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 $AB = C$.

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

Obvious Solution?

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

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.

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

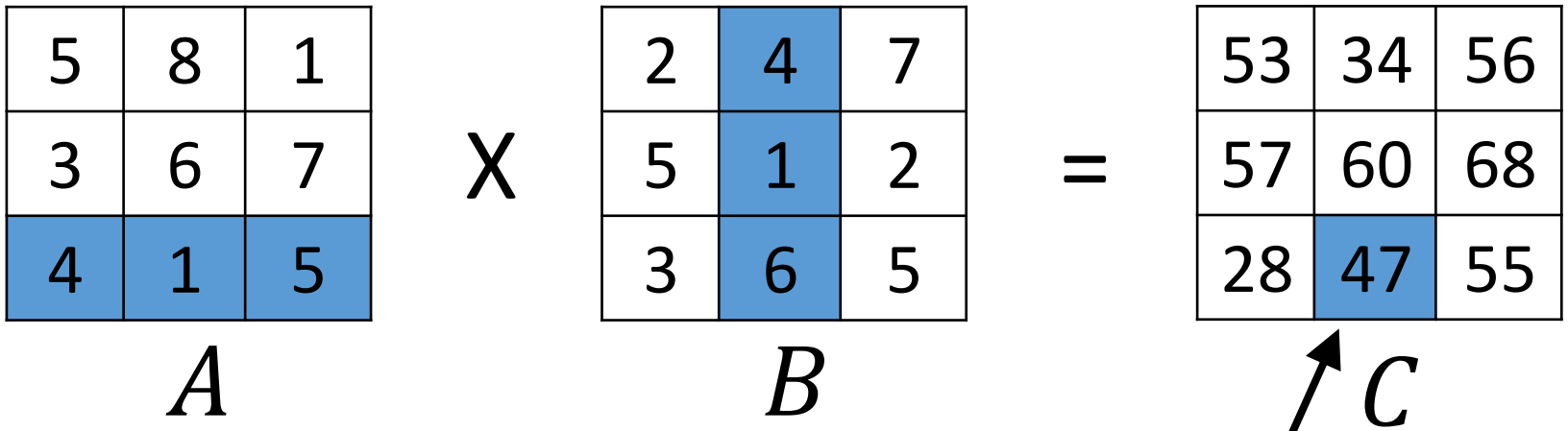
Problem: Given three $n \times n$ matrices A, B, and C, verify that $AB = C$.

Obvious Solution?

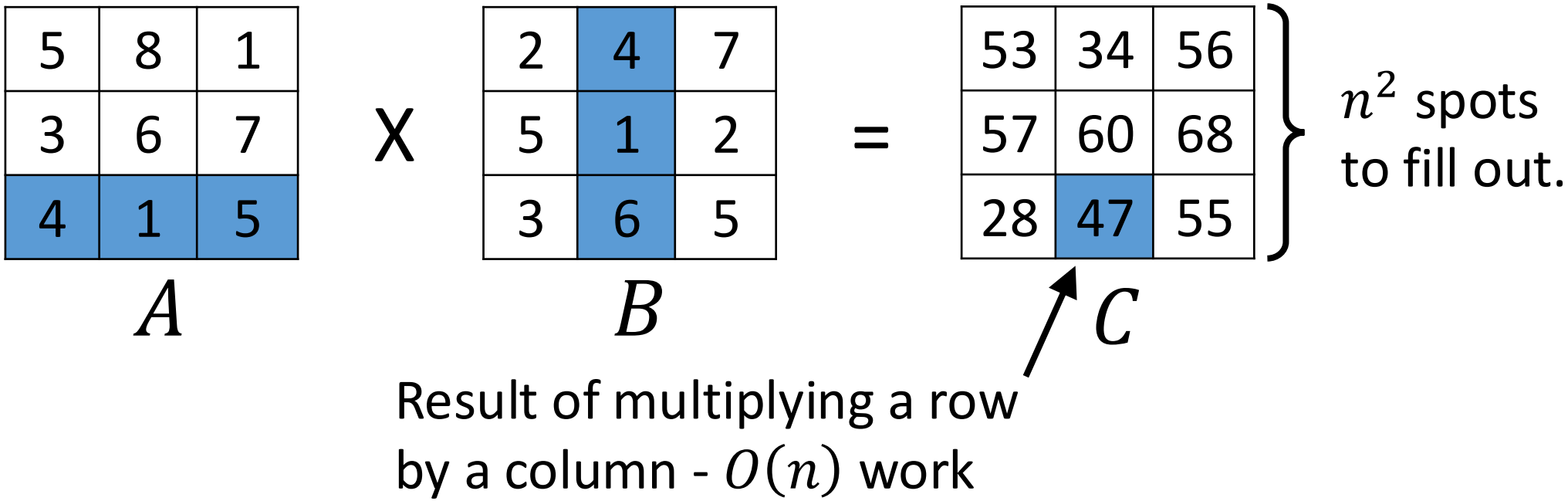
Do the multiplication of A and B directly and compare to C.

Running Time?

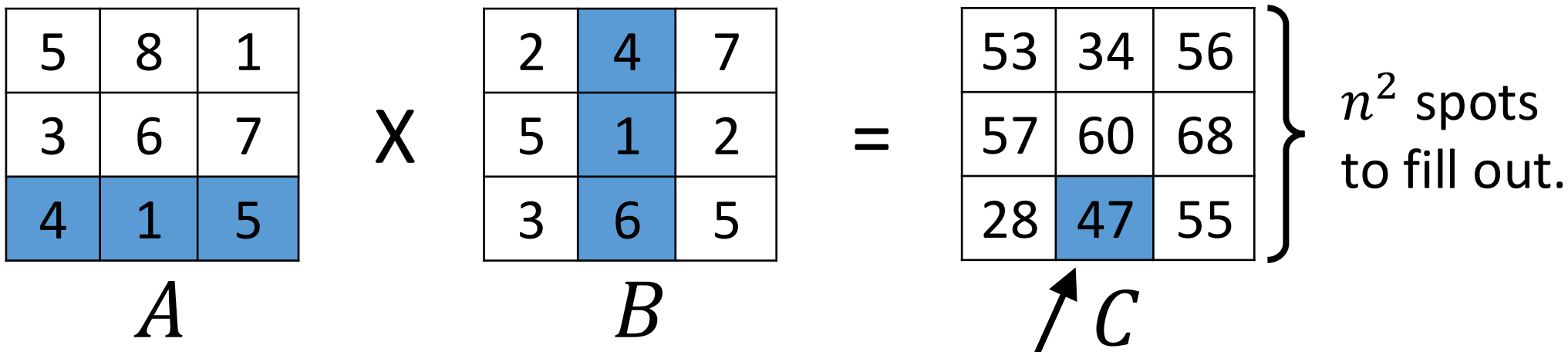
Matrix Multiplication



Matrix Multiplication



Matrix Multiplication



Thus, $O(n^3)$ total running time.

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

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

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

1.

2.

3.

Freivalds' Algorithm

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

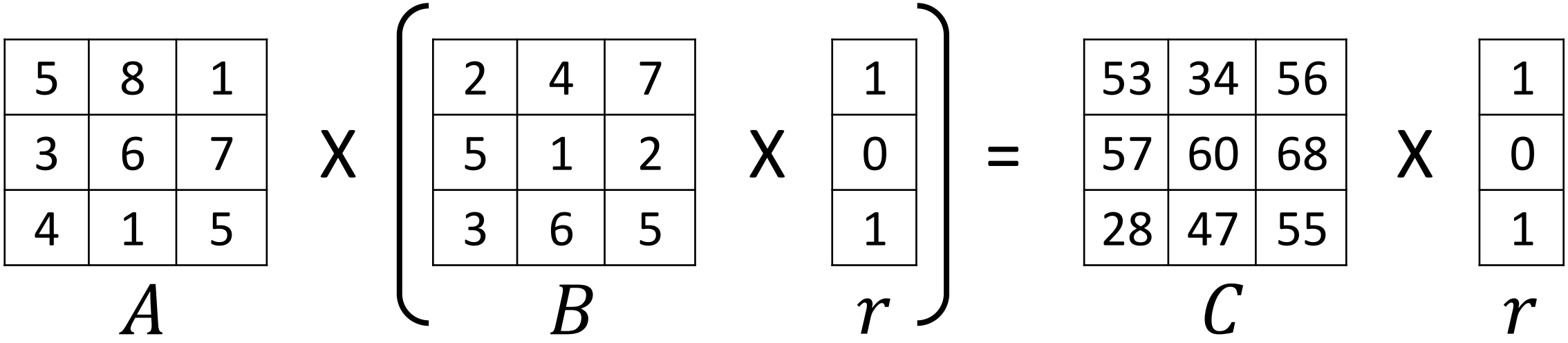
$r =$

1
0
1

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

1. Generate $n \times 1$ vector r containing random 0 or 1 values.
2.
3.

Freivalds' Algorithm

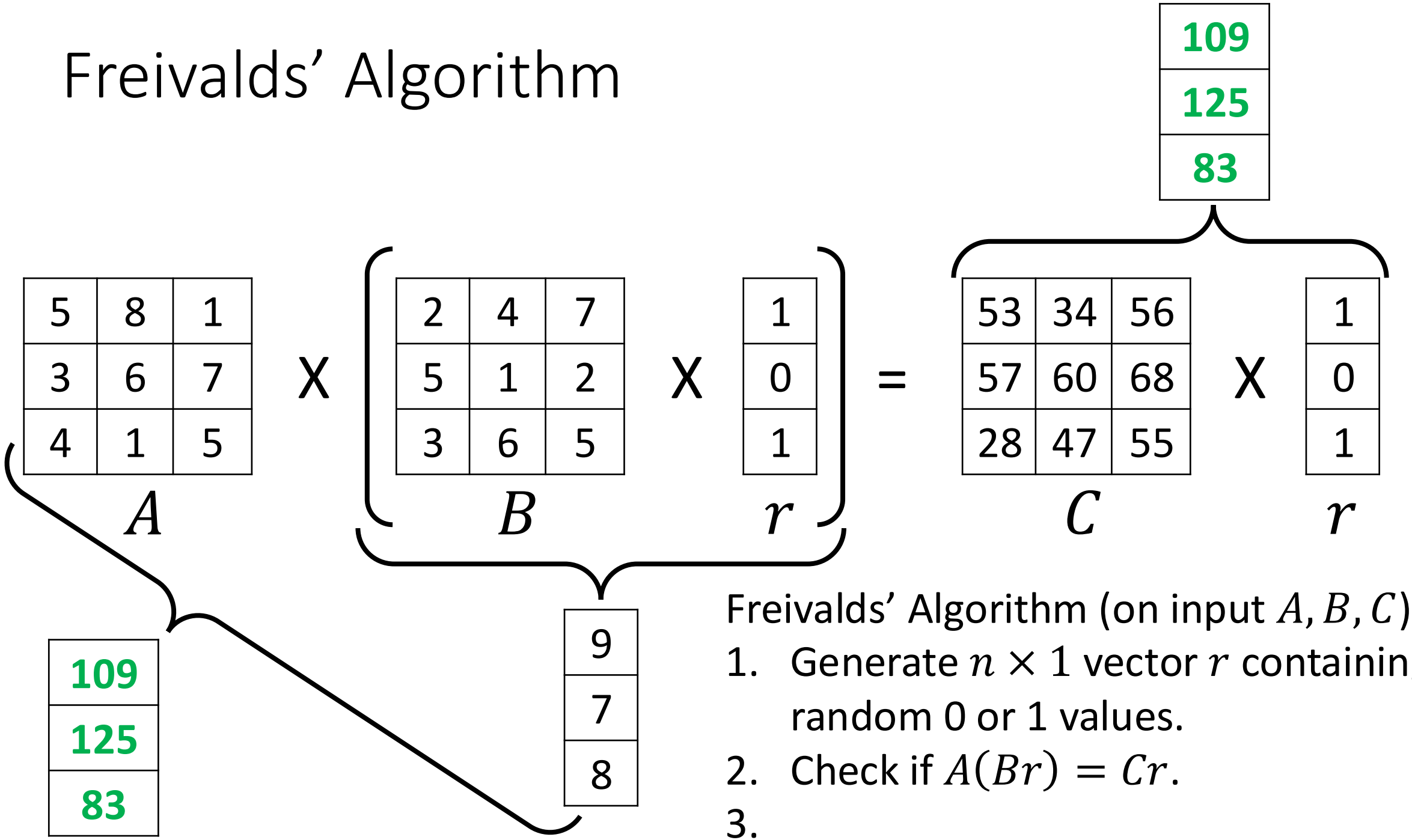


$$r = \begin{array}{|c|}\hline 1 \\ \hline 0 \\ \hline 1 \\ \hline \end{array}$$

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.

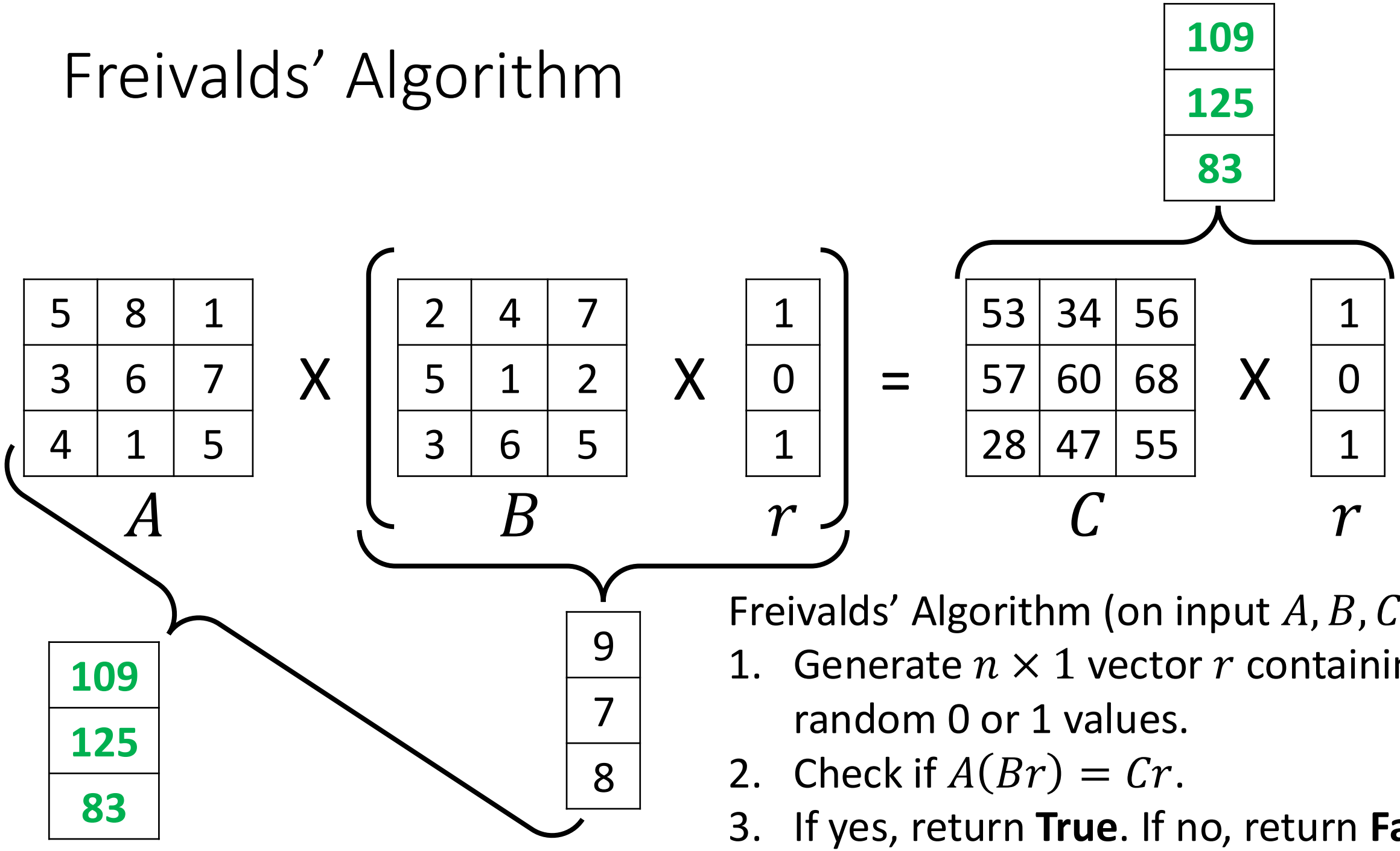
Freivalds' Algorithm



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.

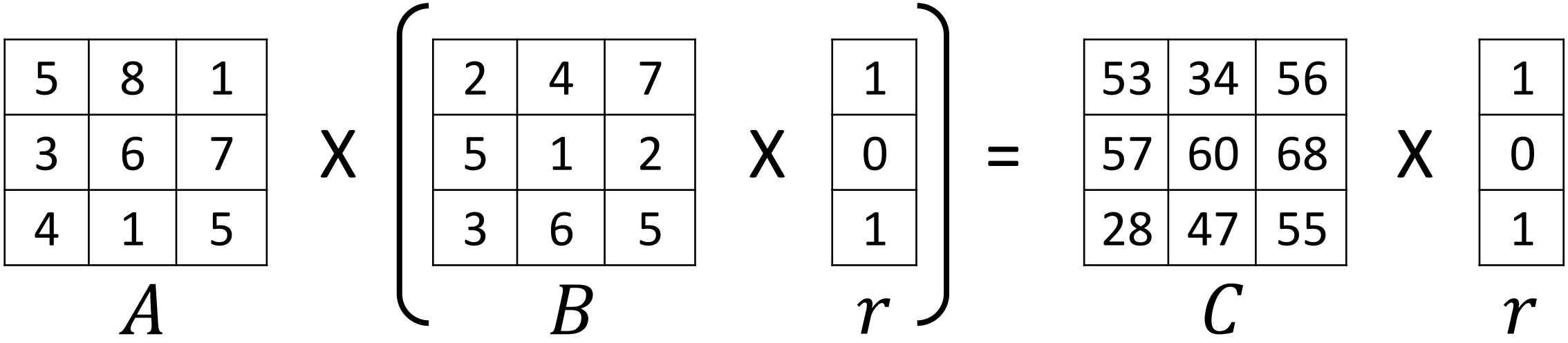
Freivalds' Algorithm



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

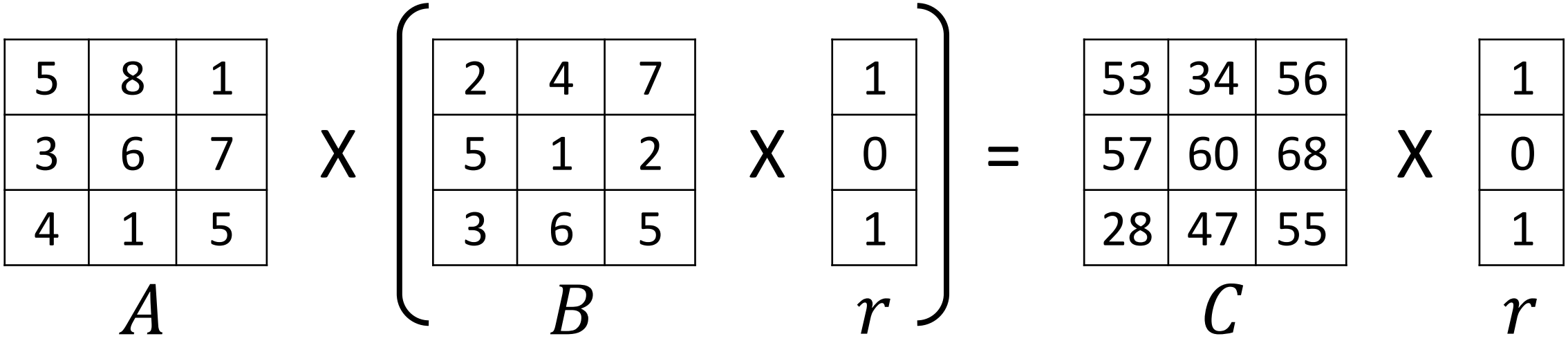


$A(Br) = (AB)r$, so if $AB = C$, then $A(Br) = (AB)r = Cr$

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



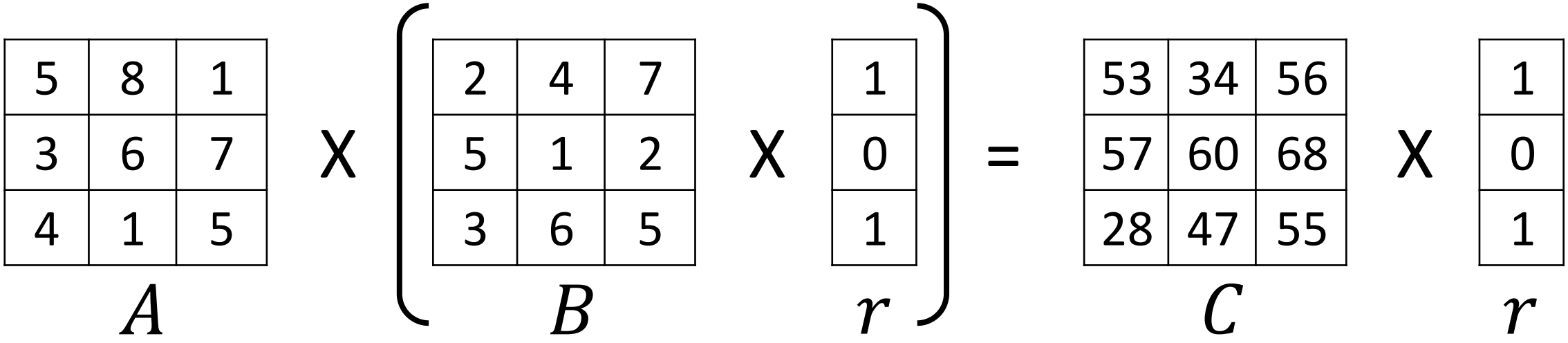
Randomness (generally) impacts an algorithm's correctness or running time.

	Correctness	Running Time
Monte Carlo	Random	Bounded
Las Vegas	Guaranteed	Random

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



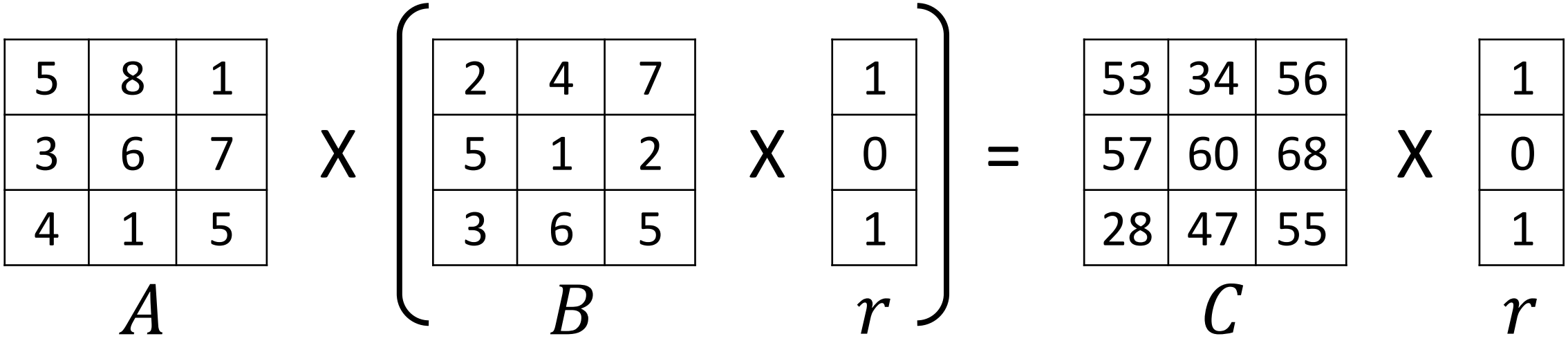
Randomness (generally) impacts an algorithm's correctness or running time.

	Correctness	Running Time
Monte Carlo	Random	Bounded
Las Vegas	Guaranteed	Random

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

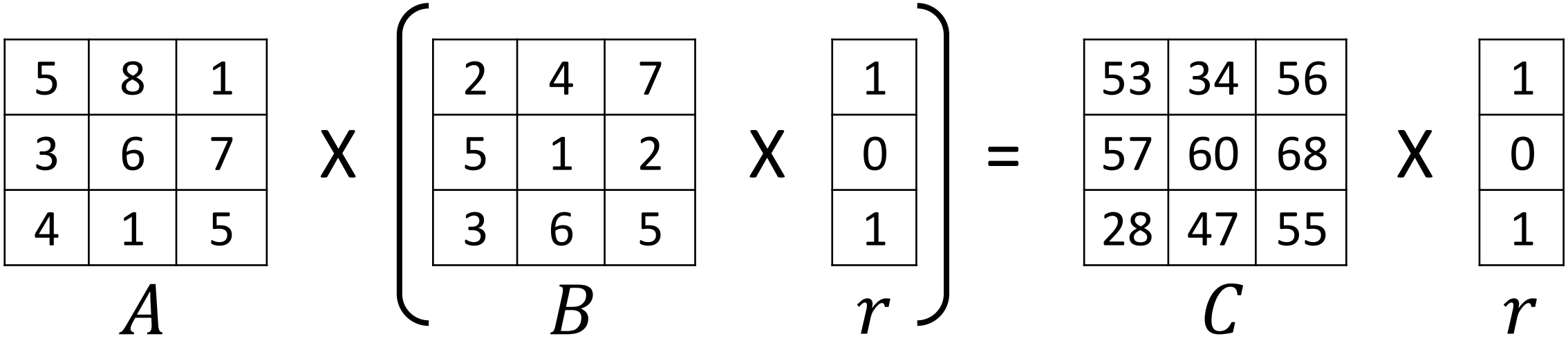


Running Time?

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



Running Time?

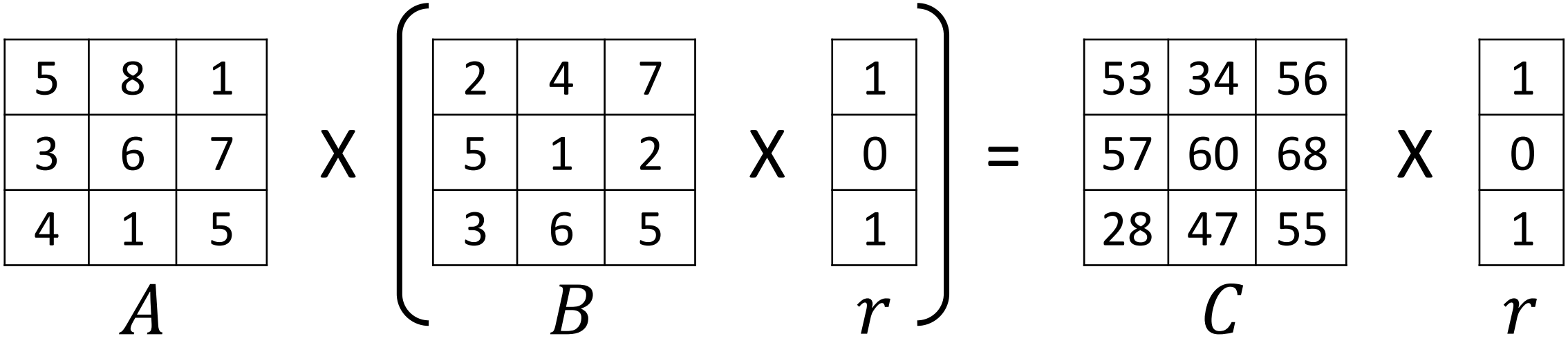
$$A(Br) = Cr$$

? ? ?

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



Running Time?

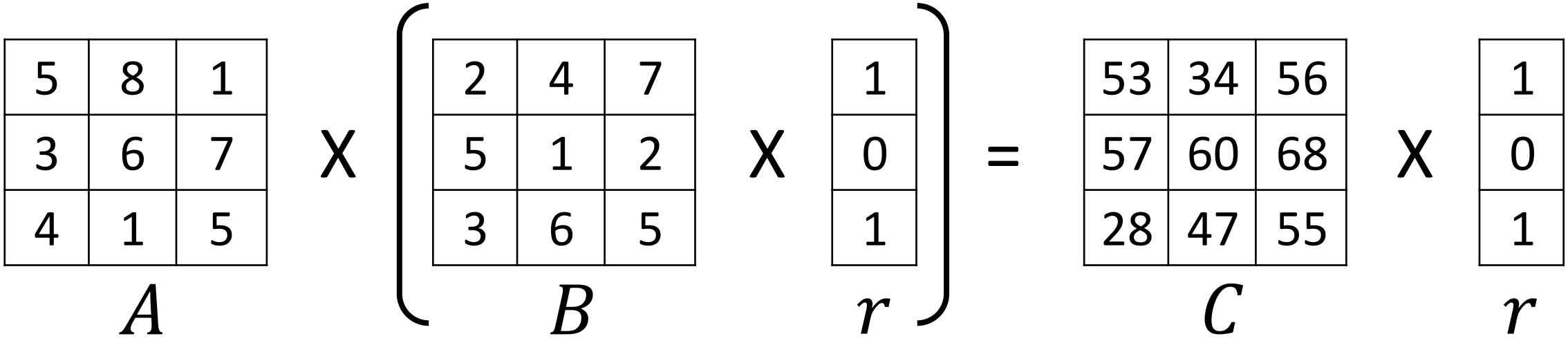
$$A(Br) = Cr$$

$O(n^2)$ $O(n^2)$ $O(n^2)$

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



Running Time?

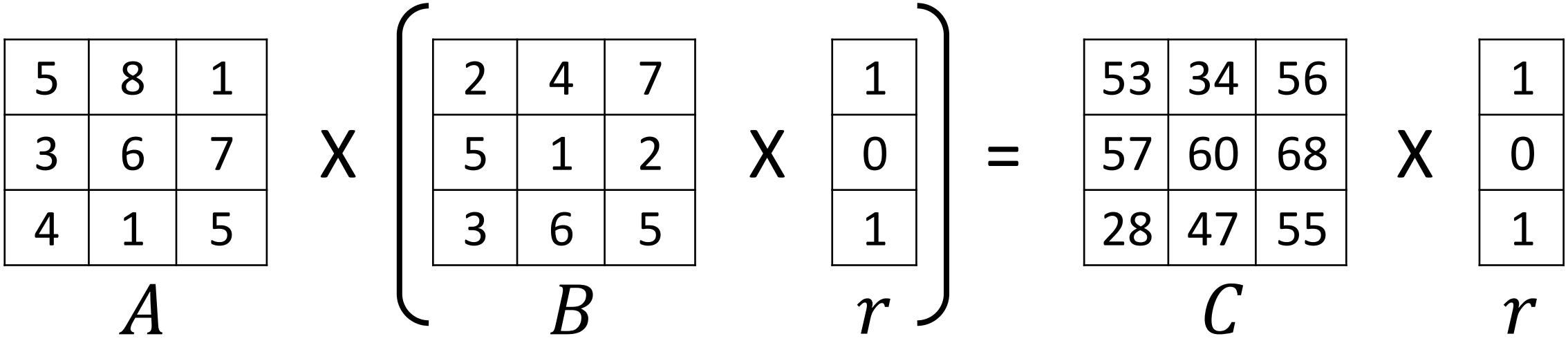
$$A(Br) = Cr$$

$O(n^2)$ $O(n^2)$ $O(n^2)$ } $O(n^2)$

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



Running Time?

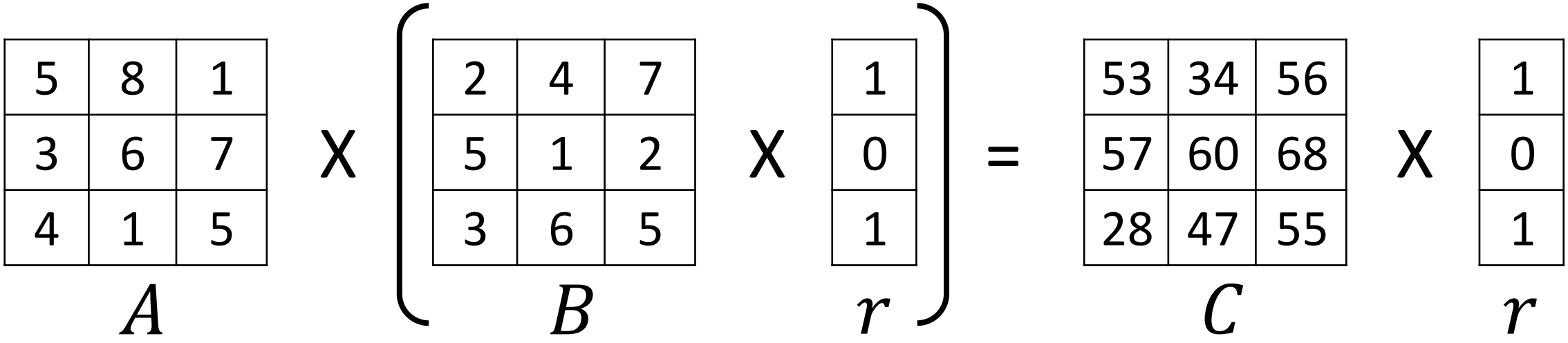
$$(AB)r = Cr$$

$O(n^3)$ $O(n^2)$ $O(n^2)$ } $O(n^3)$

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



Running Time?

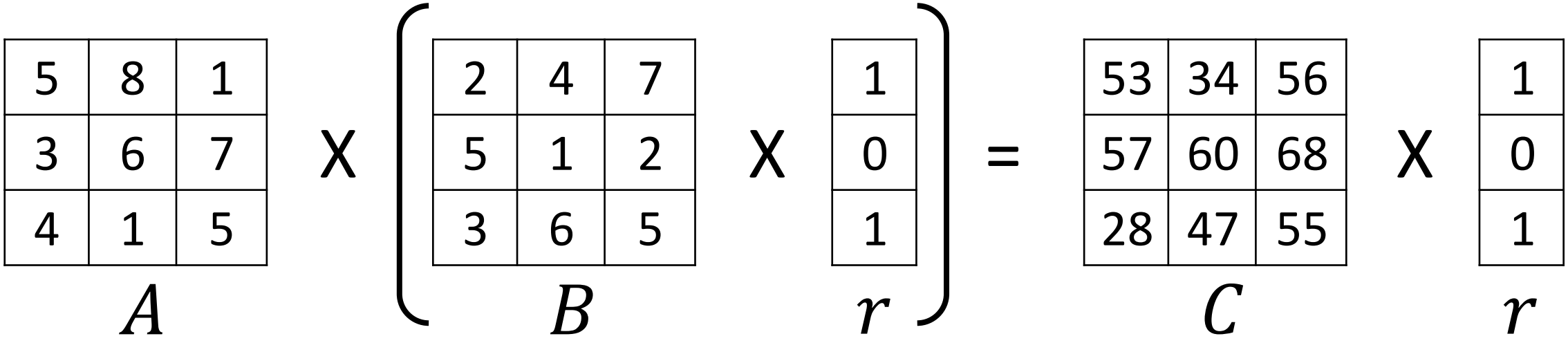
$$A(Br) = Cr$$

$O(n^2)$ $O(n^2)$ $O(n^2)$ } $O(n^2)$

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



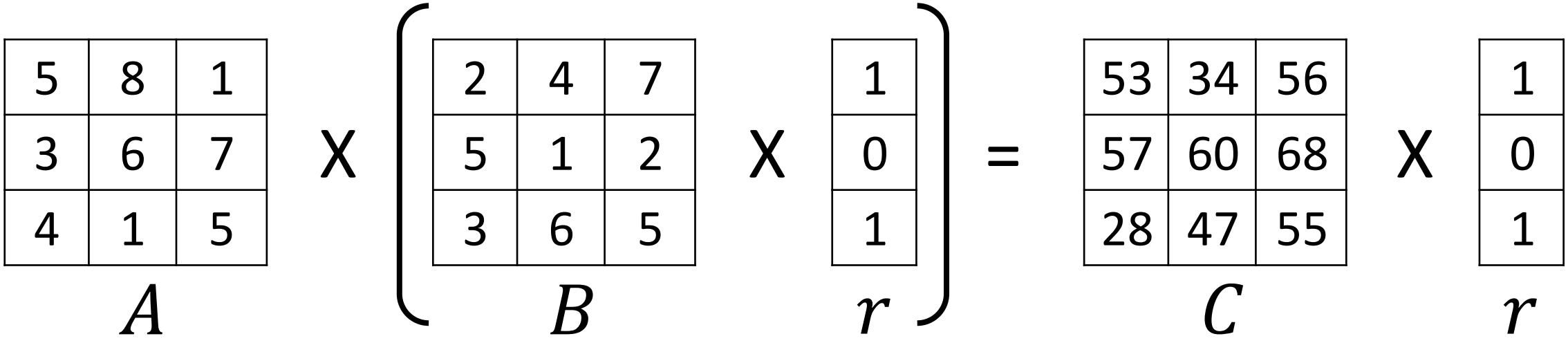
Randomized Algorithm Error Analysis:

- Where is the error?
- What conditions lead to error?
- How likely is the error?
- How do we mitigate the error?

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



Error Types:

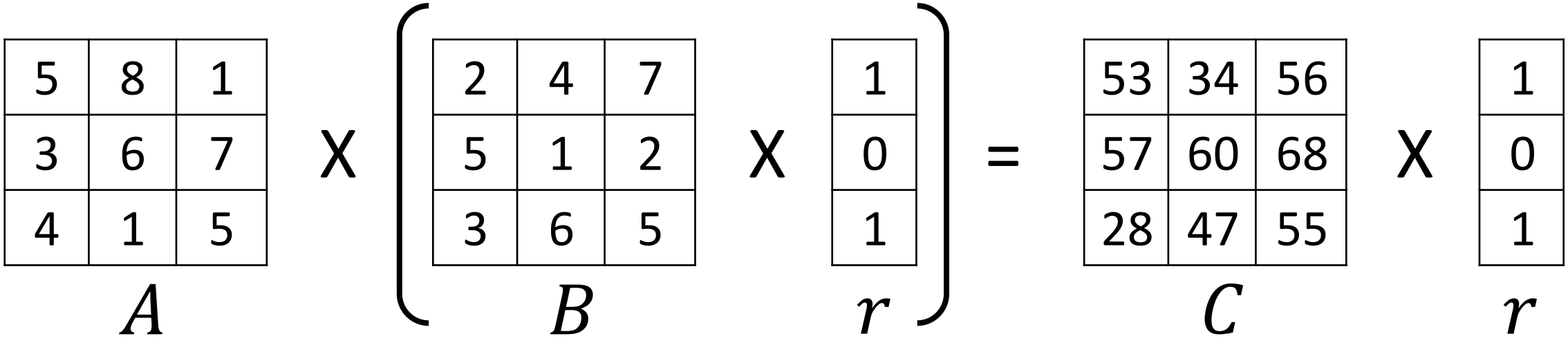
1. False Negative.

2. False Positive.

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



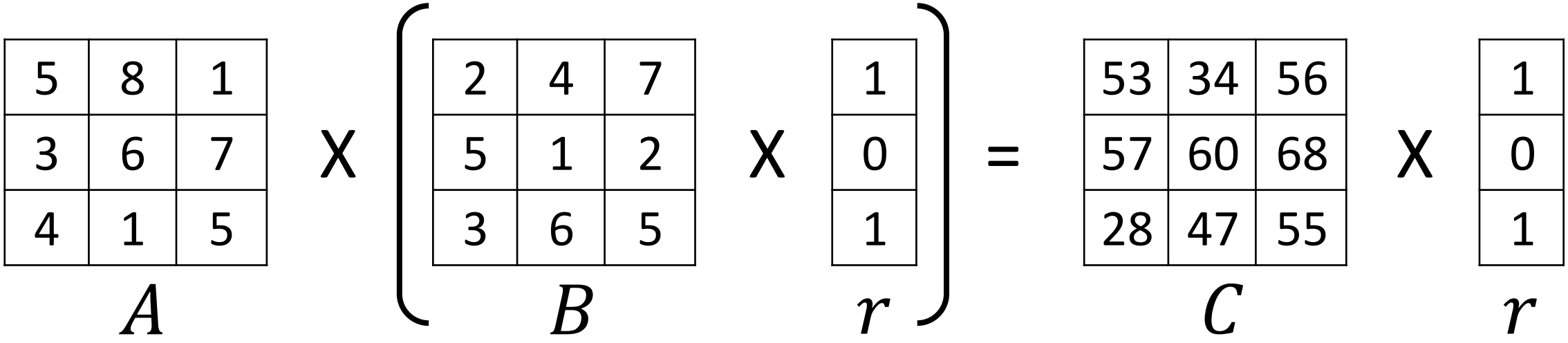
Error Types:

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

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



Error Types:

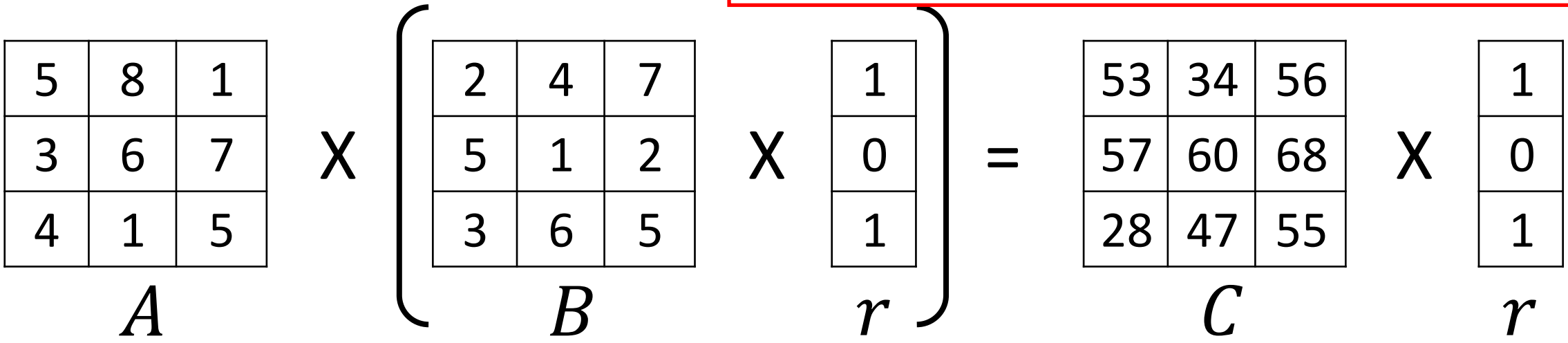
1. False Negative. $AB = C$, but Freivalds' says **false**.
2. False Positive. $AB \neq C$, but Freivalds' says **true**.

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

What is the probability of a false negative?



Error Types:

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

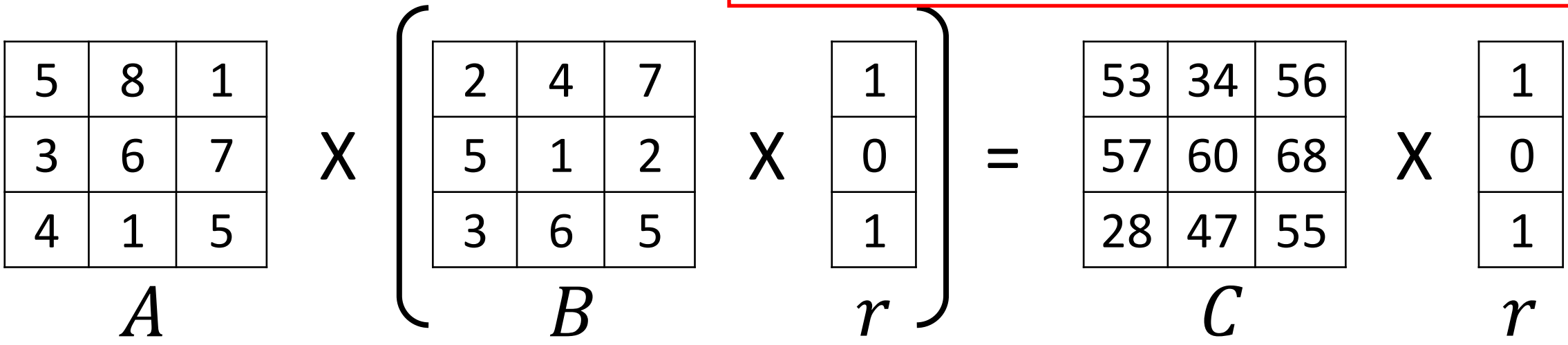
Freivalds' Algorithm (on input A, B, C):

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

What is the probability of a false negative?

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



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

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.

$$\begin{bmatrix} 5 & 8 & 1 \\ 3 & 6 & 7 \\ 4 & 1 & 5 \end{bmatrix} \quad A$$

$$X \left(\begin{bmatrix} 2 & 4 & 7 \\ 5 & 1 & 2 \\ 3 & 6 & 5 \end{bmatrix} \quad B \quad X \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad r \right) =$$

$$\begin{bmatrix} 53 & 34 & 56 \\ 57 & 60 & 68 \\ 28 & 47 & 55 \end{bmatrix} \quad C \quad X \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad r$$

Error Types:

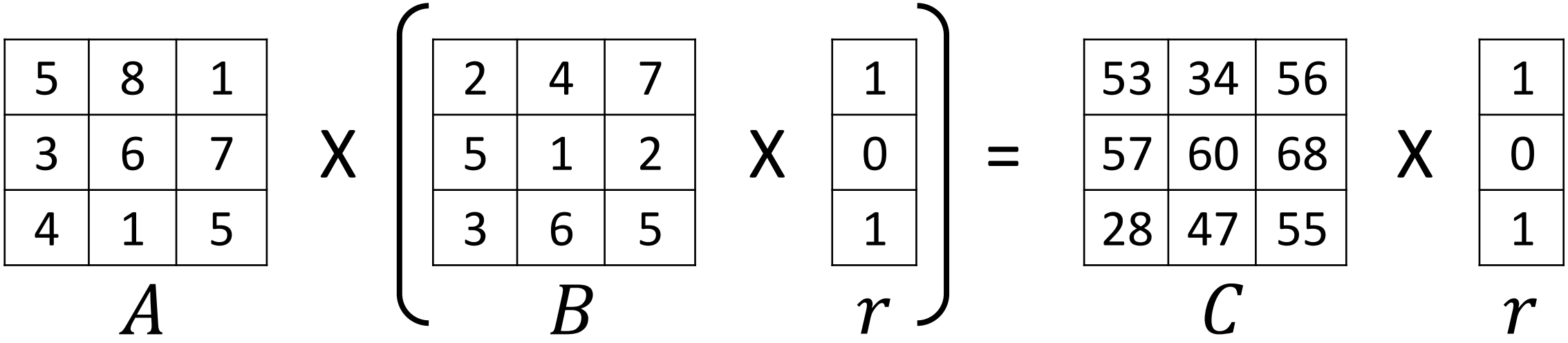
1. ~~False Negative. $AB = C$, but Freivalds' says **false**~~
2. False Positive. $AB \neq C$, but Freivalds' says **true**.

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

Is the probability of a false positive also 0?



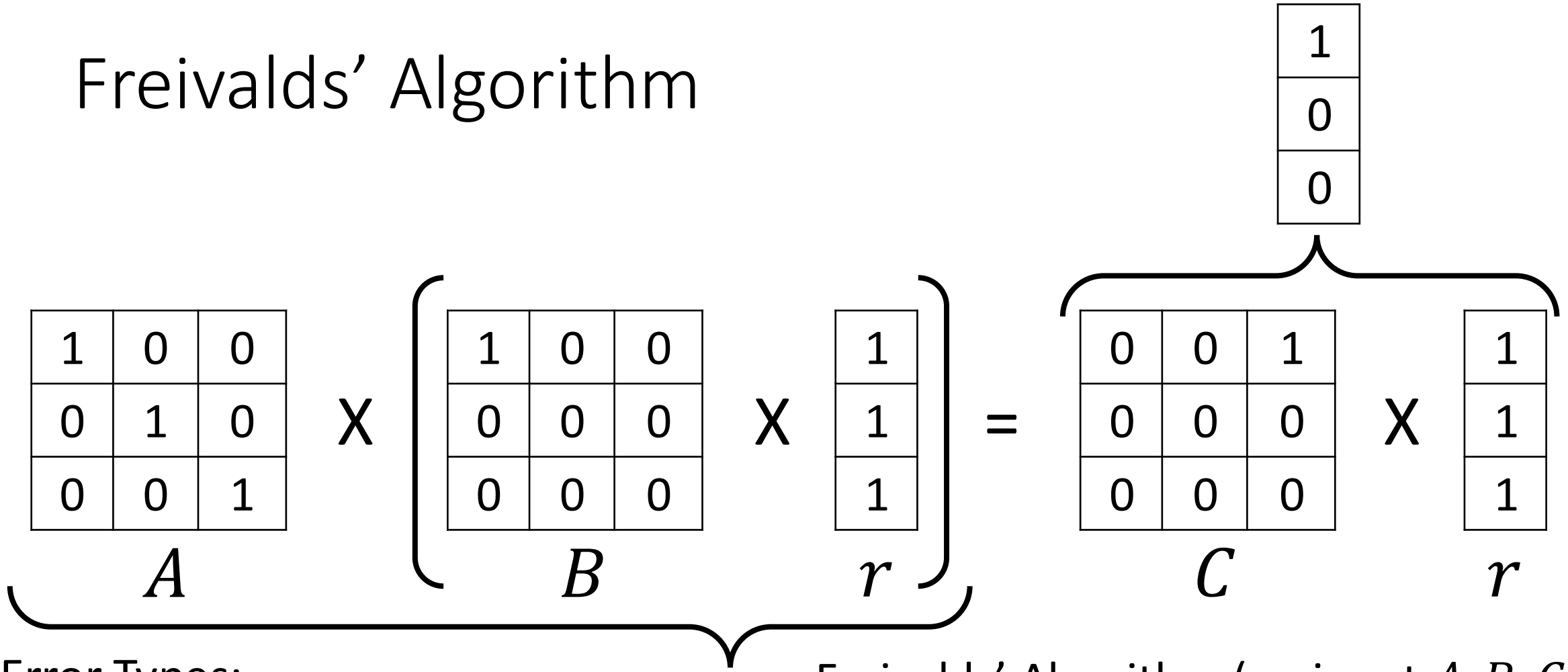
Error Types:

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



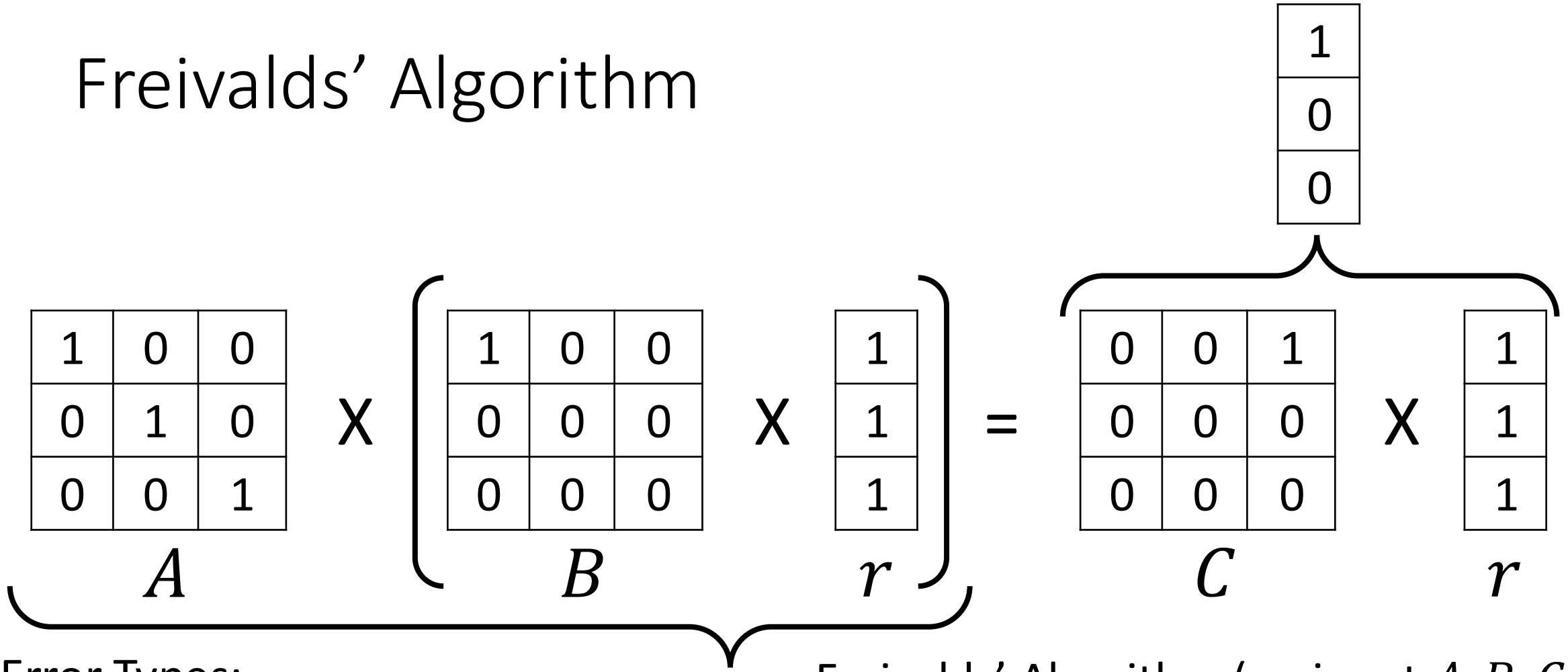
Error Types:

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



Error Types:

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

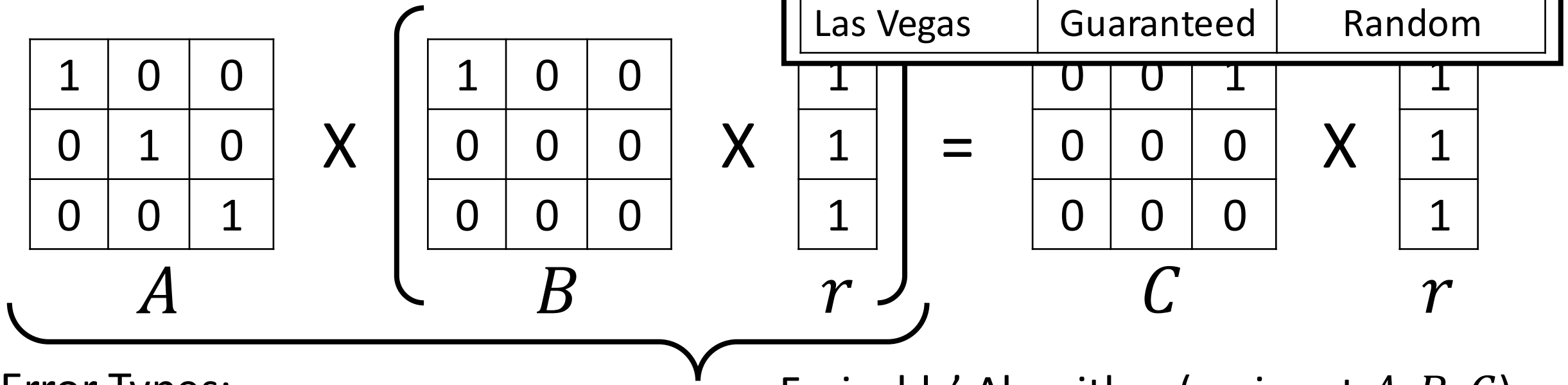
Freivalds' Algorithm (on input A, B, C):

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

Randomness (generally) impacts an algorithm's correctness or running time.

	Correctness	Running Time
Monte Carlo	Random	Bounded
Las Vegas	Guaranteed	Random



Error Types:

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

1
0
0

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' Error Analysis

- Where is the error?
- What conditions lead to the error?
- How likely is the error?
- How do we mitigate the error?

Freivalds' Error Analysis

- Where is the error?

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

- What conditions lead to the error?

- How likely is the error?

- How do we mitigate the error?

Freivalds' Error Analysis

- Where is the error?
  $AB \neq C$, but Freivalds' returns **true**.
- What conditions lead to the error?
  $AB \neq C$, but $ABr = Cr$.
- How likely is the error?

- How do we mitigate the error?

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 $ABr = Cr$.
- How likely is the error?

- How do we mitigate the error?

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?

- How do we mitigate the error?

Freivalds' Error Analysis

Freivalds' fails when:

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

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 $Dr = 0$

Freivalds' Error Analysis

What is the probability that Freivalds' fails?

Freivalds' fails when:

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

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

Conditional Probability:

$\Pr[E|F]$ - Probability of event E occurring given that event F has occurred.

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?

$\Pr[\text{Freivalds' returns } \mathbf{true} | AB \neq C]$ ← Given that the instance is wrong, what is the chance that Freivalds' says it is correct?

Conditional Probability:

$\Pr[E|F]$ - Probability of event E occurring given that event F has occurred.

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?

$\Pr[\text{Freivalds' returns } \mathbf{true} | AB \neq C]$ ⟵ Given that the instance is wrong, what is the chance that Freivalds' says it is correct?

$\Pr[AB \neq C | \text{Freivalds' returns } \mathbf{true}]$ ⟵ Given that Frieval's says the instance is correct, what is the chance it is actually wrong?

Conditional Probability:

$\Pr[E|F]$ - Probability of event E occurring given that event F has occurred.

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?

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

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 $D \neq 0$.

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).

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' Error Analysis

Freivalds' fails when:

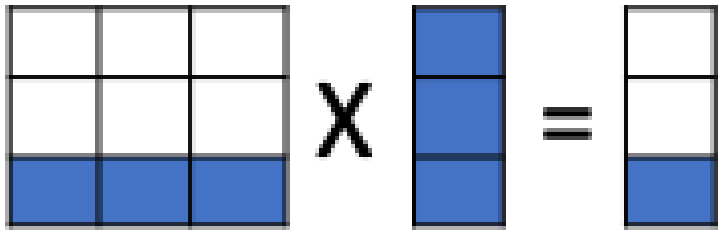
$$AB - C \neq 0 \text{ and } (AB - C)r = 0$$

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 $d \cdot r = 0$.



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,

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

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,

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

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,

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

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,

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

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,

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

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' 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 $d_j \neq 0$.

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:

$AB - C \neq 0$ 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, $\Pr[d \cdot r = 0 | D \neq 0] \leq \frac{1}{2}$