 \end{bmatrix}} \times \underset{r}{\begin{bmatrix} {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \\ {}^0/_1 \end{bmatrix}} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

For D very close to 0, it would not be hard to get $Dr = 0$.

Freivalds' Follies

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

$$\underset{D}{\begin{bmatrix} \boldsymbol{a} & 0 & 0 & 0 & \boldsymbol{b} \\ 0 & 0 & \boldsymbol{c} & 0 & 0 \\ 0 & \boldsymbol{e} & 0 & \boldsymbol{d} & 0 \\ \boldsymbol{h} & 0 & 0 & \boldsymbol{f} & \boldsymbol{g} \\ 0 & 0 & \boldsymbol{i} & 0 & 0 \end{bmatrix}} \times \underset{r}{\begin{bmatrix} ^0/_1 \\ ^0/_1 \\ ^0/_1 \\ ^0/_1 \\ ^0/_1 \end{bmatrix}} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

For D very close to 0, it would not be hard to get $Dr = 0$.

For D very far from 0, it requires substantially more luck to get $Dr = 0$.

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \dots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S, & \text{if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \dots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S, & \text{if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \dots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

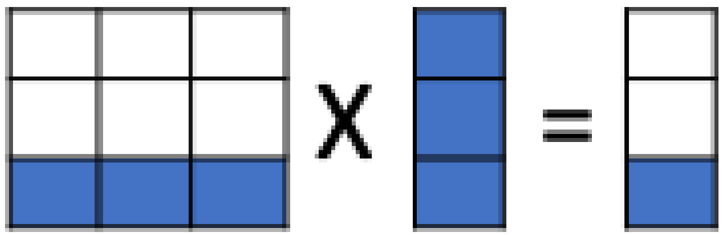
$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S \quad , \text{if } r_j = 0 \\ d_j + S, \text{if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

$Dr = 0$ requires $b \cdot r = 0$ for every row b of D.



Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \dots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S & \text{, if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

$Dr = 0$ requires $b \cdot r = 0$ for every row b of D. So, the probability that $Dr = 0$ must be $\leq$ the probability that $b \cdot r = 0$ for any individual row b.

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \dots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S & \text{, if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

$Dr = 0$ requires $b \cdot r = 0$ for every row b of D. So, the probability that $Dr = 0$ must be $\leq$ the probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0]$

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \ldots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S, & \text{if } r_j = 0 \\ d_j + S, & \text{if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

$Dr = 0$ requires $b \cdot r = 0$ for every row b of D. So, the probability that $Dr = 0$ must be $\leq$ the probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose $D \neq 0$. Then at least one element of D must be nonzero (d_j). Let $d = (d_1, d_2, \dots, d_n)$ be the row containing d_j. Freivalds' fails if $Dr = 0$, which requires $d \cdot r = 0$. Then,

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i + d_j r_j + \sum_{i=j+1}^{n} d_i r_i = d_j r_j + \sum_{i \neq j} d_i r_i = d_j r_j + S$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S & \text{, if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since $d_j \neq 0$. Thus, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$

$Dr = 0$ requires $b \cdot r = 0$ for every row b of D. So, the probability that $Dr = 0$ must be $\leq$ the probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow \boldsymbol{Pr[\text{Freivalds' returns true} | AB \neq C] \leq \frac{1}{2}}$

Freivalds' Error Analysis

Freivalds' fails when:

$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

i.e., if $D = AB - C$, when $D \neq 0$ and $Dr = 0$

What is the probability that Freivalds' fails?

$$\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] = \Pr[Dr = 0 | D \neq 0] = ?$$

Suppose D … $\dots, d_n)$

be the row

d

So,

d

S and $d_j +$

$Dr = 0$ req … $\leq$ the

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow$ ***Pr*[Freivalds' returns true|*AB* ≠ *C*] ≤ $\frac{1}{2}$**

Freivalds' Error Analysis

- Where is the error?

  $AB \neq C$, but Freivalds' returns **true**.

- What conditions lead to the error?

  $AB - C \neq 0$, but $(AB - C)r = 0$.

- How likely is the error?

  $\Pr[\text{Freivalds' returns } \mathbf{true} | AB \neq C] \leq \frac{1}{2}$

- How do we mitigate the error?

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that?

Freivalds' Amplification

Probability Product Rule:
For independent events E and F,
$\Pr[E \cap F] = \Pr[E] \times \Pr[F]$

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that?

Freivalds' Amplification

Probability Product Rule:
For independent events E and F,
$\Pr[E \cap F] = \Pr[E] \times \Pr[F]$

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

Amplification: Running a randomized algorithm (independently) multiple times to boost the probability of correctness.

Freivalds' Amplification

Probability Complement Rule:
$\Pr[\text{not } E] = 1 - \Pr[E]$

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

$\Rightarrow$ Probability we get correct answer $\geq 1 - \frac{1}{4}$

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

$\Rightarrow$ Probability we get correct answer $\geq 1 - \frac{1}{4}$

What if we do it k times?

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

$\Rightarrow$ Probability we get correct answer $\geq 1 - \frac{1}{4}$

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

$\Rightarrow$ Probability we get correct answer $\geq 1 - \frac{1}{4}$

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

k	Probability we are right
1	0.5
2	0.75
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

$\Rightarrow$ Probability we get correct answer $\geq 1 - \frac{1}{4}$

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

k	Probability we are right
1	0.5
2	0.75
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

Freivalds' Amplification

Problem: If the input instance is wrong (i.e., $AB \neq C$) , Freivalds' has as much as a 50% chance of being incorrect.

Solution: What if we run Freivalds' (independently) twice and return **false** if either run returned **false**? We are wrong only if both runs were wrong.

What is the probability of that? $\leq \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

$\Rightarrow$ Probability we get correct answer $\geq 1 - \frac{1}{4}$

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

$$O(kn^2) \in O(n^2), \text{ if } k \text{ is a fixed constant}$$

k	Probability we are right
1	0.5
2	0.75
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

Fre

An event occurs **with high probability** if its probability goes to 1 as n goes to infinity.

Problem:
much as a

Solution:
if either ru

What is th

⇒ Probab

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

$$O(kn^2) \in O(n^2), \text{ if } k \text{ is a fixed constant}$$

	t
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

Fre

An event occurs **with high probability** if its probability goes to 1 as n goes to infinity. So, running Freivalds' for a fixed k number of runs does not qualify as succeeding with high probability.

Problem:
much as a

Solution:
if either r

What is th

$\Rightarrow$ Probab

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

$$O(kn^2) \in O(n^2)\text{, if } k \text{ is a fixed constant}$$

	t
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

Fre

Problem:

much as a

Solution:

if either r

What is th

⇒ Probab

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

$$O(kn^2) \in O(n^2) \text{, if } k \text{ is a fixed constant}$$

	t
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

An event occurs **with high probability** if its probability goes to 1 as n goes to infinity. So, running Freivalds' for a fixed k number of runs does not qualify as succeeding with high probability.

But, if we let $k = \log_2 n$, the probability of running it k times succeeding becomes at least:

$$1 - \frac{1}{2^{\log_2 n}} = 1 - \frac{1}{n} \xrightarrow[n \to \infty]{} 1$$

Fre

An event occurs **with high probability** if its probability goes to 1 as n goes to infinity. So, running Freivalds' for a fixed k number of runs does not qualify as succeeding with high probability.

But, if we let $k = \log_2 n$, the probability of running it k times succeeding becomes at least:

$$1 - \frac{1}{2^{\log_2 n}} = 1 - \frac{1}{n} \xrightarrow[n \to \infty]{} 1$$

Running time:

$$O(n^2 \log n) \in o(n^{2+\varepsilon}), \forall \varepsilon > 0$$

Problem:

much as a

Solution:

if either r

What is th

$\Rightarrow$ Probab

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

$$O(kn^2) \in O(n^2), \text{ if } k \text{ is a fixed constant}$$

	t
5	0.97
10	0.99902
20	0.99999905
50	0.9999999999999991

Freivalds' Error Analysis

- Where is the error?

  $AB \neq C$, but Freivalds' returns **true**.

- What conditions lead to the error?

  $AB - C \neq 0$, but $(AB - C)r = 0$.

- How likely is the error?

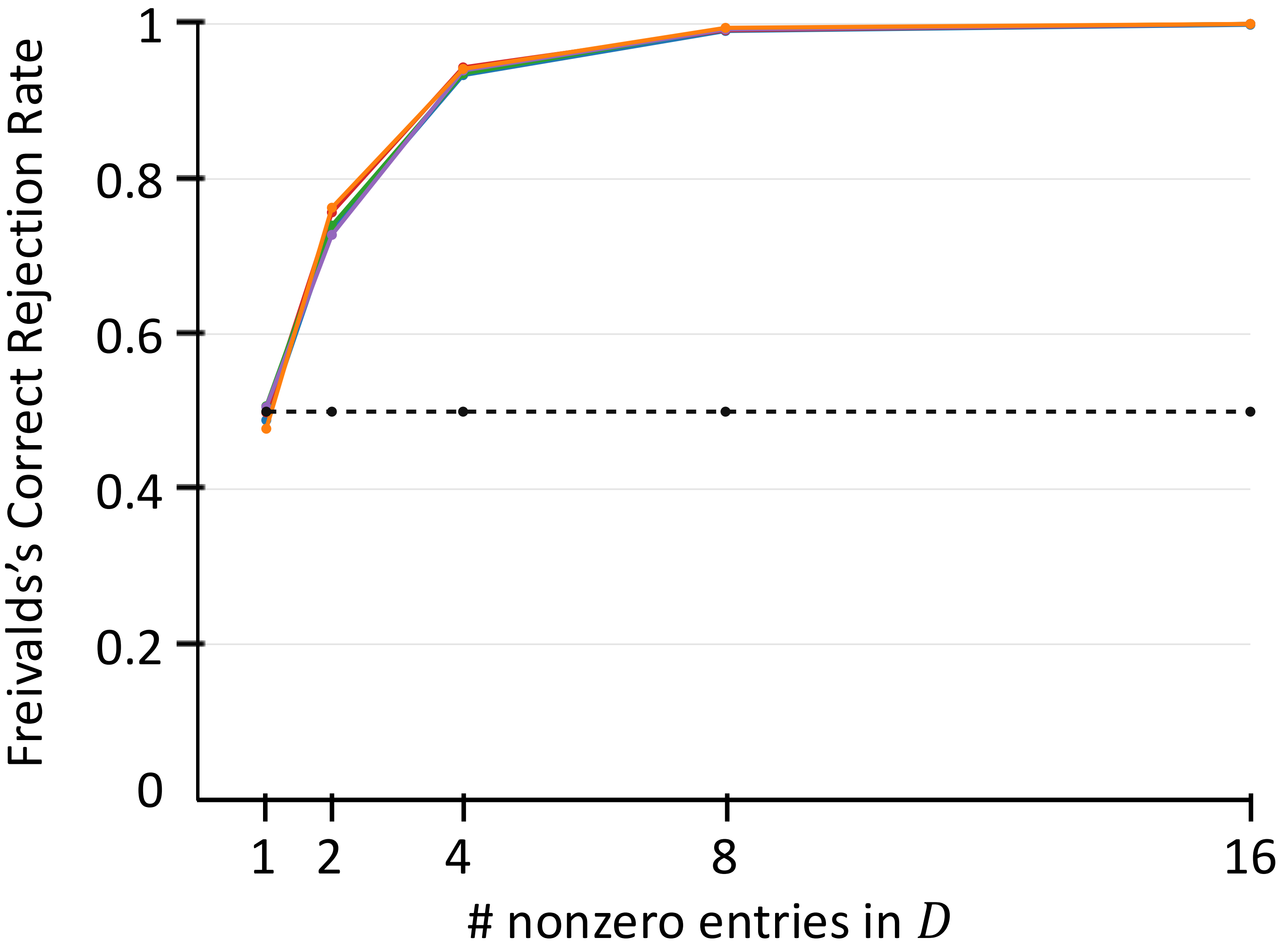
  $\Pr[\text{Freivalds' returns } \textbf{true} | AB \neq C] \leq \frac{1}{2}$

- How do we mitigate the error?

  Repeat Freivald's k times to push error to $\leq \frac{1}{2^k}$

Freivalds' in Practice

Accuracy of Freivalds' as number of nonzero entries in D increases.



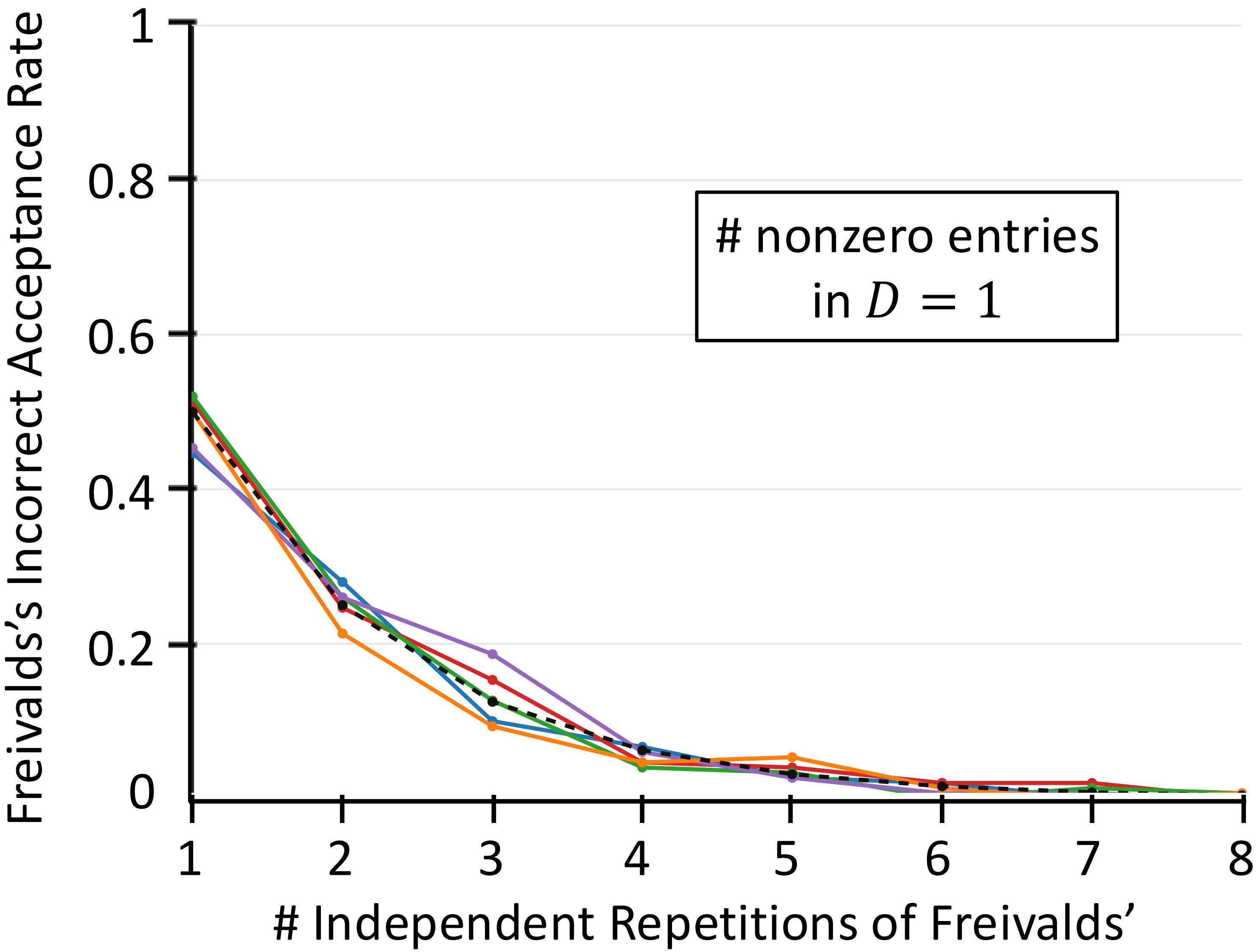
Notes:

- 64x64-sized matrices
- 5,000 runs per data point.

Experiments conducted by Blake Sigmundstad

Freivalds' in Practice

Performance of amplification on worst-case scenario.



Notes:

- 64x64-sized matrices
- 5,000 runs per data point.
- Different types of matrices considered (e.g., Sparse, Dense, Binary,…)

Experiments conducted by Blake Sigmundstad

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

Freivalds' Improvement

0

Where does the 2 come from?

What is the probability that Freivalds'

Pr[Freivalds' returns **true**$|AB$

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S\text{,} & \text{if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow$ ***Pr*[Freivalds' returns true$|AB \neq C] \leq \frac{1}{2}$**

Freivalds' Improvement

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

0

What is the probability that Freivalds'

$\Pr[$Freivalds' returns **true**$|AB$

Where does the 2 come from?

From the fact there are 2 options for r_j.

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S, & \text{if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow Pr[$**Freivalds' returns true**$|AB \neq C] \leq \frac{1}{2}$

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

Freivalds' Improvement

What is the probability that Freivalds'

Pr[Freivalds' returns **true**$|AB$

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S & \text{, if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow$ ***Pr[Freivalds' returns true$|AB \neq C] \leq \frac{1}{2}$***

Where does the 2 come from?

From the fact there are 2 options for r_j.

What can we do to make that probability smaller?

Freivalds' Improvement

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

What is the probability that Freivalds'

Pr[Freivalds' returns **true**$|AB$

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S & \text{, if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow Pr$[Freivalds' returns true$|AB \neq C] \leq \frac{1}{2}$

Where does the 2 come from?

From the fact there are 2 options for r_j.

What can we do to make that probability smaller?

Provide more options for r_j.

How many options?

Freivalds' Improvement

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

0

What is the probability that Freivalds'

Pr[Freivalds' returns **true**$|AB$

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

$$d \cdot r = \begin{cases} S & \text{, if } r_j = 0 \\ d_j + S & \text{, if } r_j = 1 \end{cases}$$

S and $d_j + S$ can't both equal 0, since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

$\Rightarrow Pr$[Freivalds' returns true$|AB \neq C] \leq \frac{1}{2}$

Where does the 2 come from?

From the fact there are 2 options for r_j.

What can we do to make that probability smaller?

Provide more options for r_j.

How many options?

If we provide n options, probability of being incorrect $\leq \frac{1}{n}$, which fits the definition of "with high probability" without needing amplification!

Freivalds' Improvement

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

0

What is the probability that Freivalds'

Pr[Freivalds' returns **true**$|AB$

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

S , if $r_j = 0$

1

Running Time?

S ar ... since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

Where does the 2 come from?

From the fact there are 2 options for r_j.

What can we do to make that probability smaller?

Provide more options for r_j.

How many options?

If we provide n options, probability of being incorrect $\leq \frac{1}{n}$, which fits the definition of "with high probability" without needing amplification!

$\Rightarrow Pr$**[Freivalds' returns true**$|AB \neq C] \leq \frac{1}{2}$

Fre

An event occurs **with high probability** if its probability goes to 1 as n goes to infinity. So, running Freivalds' for a fixed k number of runs does not qualify as succeeding with high probability.

But, if we let $k = \log_2 n$, the probability of running it k times succeeding becomes at least:

$$1 - \frac{1}{2^{\log_2 n}} = 1 - \frac{1}{n} \xrightarrow[n \to \infty]{} 1$$

Running time:

$$O(n^2 \log n) \in o(n^{2+\varepsilon}), \forall \varepsilon > 0$$

Problem:

much as a

Solution:

if either r

What is th

$\Rightarrow$ Probab

What if we do it k times?

$$\Pr[\text{correct answer}] \geq 1 - \frac{1}{2^k}$$

Running time consequences?

$$O(kn^2) \in O(n^2), \text{ if } k \text{ is a fixed constant}$$

	t
5	0.97
10	0.99902
20	0.99999905
50	0.999999999999991

Freivalds' Improvement

Freivalds' fails when:

$AB - C \neq 0$ and $(AB - C)r = 0$

0

What is the probability that Freivalds'

$\Pr[\text{Freivalds' returns } \textbf{true} | AB$

Suppose $D \neq 0$. Then at least one ele

be the row containing d_j. Freivalds' fa

$$d \cdot r = \sum_{i=1}^{n} d_i r_i = \sum_{i=1}^{j-1} d_i r_i +$$

So,

S , if $r_j = 0$

1

Running Time?

$\boldsymbol{O(n^2 \log n)}$ **vs** $\boldsymbol{O(n^2)}$

S ar since

$Dr = 0$ requires $b \cdot r = 0$ for every ro

probability that $b \cdot r = 0$ for any individual row b.

I.e., $\Pr[Dr = 0 | D \neq 0] \leq \Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$.

Where does the 2 come from?

From the fact there are 2 options for r_j.

What can we do to make that probability smaller?

Provide more options for r_j.

How many options?

If we provide n options, probability of being incorrect $\leq \frac{1}{n}$, which fits the definition of "with high probability" without needing amplification!

$\Rightarrow$ ***Pr*****[Freivalds' returns true$|AB \neq C] \leq \frac{1}{2}$**