Seminar Algorithms for Big Data

Fast Random Integer Generation in an Interval

Based on a paper of the same title by Daniel Lemire

Lukas Geis
Supervised by Dr. Manuel Penschuck

29th February 2024 · Algorithm Engineering (Prof. Dr. Ulrich Meyer)

What is the problem?

$$0$$

What is the problem?

$$1$$

What is the problem?

$$1$$

$$\uparrow$$

uniform random bit

Motivation

What is the problem?

$$1$$

$$\uparrow$$

$$\text{uniform random bit}$$

$$\uparrow \qquad\qquad \uparrow$$

$$0 \sim 50\% \qquad\qquad 1 \sim 50\%$$

What is the problem?

1 1 0 1 0 0 0 1

What is the problem?

$$1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1$$

$W = 8$ independent uniform bits

What is the problem?

$$1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1$$

$W = 8$ independent uniform bits

Goal:

Generate a uniform integer between 100 and 200

What is the problem?

1 1 0 1 0 0 0 1

interpret as unsigned 8-bit integer

Goal:

Generate a uniform integer between 100 and 200

What is the problem?

$$2^0$$

$$\downarrow$$

$$1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1$$

interpret as unsigned 8-bit integer

Goal:

Generate a uniform integer between 100 and 200

What is the problem?

$$\begin{array}{cccccccc} & & & & & & 2^1 & 2^0 \\ & & & & & & \downarrow & \downarrow \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}$$

interpret as unsigned 8-bit integer

Goal:

Generate a uniform integer between 100 and 200

What is the problem?

$$\begin{array}{cccccccc} & & & & & 2^2 & 2^1 & 2^0 \\ & & & & & \downarrow & \downarrow & \downarrow \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}$$

interpret as unsigned 8-bit integer

Goal:

Generate a uniform integer between 100 and 200

Motivation

What is the problem?

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
1	1	0	1	0	0	0	1

interpret as unsigned 8-bit integer

Goal:

Generate a uniform integer between 100 and 200

What is the problem?

209 in binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
1	1	0	1	0	0	0	1

interpret as unsigned 8-bit integer

Goal:

Generate a uniform integer between 100 and 200

What is the problem?

209 in binary

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
1	1	0	1	0	0	0	1

interpret as uniform 8-bit integer in $[0, 2^8)$

Goal:

Generate a uniform integer between 100 and 200

Table of Contents

1 Preliminaries

Formal Definition

Formal Definition

Input:

Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`

Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`
- upper bound of interval $n \in \mathbb{N}$

Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`
- upper bound of interval $n \in \mathbb{N}$

Output:

- uniform random integer in interval $[0, n)$

Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`
- upper bound of interval $n \in \mathbb{N}$

Output:

- uniform random integer in interval $[0, n)$

Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`
- upper bound of interval $n \in \mathbb{N}$

Output:

- uniform random integer in interval $[0, n)$

Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`
- upper bound of interval $n \in \mathbb{N}$

Output:

- uniform random integer in interval $[0, n)$

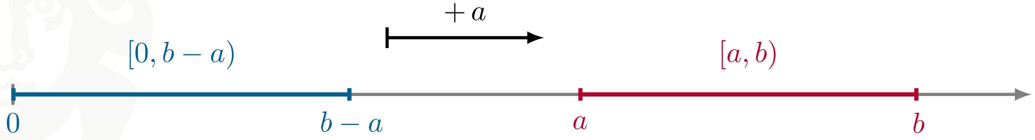
Formal Definition

Input:

- source of uniform random integers in $[0, 2^W)$: `rand()`
- upper bound of interval $n \in \mathbb{N}$

Output:

- uniform random integer in interval $[0, n)$



Operations

Operations

Definition (Common Operations)

Operations

Definition (Common Operations)

- Integer-Division: $x \div y \quad := \left\lfloor {}^{x}\!/_{y} \right\rfloor$

Operations

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Definition (Common Operations)

- Integer-Division: $x \div y \quad := \lfloor x/y \rfloor$
- Remainder-Operation: $x \bmod y := x - (x \div y)y$

Operations

Definition (Common Operations)

- Integer-Division: $x \div y := \lfloor x/y \rfloor$
- Remainder-Operation: $x \bmod y := x - (x \div y)y$
- Bit-RightShift: $x \gg W := x \div 2^W$

Operations

Definition (Common Operations)

- Integer-Division: $x \div y \quad := \lfloor x/y \rfloor$
- Remainder-Operation: $x \bmod y \quad := x - (x \div y)y$
- Bit-RightShift: $x \gg W \quad := x \div 2^W$
- Bit-LeftShift: $x \ll W \quad := x \cdot 2^W$

Operations

Definition (Common Operations)

- Integer-Division: $x \div y := \lfloor x/y \rfloor$
- Remainder-Operation: $x \bmod y := x - (x \div y)y$
- Bit-RightShift: $x \gg W := x \div 2^W$
- Bit-LeftShift: $x \ll W := x \cdot 2^W$
- Bitwise-And: $x \ \& \ y$

Operations

Definition (Common Operations)

- Integer-Division: $x \div y \quad := \lfloor x/y \rfloor$
- Remainder-Operation: $x \bmod y := x - (x \div y)y$
- Bit-RightShift: $x \gg W \quad := x \div 2^W$
- Bit-LeftShift: $x \ll W \quad := x \cdot 2^W$
- Bitwise-And: $x \ \& \ y \quad \to x \bmod 2^W := x \ \& \ (2^W - 1)$

Operations

Definition (Common Operations)

- Integer-Division: $x \div y \quad := \lfloor x/y \rfloor$
- Remainder-Operation: $x \bmod y := x - (x \div y)y$
- Bit-RightShift: $x \gg W \quad := x \div 2^W$
- Bit-LeftShift: $x \ll W \quad := x \cdot 2^W$
- Bitwise-And: $x \ \& \ y \quad \to x \bmod 2^W := x \ \& \ (2^W - 1)$

Definition (Power Remainder)

For $W, n \in \mathbb{N}$, we write $\mathcal{R}$ for $2^W \bmod n$.

The Naive Approach

The Naive Approach

$$\texttt{rand()} \bmod n$$

The Naive Approach

$$\texttt{rand()} \bmod n$$

Does this work?

The Naive Approach

$$\texttt{rand()} \bmod n$$

Does this work?

- Yes, the generated number is in $[0, n)$.

The Naive Approach

$$\texttt{rand()} \bmod n$$

Does this work?

- Yes, the generated number is in $[0, n)$.

Is this efficient?

The Naive Approach

$$\texttt{rand()} \bmod n$$

Does this work?

- Yes, the generated number is in $[0, n)$.

Is this efficient?

- No, we require one expensive integer division operation.

The Naive Approach

$$\texttt{rand()} \bmod n$$

Does this work?

- Yes, the generated number is in $[0, n)$.

Is this efficient?

- No, we require one expensive integer division operation.

Is the generated number uniform in $[0, n)$?

The Naive Approach - Bias

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}, \overbrace{0, 1, \ldots, n-1}^{n \text{ values}}, \ldots, \overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{(2^W \div n) \cdot n \text{ values}}, \underbrace{0, 1, \ldots, \mathcal{R}-1}_{\mathcal{R} \text{ values}}}^{2^W \text{ values}}$$

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

$$\overbrace{\underbrace{\overbrace{0,1,\ldots,n-1}^{n\text{ values}},\overbrace{0,1,\ldots,n-1}^{n\text{ values}},\ldots,\overbrace{0,1,\ldots,n-1}^{n\text{ values}}}_{(2^W \div n)\cdot n\text{ values}},\underbrace{0,1,\ldots,\mathcal{R}-1}_{\mathcal{R}\text{ values}}}^{2^W\text{ values}}$$

We have a leftover interval that introduces bias.

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}, \overbrace{0, 1, \ldots, n-1}^{n \text{ values}}, \ldots, \overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{(2^W \div n) \cdot n \text{ values}}, \underbrace{0, 1, \ldots, \mathcal{R}-1}_{\mathcal{R} \text{ values}}}^{2^W \text{ values}}$$

We have a leftover interval that introduces bias.

Deterministic Mappings

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

$$\overbrace{\underbrace{\overbrace{0,1,\dots,n-1}^{n \text{ values}},\overbrace{0,1,\dots,n-1}^{n \text{ values}},\dots,\overbrace{0,1,\dots,n-1}^{n \text{ values}}}_{(2^W \div n)\cdot n \text{ values}},\underbrace{0,1,\dots,\mathcal{R}-1}_{\mathcal{R} \text{ values}}}^{2^W \text{ values}}$$

We have a leftover interval that introduces bias.

Deterministic Mappings

Every deterministic mapping $f\colon [0, 2^W) \to [0, n)$

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

$$\overbrace{\underbrace{\overbrace{0,1,\ldots,n-1}^{n \text{ values}},\overbrace{0,1,\ldots,n-1}^{n \text{ values}},\ldots,\overbrace{0,1,\ldots,n-1}^{n \text{ values}}}_{(2^W \div n)\cdot n \text{ values}},\underbrace{0,1,\ldots,\mathcal{R}-1}_{\mathcal{R} \text{ values}}}^{2^W \text{ values}}$$

We have a leftover interval that introduces bias.

Deterministic Mappings

Every deterministic mapping $f\colon [0, 2^W) \to [0, n)$ does not generate uniform random integers in one step

The Naive Approach - Bias

In general, applying $x \bmod n$ to $[0, 2^W)$ yields

$$\overbrace{\underbrace{\overbrace{0,1,\ldots,n-1}^{n \text{ values}},\overbrace{0,1,\ldots,n-1}^{n \text{ values}},\ldots,\overbrace{0,1,\ldots,n-1}^{n \text{ values}}}_{(2^W \div n)\cdot n \text{ values}},\underbrace{0,1,\ldots,\mathcal{R}-1}_{\mathcal{R} \text{ values}}}^{2^W \text{ values}}$$

We have a leftover interval that introduces bias.

Deterministic Mappings

Every deterministic mapping $f\colon [0, 2^W) \to [0, n)$ does not generate uniform random integers in one step whenever n does not divide 2^W.

Unbiased Algorithms

The OpenBSD Algorithm

The OpenBSD Algorithm

- Shift the rejection interval to the left:

The OpenBSD Algorithm

- Shift the rejection interval to the left:

$$\overbrace{\underbrace{0, 1, \ldots, \mathcal{R}-1}_{\mathcal{R}\text{ values}}, \underbrace{\overbrace{\mathcal{R}, \ldots, n-1, 0, \ldots, \mathcal{R}-1}^{n\text{ values}}, \ldots, \overbrace{\mathcal{R}, \ldots, n-1, 0, \ldots, \mathcal{R}-1}^{n\text{ values}}}_{(2^W \div n)\cdot n\text{ values}}}^{2^W\text{ values}}$$

The OpenBSD Algorithm

- Shift the rejection interval to the left:

$$\overbrace{\underbrace{0,1,\ldots,\mathcal{R}-1}_{\mathcal{R}\text{ values}},\underbrace{\overbrace{\mathcal{R},\ldots,n-1,0,\ldots,\mathcal{R}-1}^{n\text{ values}},\ldots,\overbrace{\mathcal{R},\ldots,n-1,0,\ldots,\mathcal{R}-1}^{n\text{ values}}}_{(2^W\div n)\cdot n\text{ values}}}^{2^W\text{ values}}$$

- Algorithm:

The OpenBSD Algorithm

- Shift the rejection interval to the left:

$$\overbrace{\underbrace{0, 1, \ldots, \mathcal{R}-1}_{\mathcal{R}\text{ values}}, \underbrace{\overbrace{\mathcal{R}, \ldots, n-1, 0, \ldots, \mathcal{R}-1}^{n\text{ values}}, \ldots, \overbrace{\mathcal{R}, \ldots, n-1, 0, \ldots, \mathcal{R}-1}^{n\text{ values}}}_{(2^W \div n)\cdot n\text{ values}}}^{2^W\text{ values}}$$

- Algorithm:
  - Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$

The OpenBSD Algorithm

- Shift the rejection interval to the left:

$$\overbrace{\underbrace{0,1,\ldots,\mathcal{R}-1}_{\mathcal{R}\text{ values}},\underbrace{\overbrace{\mathcal{R},\ldots,n-1,0,\ldots,\mathcal{R}-1}^{n\text{ values}},\ldots,\overbrace{\mathcal{R},\ldots,n-1,0,\ldots,\mathcal{R}-1}^{n\text{ values}}}_{(2^W\div n)\cdot n\text{ values}}}^{2^W\text{ values}}$$

- Algorithm:
  - Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$
  - Return $x \bmod n$

The OpenBSD Algorithm - Efficiency

Algorithm:

- Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$
- Return $x \bmod n$

The OpenBSD Algorithm - Efficiency

Algorithm:

- Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$
- Return $x \bmod n$

Efficiency

The OpenBSD Algorithm - Efficiency

Algorithm:

- Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$
- Return $x \bmod n$

Efficiency

We require 2 integer division operations:

The OpenBSD Algorithm - Efficiency

Algorithm:

- Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$
- Return $x \bmod n$

Efficiency

We require 2 integer division operations:

- one for computing $\mathcal{R}$

The OpenBSD Algorithm - Efficiency

Algorithm:

- Generate a uniform random number $x \in [0, 2^W)$ until $x \geq \mathcal{R}$
- Return $x \bmod n$

Efficiency

We require 2 integer division operations:

- one for computing $\mathcal{R}$
- and one for computing $x \bmod n$.

The Java Algorithm

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{0, 1, \ldots, n-1}_{n \text{ values}}, \underbrace{0, 1, \ldots, n-1}_{n \text{ values}}, \ldots, \underbrace{0, 1, \ldots, n-1}_{n \text{ values}}}^{(2^W \div n) \cdot n \text{ values}}, \underbrace{0, 1, \ldots, \mathcal{R}-1}_{\mathcal{R} \text{ values}}$$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } 0}, \overbrace{0, 1, \ldots, n-1}^{n \text{ values}}, \ldots, \overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}^{(2^W \div n) \cdot n \text{ values}}, \overbrace{0, 1, \ldots, \mathcal{R}-1}^{\mathcal{R} \text{ values}}$$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0, 1, \dots, n-1}^{n \text{ values}}}_{\text{mapped to } 0}, \underbrace{\overbrace{0, 1, \dots, n-1}^{n \text{ values}}}_{\text{mapped to } n}, \dots, \overbrace{0, 1, \dots, n-1}^{n \text{ values}}}^{(2^W \div n) \cdot n \text{ values}}, \overbrace{0, 1, \dots, \mathcal{R}-1}^{\mathcal{R} \text{ values}}$$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0,1,\dots,n-1}^{n\text{ values}}}_{\text{mapped to }0},\underbrace{\overbrace{0,1,\dots,n-1}^{n\text{ values}}}_{\text{mapped to }n},\dots,\underbrace{\overbrace{0,1,\dots,n-1}^{n\text{ values}}}_{\substack{\text{mapped to}\\ 2^W-n-\mathcal{R}}}}^{(2^W \div n)\cdot n\text{ values}},\overbrace{0,1,\dots,\mathcal{R}-1}^{\mathcal{R}\text{ values}}$$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } 0}, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } n}, \ldots, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\substack{\text{mapped to} \\ 2^W - n - \mathcal{R}}}}^{(2^W \div n) \cdot n \text{ values}}, \underbrace{\overbrace{0, 1, \ldots, \mathcal{R}-1}^{\mathcal{R} \text{ values}}}_{\substack{\text{mapped to} \\ 2^W - \mathcal{R}}}$$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } 0}, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } n}, \ldots, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\substack{\text{mapped to}\\ 2^W - n - \mathcal{R}}}}^{(2^W \div n) \cdot n \text{ values}}, \underbrace{\overbrace{0, 1, \ldots, \mathcal{R}-1}^{\mathcal{R} \text{ values}}}_{\substack{\text{mapped to}\\ 2^W - \mathcal{R}}}$$

- Map every number to the next-smallest multiple of n

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0,1,\dots,n-1}^{n\text{ values}}}_{\text{mapped to }0},\underbrace{\overbrace{0,1,\dots,n-1}^{n\text{ values}}}_{\text{mapped to }n},\dots,\underbrace{\overbrace{0,1,\dots,n-1}^{n\text{ values}}}_{\substack{\text{mapped to}\\ 2^W-n-\mathcal{R}}}}^{(2^W \div n)\cdot n\text{ values}},\underbrace{\overbrace{0,1,\dots,\mathcal{R}-1}^{\mathcal{R}\text{ values}}}_{\substack{\text{mapped to}\\ 2^W-\mathcal{R}}}$$

- Map every number to the next-smallest multiple of n
- Only numbers in leftover interval mapped to $2^W - \mathcal{R} > 2^W - n$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } 0}, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } n}, \ldots, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } 2^W - n - \mathcal{R}}}^{(2^W \div n) \cdot n \text{ values}}, \underbrace{\overbrace{0, 1, \ldots, \mathcal{R}-1}^{\mathcal{R} \text{ values}}}_{\text{mapped to } 2^W - \mathcal{R}}$$

- Map every number to the next-smallest multiple of n
- Only numbers in leftover interval mapped to $2^W - \mathcal{R} > 2^W - n$
- Algorithm:

The Java Algorithm

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0,1,\ldots,n-1}^{n\text{ values}}}_{\text{mapped to }0},\underbrace{\overbrace{0,1,\ldots,n-1}^{n\text{ values}}}_{\text{mapped to }n},\ldots,\underbrace{\overbrace{0,1,\ldots,n-1}^{n\text{ values}}}_{\substack{\text{mapped to}\\ 2^W-n-\mathcal{R}}}}^{(2^W \div n)\cdot n\text{ values}},\underbrace{\overbrace{0,1,\ldots,\mathcal{R}-1}^{\mathcal{R}\text{ values}}}_{\substack{\text{mapped to}\\ 2^W-\mathcal{R}}}$$

- Map every number to the next-smallest multiple of n
- Only numbers in leftover interval mapped to $2^W - \mathcal{R} > 2^W - n$
- Algorithm:
  (1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

The Java Algorithm

- Consider $x - (x \bmod n)$ for $x \in [0, 2^W)$:

$$\overbrace{\underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } 0}, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\text{mapped to } n}, \ldots, \underbrace{\overbrace{0, 1, \ldots, n-1}^{n \text{ values}}}_{\substack{\text{mapped to} \\ 2^W - n - \mathcal{R}}}}^{(2^W \div n) \cdot n \text{ values}}, \underbrace{\overbrace{0, 1, \ldots, \mathcal{R}-1}^{\mathcal{R} \text{ values}}}_{\substack{\text{mapped to} \\ 2^W - \mathcal{R}}}$$

- Map every number to the next-smallest multiple of n
- Only numbers in leftover interval mapped to $2^W - \mathcal{R} > 2^W - n$
- Algorithm:
  (1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$
  (2) Return r if $x - r \le 2^W - n$ else goto **(1)**

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \leq 2^W - n$ else goto **(1)**

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \leq 2^W - n$ else goto **(1)**

Efficiency

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \leq 2^W - n$ else goto **(1)**

Efficiency

- At least one integer division operation

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \leq 2^W - n$ else goto **(1)**

Efficiency

- At least one integer division operation
- Number of integer divisions operations equal to number of rounds

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \le 2^W - n$ else goto **(1)**

Efficiency

- At least one integer division operation
- Number of integer divisions operations equal to number of rounds
- Return number in round if $x < 2^W - \mathcal{R}$

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \leq 2^W - n$ else goto **(1)**

Efficiency

- At least one integer division operation
- Number of integer divisions operations equal to number of rounds
- Return number in round if $x < 2^W - \mathcal{R}$
- Happens with probability $\frac{2^W - \mathcal{R}}{2^W} > \frac{1}{2}$

The Java Algorithm - Efficiency

Algorithm:

(1) Draw $x \in [0, 2^W)$ and compute $r = x \bmod n$

(2) Return r if $x - r \leq 2^W - n$ else goto **(1)**

Efficiency

- At least one integer division operation
- Number of integer divisions operations equal to number of rounds
- Return number in round if $x < 2^W - \mathcal{R}$
- Happens with probability $\frac{2^W - \mathcal{R}}{2^W} > \frac{1}{2}$
- Expected number of integer division operations is $\frac{2^W}{2^W - \mathcal{R}} < 2$

Lemire's Algorithm

Multiply-And-Shift

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$(\texttt{rand()} \cdot n) \gg W$$

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$(\texttt{rand()} \cdot n) \div 2^W$$

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$(\underbrace{\texttt{rand()}}_{\in[0,2^W)} \cdot n) \div 2^W$$

Multiply-And-Shift

- Map $\texttt{rand()}$ to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n)}_{\in[0, n \cdot 2^W)} \div 2^W$$

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n)}_{\in[0, n\cdot 2^W)} \div 2^W$$

- $n < 2^W \implies n \cdot 2^W < 2^W \cdot 2^W = 2^{2W}$

Multiply-And-Shift

- Map $\texttt{rand()}$ to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n)}_{\in[0, n \cdot 2^W)} \div 2^W$$

- $n < 2^W \implies n \cdot 2^W < 2^W \cdot 2^W = 2^{2W}$
- $2W$ bits enough to represent $\texttt{rand()} \cdot n$

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n) \div 2^W}_{\in[0,n)}$$

- $n < 2^W \implies n \cdot 2^W < 2^W \cdot 2^W = 2^{2W}$
- $2W$ bits enough to represent $\texttt{rand()} \cdot n$

Multiply-And-Shift

- Map $\texttt{rand()}$ to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n) \div 2^W}_{\in[0,n)}$$

- $n < 2^W \implies n \cdot 2^W < 2^W \cdot 2^W = 2^{2W}$
- $2W$ bits enough to represent $\texttt{rand()} \cdot n$

Is this uniform?

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n) \div 2^W}_{\in[0,n)}$$

- $n < 2^W \implies n \cdot 2^W < 2^W \cdot 2^W = 2^{2W}$
- $2W$ bits enough to represent $\texttt{rand()} \cdot n$

Is this uniform?

- Mapping is deterministic!

Multiply-And-Shift

- Map `rand()` to $[0, n)$ divisionless with $(\texttt{rand()} \cdot n) \gg W$:

$$\underbrace{(\texttt{rand()} \cdot n) \div 2^W}_{\in [0,n)}$$

- $n < 2^W \implies n \cdot 2^W < 2^W \cdot 2^W = 2^{2W}$
- $2W$ bits enough to represent $\texttt{rand()} \cdot n$

Is this uniform?

- Mapping is deterministic!
- Mapping can not be uniform for all n!

The Algorithm - Intervals

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

$$\overbrace{\underbrace{0, \ldots, 2^W - 1}_{\substack{0^{\text{th}} \text{ interval} \\ \text{mapped to } 0 \text{ by } \gg W}}, \ldots, \underbrace{i \cdot 2^W, \ldots, (i+1) \cdot 2^W - 1}_{\substack{i^{\text{th}} \text{ interval} \\ \text{mapped to } i \text{ by } \gg W}}, \ldots, \underbrace{(n-1) \cdot 2^W, \ldots, n \cdot 2^W - 1}_{\substack{(n-1)^{\text{th}} \text{ interval} \\ \text{mapped to } n-1 \text{ by } \gg W}},}^{n \cdot 2^W \text{ values}}$$

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

$$\overbrace{\underbrace{0, \ldots, 2^W - 1}_{\substack{0^{\text{th}} \text{ interval} \\ \text{mapped to } 0 \text{ by } \gg W}}, \ldots, \underbrace{i \cdot 2^W, \ldots, (i+1) \cdot 2^W - 1}_{\substack{i^{\text{th}} \text{ interval} \\ \text{mapped to } i \text{ by } \gg W}}, \ldots, \underbrace{(n-1) \cdot 2^W, \ldots, n \cdot 2^W - 1}_{\substack{(n-1)^{\text{th}} \text{ interval} \\ \text{mapped to } n-1 \text{ by } \gg W}},}^{n \cdot 2^W \text{ values}}$$

- Define the restricted i^{th} interval as $[i \cdot 2^W + \mathcal{R}, (i+1) \cdot 2^W)$

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

$$\overbrace{\underbrace{0, \ldots, 2^W - 1}_{\substack{0^{\text{th}} \text{ interval} \\ \text{mapped to } 0 \text{ by } \gg W}}, \ldots, \underbrace{i \cdot 2^W, \ldots, (i+1) \cdot 2^W - 1}_{\substack{i^{\text{th}} \text{ interval} \\ \text{mapped to } i \text{ by } \gg W}}, \ldots, \underbrace{(n-1) \cdot 2^W, \ldots, n \cdot 2^W - 1}_{\substack{(n-1)^{\text{th}} \text{ interval} \\ \text{mapped to } n-1 \text{ by } \gg W}},}^{n \cdot 2^W \text{ values}}$$

- Define the restricted i^{th} interval as $[i \cdot 2^W + \mathcal{R}, (i+1) \cdot 2^W)$
- This interval has size

$$(i+1) \cdot 2^W - (i \cdot 2^W + \mathcal{R}) = 2^W - \mathcal{R}$$

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

$$\overbrace{\underbrace{0, \ldots, 2^W - 1}_{\substack{0^{\text{th}} \text{ interval} \\ \text{mapped to } 0 \text{ by } \gg W}}, \ldots, \underbrace{i \cdot 2^W, \ldots, (i+1) \cdot 2^W - 1}_{\substack{i^{\text{th}} \text{ interval} \\ \text{mapped to } i \text{ by } \gg W}}, \ldots, \underbrace{(n-1) \cdot 2^W, \ldots, n \cdot 2^W - 1}_{\substack{(n-1)^{\text{th}} \text{ interval} \\ \text{mapped to } n-1 \text{ by } \gg W}},}^{n \cdot 2^W \text{ values}}$$

- Define the restricted i^{th} interval as $[i \cdot 2^W + \mathcal{R}, (i+1) \cdot 2^W)$
- This interval has size

$$(i+1) \cdot 2^W - (i \cdot 2^W + \mathcal{R}) = 2^W - \mathcal{R}$$

which is divisible by n

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

$$\overbrace{\underbrace{0, \ldots, 2^W - 1}_{\substack{0^{\text{th}} \text{ interval} \\ \text{mapped to } 0 \text{ by } \gg W}}, \ldots, \underbrace{i \cdot 2^W, \ldots, (i+1) \cdot 2^W - 1}_{\substack{i^{\text{th}} \text{ interval} \\ \text{mapped to } i \text{ by } \gg W}}, \ldots, \underbrace{(n-1) \cdot 2^W, \ldots, n \cdot 2^W - 1}_{\substack{(n-1)^{\text{th}} \text{ interval} \\ \text{mapped to } n-1 \text{ by } \gg W}},}^{n \cdot 2^W \text{ values}}$$

- Define the restricted i^{th} interval as $[i \cdot 2^W + \mathcal{R}, (i+1) \cdot 2^W)$
- This interval has size

$$(i+1) \cdot 2^W - \left(i \cdot 2^W + \mathcal{R}\right) = 2^W - \mathcal{R}$$

  which is divisible by n
- Every restricted i^{th} interval has $\frac{2^W - \mathcal{R}}{n} = \lfloor \frac{2^W}{n} \rfloor$ multiples of n

The Algorithm - Intervals

- Split $[0, n \cdot 2^W)$ into intervals $[i \cdot 2^W, (i+1) \cdot 2^W)$ for $i < n$

$$\overbrace{\underbrace{0, \dots, 2^W - 1}_{\substack{0^{\text{th}} \text{ interval} \\ \text{mapped to } 0 \text{ by } \gg W}}, \dots, \underbrace{i \cdot 2^W, \dots, (i+1) \cdot 2^W - 1}_{\substack{i^{\text{th}} \text{ interval} \\ \text{mapped to } i \text{ by } \gg W}}, \dots, \underbrace{(n-1) \cdot 2^W, \dots, n \cdot 2^W - 1}_{\substack{(n-1)^{\text{th}} \text{ interval} \\ \text{mapped to } n-1 \text{ by } \gg W}},}^{n \cdot 2^W \text{ values}}$$

- Define the restricted i^{th} interval as $[i \cdot 2^W + \mathcal{R}, (i+1) \cdot 2^W)$
- This interval has size

$$(i+1) \cdot 2^W - \left(i \cdot 2^W + \mathcal{R}\right) = 2^W - \mathcal{R}$$

  which is divisible by n
- Every restricted i^{th} interval has $\frac{2^W - \mathcal{R}}{n} = \lfloor \frac{2^W}{n} \rfloor$ multiples of n
- We can make Multiply-And-Shift uniform by only accepting multiples of n in restricted intervals

The Algorithm - Rejection

The Algorithm - Rejection

When do we reject $x := \texttt{rand()} \cdot n$?

The Algorithm - Rejection

When do we reject $x := \texttt{rand()} \cdot n$?

- $x \in [i \cdot 2^W, i \cdot 2^W + \mathcal{R})$ for some $i < n$

The Algorithm - Rejection

When do we reject $x := \texttt{rand()} \cdot n$?

- $x \in [i \cdot 2^W, i \cdot 2^W + \mathcal{R})$ for some $i < n$
- Applying $x \bmod 2^W$ to any i^{th} interval yields

The Algorithm - Rejection

When do we reject $x := \texttt{rand()} \cdot n$?

- $x \in [i \cdot 2^W, i \cdot 2^W + \mathcal{R})$ for some $i < n$
- Applying $x \bmod 2^W$ to any i^{th} interval yields

$$\overbrace{\underbrace{0, 1, \dots, \mathcal{R} - 1}_{\text{rejected part}}, \underbrace{\mathcal{R}, \dots, n, \dots, 2^W - 1}_{\text{restricted } i^{\text{th}} \text{ interval}}}^{2^W \text{ values}}$$

The Algorithm - Rejection

When do we reject $x := \texttt{rand}() \cdot n$?

- $x \in [i \cdot 2^W, i \cdot 2^W + \mathcal{R})$ for some $i < n$
- Applying $x \bmod 2^W$ to any i^{th} interval yields

$$\overbrace{\underbrace{0, 1, \ldots, \mathcal{R} - 1}_{\text{rejected part}}, \underbrace{\mathcal{R}, \ldots, n, \ldots, 2^W - 1}_{\text{restricted } i^{\text{th}} \text{ interval}}}^{2^W \text{ values}}$$

- We reject x if $x \bmod 2^W < \mathcal{R}$

The Algorithm - Sketch

The Algorithm - Sketch

$\mathcal{R} \leftarrow 2^W \bmod n$ `/* Compute rejection threshold */`

The Algorithm - Sketch

```
R ← 2^W mod n                    /* Compute rejection threshold */
while true do
```

$\mathcal{R} \leftarrow 2^{W} \bmod n$ /* Compute rejection threshold */

while *true* **do**

The Algorithm - Sketch

```
R ← 2^W mod n                    /* Compute rejection threshold */
while true do
    x ← rand()
```

The Algorithm - Sketch

```
R ← 2^W mod n                    /* Compute rejection threshold */
while true do
    x ← rand()
    m ← x · n                    /* Use 2W bits for representation */
```

The Algorithm - Sketch

```
R ← 2^W mod n                      /* Compute rejection threshold */
while true do
    x ← rand()
    m ← x · n                      /* Use 2W bits for representation */
    l ← m & (2^W − 1)              /* m mod 2^W */
```

The Algorithm - Sketch

$\mathcal{R} \leftarrow 2^W \bmod n$ /* Compute rejection threshold */
while *true* **do**
  $x \leftarrow$ `rand()`
  $m \leftarrow x \cdot n$ /* Use $2W$ bits for representation */
  $l \leftarrow m \ \& \ (2^W - 1)$ /* $m \bmod 2^W$ */
  if $l \geq \mathcal{R}$ **then** /* Apply rejection rule */

The Algorithm - Sketch

$\mathcal{R} \leftarrow 2^W \bmod n$ /* Compute rejection threshold */

while *true* **do**

  $x \leftarrow \texttt{rand()}$

  $m \leftarrow x \cdot n$ /* Use $2W$ bits for representation */

  $l \leftarrow m \ \& \ (2^W - 1)$ /* $m \bmod 2^W$ */

  if $l \geq \mathcal{R}$ **then** /* Apply rejection rule */

    return $m \gg W$

The Algorithm - Avoiding Division

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$
- If not, we compute $\mathcal{R}$ and proceed as before

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$
- If not, we compute $\mathcal{R}$ and proceed as before

With what probability do we need to compute $\mathcal{R}$:

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$
- If not, we compute $\mathcal{R}$ and proceed as before

With what probability do we need to compute $\mathcal{R}$:

- We assume x to be uniform in $[0, 2^W)$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$
- If not, we compute $\mathcal{R}$ and proceed as before

With what probability do we need to compute $\mathcal{R}$:

- We assume x to be uniform in $[0, 2^W)$ $\longrightarrow$ l is also uniform in $[0, 2^W)$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$
- If not, we compute $\mathcal{R}$ and proceed as before

With what probability do we need to compute $\mathcal{R}$:

- We assume x to be uniform in $[0, 2^W)$ $\longrightarrow$ l is also uniform in $[0, 2^W)$
- We compute $\mathcal{R}$ if $l < n$

The Algorithm - Avoiding Division

Consider the first iteration of the loop:

- We reject x if $l < \mathcal{R}$ $\longrightarrow$ we need to compute $\mathcal{R}$ beforehand
- But we know $\mathcal{R} < n$ $\longrightarrow$ if $l \geq n$ we do not need to know $\mathcal{R}$

We can alter the first iteration of the loop:

- We do not compute $\mathcal{R}$ beforehand
- If $l \geq n$, we accept x without computing $\mathcal{R}$
- If not, we compute $\mathcal{R}$ and proceed as before

With what probability do we need to compute $\mathcal{R}$:

- We assume x to be uniform in $[0, 2^W)$ $\longrightarrow$ l is also uniform in $[0, 2^W)$
- We compute $\mathcal{R}$ if $l < n$ $\longrightarrow$ happens with probability $\frac{n}{2^W}$

The Algorithm - Pseudocode

The Algorithm - Pseudocode

$x \leftarrow$ `rand()`

The Algorithm - Pseudocode

```
x ← rand()
m ← x · n                         /* Use 2W bits for representation */
```

The Algorithm - Pseudocode

$x \leftarrow$ `rand()`

$m \leftarrow x \cdot n$ /* Use $2W$ bits for representation */

$l \leftarrow m \ \& \ (2^W - 1)$ /* $m \bmod 2^W$ */

The Algorithm - Pseudocode

```
x ← rand()
m ← x · n                     /* Use 2W bits for representation */
l ← m & (2^W − 1)             /* m mod 2^W */
if l < n then                 /* Possibly skip division */
```

The Algorithm - Pseudocode

$x \leftarrow$ `rand()`

$m \leftarrow x \cdot n$ /* Use $2W$ bits for representation */

$l \leftarrow m \;\&\; (2^W - 1)$ /* $m \bmod 2^W$ */

if $l < n$ **then** /* Possibly skip division */

return $m \gg W$

The Algorithm - Pseudocode

$x \leftarrow$ `rand()`

$m \leftarrow x \cdot n$ /* Use $2W$ bits for representation */

$l \leftarrow m \ \& \ (2^W - 1)$ /* $m \bmod 2^W$ */

if $l < n$ **then** /* Possibly skip division */

  $\mathcal{R} \leftarrow 2^W \bmod n$ /* Compute rejection threshold */

return $m \gg W$

The Algorithm - Pseudocode

$x \leftarrow$ `rand()`
$m \leftarrow x \cdot n$ /* Use $2W$ bits for representation */
$l \leftarrow m \;\&\; (2^W - 1)$ /* $m \bmod 2^W$ */
if $l < n$ **then** /* Possibly skip division */
  $\mathcal{R} \leftarrow 2^W \bmod n$ /* Compute rejection threshold */
  while $l < \mathcal{R}$ **do** /* Apply rejection rule */
return $m \gg W$

The Algorithm - Pseudocode

```
x ← rand()
m ← x · n                              /* Use 2W bits for representation */
l ← m & (2^W − 1)                      /* m mod 2^W */
if l < n then                          /* Possibly skip division */
    R ← 2^W mod n                      /* Compute rejection threshold */
    while l < R do                     /* Apply rejection rule */
        x ← rand()
        m ← x · n
        l ← m & (2^W − 1)
return m ≫ W
```

4 Summary

Summary

Summary

	expected number of integer division operations	maximum number of integer division operations	Unbiased?

Summary

	expected number of integer division operations	maximum number of integer division operations	Unbiased?
Modulo Reduction	1	1	✗

Summary

	expected number of integer division operations	maximum number of integer division operations	Unbiased?
Modulo Reduction	1	1	✗
Multiply-and-Shift	0	0	✗

Summary

	expected number of integer division operations	maximum number of integer division operations	Unbiased?
Modulo Reduction	1	1	✗
Multiply-and-Shift	0	0	✗
OpenBSD	2	2	✓

Summary

	expected number of integer division operations	maximum number of integer division operations	Unbiased?
Modulo Reduction	1	1	✗
Multiply-and-Shift	0	0	✗
OpenBSD	2	2	✓
Java	$\frac{2^W}{2^W - \mathcal{R}}$	∞	✓

Summary

	expected number of integer division operations	maximum number of integer division operations	Unbiased?
Modulo Reduction	1	1	✗
Multiply-and-Shift	0	0	✗
OpenBSD	2	2	✓
Java	$\frac{2^W}{2^W - \mathcal{R}}$	∞	✓
Lemire	$\frac{n}{2^W}$	1	✓

End of Talk

The Bitmask Algorithm - Representation

The Bitmask Algorithm - Representation

- Consider the binary representation of n:

The Bitmask Algorithm - Representation

- Consider the binary representation of n:

$$n \xrightarrow{\text{binary}} \underbrace{\overset{\overset{2^{W-1}}{\downarrow}}{0}, \ldots, 0}_{\text{only 0's}}, \overset{\overset{2^{\lfloor \log_2 n \rfloor}}{\downarrow}}{1}, \underbrace{1, \ldots, \overset{\overset{2^1}{\downarrow}}{0}, \overset{\overset{2^0}{\downarrow}}{1}}_{\text{series of 0's and 1's}}$$

The Bitmask Algorithm - Representation

- Consider the binary representation of n:

$$n \xrightarrow{\text{binary}} \underbrace{\overset{2^{W-1}}{\downarrow}\!\!0,\dots,0}_{\text{only 0's}},\overset{2^{\lfloor \log_2 n \rfloor}}{\downarrow}\!\!1,\underbrace{1,\dots,\overset{2^1}{\downarrow}\!\!0,\overset{2^0}{\downarrow}\!\!1}_{\text{series of 0's and 1's}}$$

- Every number $x \leq n$ only needs the last $\lfloor \log_2 n \rfloor + 1$ bits

The Bitmask Algorithm - Representation

- Consider the binary representation of n:

$$n \xrightarrow{\text{binary}} \underbrace{0,\dots,0}_{\text{only 0's}},\overset{2^{\lfloor \log_2 n \rfloor}}{1},\underbrace{1,\dots,0,1}_{\text{series of 0's and 1's}}$$

2^{W-1} $2^{\lfloor \log_2 n \rfloor}$ $2^1 2^0$

- Every number $x \leq n$ only needs the last $\lfloor \log_2 n \rfloor + 1$ bits
- Get these bits with a bitwise-AND with

$$2^{\lfloor \log_2 n \rfloor + 1} - 1 \xrightarrow{\text{binary}} \underbrace{0,\dots,0}_{\text{only 0's}},\underbrace{1,1,\dots,1,1}_{\text{only 1's}}$$

2^{W-1} $2^{\lfloor \log_2 n \rfloor}$ $2^1 2^0$

The Bitmask Algorithm - Mask

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$
\begin{array}{ccccccccc}
 & & 2^{W-1} & & 2^{\lfloor \log_2 n \rfloor} & & & 2^1 & 2^0 \\
 & & \downarrow & & \downarrow & & & \downarrow & \downarrow \\
n & \xrightarrow{\text{binary}} & \underbrace{0, \ldots, 0}_{\ell \text{ 0's}} & , & 1 & , & \underbrace{1, \ldots, 0, 1}_{\substack{\text{series of 0's} \\ \text{and 1's}}} & &
\end{array}
$$

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$n \xrightarrow{\text{binary}} \underbrace{\overset{2^{W-1}}{\overset{\downarrow}{0}},\dots,0}_{\ell\text{ 0's}},\ \overset{2^{\lfloor \log_2 n \rfloor}}{\overset{\downarrow}{1}},\ \underbrace{1,\dots,\overset{2^1}{\overset{\downarrow}{0}},\overset{2^0}{\overset{\downarrow}{1}}}_{\substack{\text{series of 0's}\\ \text{and 1's}}}$$

- $\lfloor \log_2 n \rfloor = W - \ell - 1$

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$2^{W-1} \qquad 2^{\lfloor \log_2 n \rfloor} \qquad 2^1 2^0$$

$$\downarrow \qquad\quad \downarrow \qquad\quad \downarrow \ \downarrow$$

$$n \xrightarrow{\text{binary}} \underbrace{0, \dots, 0}_{\ell\ 0\text{'s}}, 1, \underbrace{1, \dots, 0, 1}_{\substack{\text{series of 0's} \\ \text{and 1's}}}$$

- $\lfloor \log_2 n \rfloor = W - \ell - 1 \quad \longrightarrow \quad 2^{\lfloor \log_2 n \rfloor + 1} = 1 \ll (W - \ell)$

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$2^{W-1} \qquad 2^{\lfloor \log_2 n \rfloor} \qquad 2^1\, 2^0$$

$$n \xrightarrow{\text{binary}} \underbrace{0,\dots,0}_{\ell \text{ 0's}}, 1, \underbrace{1,\dots,0,1}_{\text{series of 0's and 1's}}$$

- $\lfloor \log_2 n \rfloor = W - \ell - 1 \qquad \longrightarrow \qquad 2^{\lfloor \log_2 n \rfloor + 1} = 1 \ll (W - \ell)$
- Algorithm:

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$
\begin{array}{cccc}
 & & 2^{W-1} \quad 2^{\lfloor \log_2 n \rfloor} \quad 2^1 2^0 \\
 & & \downarrow \quad\quad \downarrow \quad\quad \downarrow\ \downarrow \\
n & \xrightarrow{\text{binary}} & \underbrace{0, \ldots, 0}_{\ell \text{ 0's}}, 1, \underbrace{1, \ldots, 0, 1}_{\text{series of 0's and 1's}}
\end{array}
$$

- $\lfloor \log_2 n \rfloor = W - \ell - 1 \qquad \longrightarrow \qquad 2^{\lfloor \log_2 n \rfloor + 1} = 1 \ll (W - \ell)$
- Algorithm:
  (1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$\begin{array}{ccc} & & \begin{array}{cccc} 2^{W-1} & 2^{\lfloor \log_2 n \rfloor} & 2^1 & 2^0 \\ \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\ n & \xrightarrow{\text{binary}} & \underbrace{0, \ldots, 0}_{\ell \text{ 0's}}, 1, \underbrace{1, \ldots, 0, 1}_{\text{series of 0's and 1's}} \end{array}$$

- $\lfloor \log_2 n \rfloor = W - \ell - 1 \quad \longrightarrow \quad 2^{\lfloor \log_2 n \rfloor + 1} = 1 \ll (W - \ell)$
- Algorithm:
  (1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$
  (2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

The Bitmask Algorithm - Mask

- How can we compute $2^{\lfloor \log_2 n \rfloor + 1}$?
- Count the number ℓ of leading 0's in n!

$$n \xrightarrow{\text{binary}} \underbrace{\overset{\overset{2^{W-1}}{\downarrow}}{0}, \dots, 0}_{\ell\text{ 0's}}, \overset{\overset{2^{\lfloor \log_2 n \rfloor}}{\downarrow}}{1}, \underbrace{1, \dots, \overset{\overset{2^1}{\downarrow}}{0}, \overset{\overset{2^0}{\downarrow}}{1}}_{\substack{\text{series of 0's}\\ \text{and 1's}}}$$

- $\lfloor \log_2 n \rfloor = W - \ell - 1 \quad \longrightarrow \quad 2^{\lfloor \log_2 n \rfloor + 1} = 1 \ll (W - \ell)$
- Algorithm:
  (1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$
  (2) Draw $x \in [0, 2^W)$ and compute $b = x \;\&\; \mathcal{M}$
  (3) Return b if $b < n$ else goto **(2)**

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

- b at most $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1 < 2n$

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \;\&\; \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

- b at most $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1 < 2n \quad \longrightarrow \quad$ success probability at least $\approx \frac{1}{2}$

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

- b at most $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1 < 2n \quad \longrightarrow \quad$ success probability at least $\approx \frac{1}{2}$
- At most ≈ 2 rounds in expectation

Summary

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

- b at most $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1 < 2n \quad \longrightarrow \quad$ success probability at least $\approx \frac{1}{2}$
- At most ≈ 2 rounds in expectation
- No integer division at all

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

- b at most $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1 < 2n \quad \longrightarrow \quad$ success probability at least $\approx \frac{1}{2}$
- At most ≈ 2 rounds in expectation
- No integer division at all
- Computation of leading 0's requires `clz` instruction/algorithm

The Bitmask Algorithm - Efficiency

Algorithm:

(1) Compute ℓ and $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1$

(2) Draw $x \in [0, 2^W)$ and compute $b = x \ \& \ \mathcal{M}$

(3) Return b if $b < n$ else goto **(2)**

Efficiency

- b at most $\mathcal{M} = 2^{\lfloor \log_2 n \rfloor + 1} - 1 < 2n \quad \longrightarrow \quad$ success probability at least $\approx \frac{1}{2}$
- At most ≈ 2 rounds in expectation
- No integer division at all
- Computation of leading 0's requires `clz` instruction/algorithm
- Roughly as expensive as a `div` instruction