Mathematical Preliminaries

K. Subramani[1]

[1] Lane Department of Computer Science and Electrical Engineering
West Virginia University

January 26, 2015

Outline

Outline

Outline

Outline

Outline

Outline

Outline

Alphabets and strings

Alphabets and strings

Basics

Alphabets and strings

Basics

1. Alphabet -

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols,

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string. $|\epsilon| = 0$.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string. $|\epsilon| = 0$.
5. Powers of an alphabet

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string. $|\epsilon| = 0$.
5. Powers of an alphabet - Σ^k is the set of all strings of length k, each of whose symbols is in Σ.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string. $|\epsilon| = 0$.
5. Powers of an alphabet - Σ^k is the set of all strings of length k, each of whose symbols is in Σ.
6. Kleene Closure

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string. $|\epsilon| = 0$.
5. Powers of an alphabet - Σ^k is the set of all strings of length k, each of whose symbols is in Σ.
6. Kleene Closure - The set of all strings over Σ is denoted by Σ^*.

Alphabets and strings

Basics

1. Alphabet - A finite, non-empty collection of symbols, e.g., $\Sigma = \{a, b, \ldots\}$.
2. String - A finite sequence of symbols.
3. The empty string - ϵ.
4. Length of a string - Number of symbols in the string. $|\epsilon| = 0$.
5. Powers of an alphabet - Σ^k is the set of all strings of length k, each of whose symbols is in Σ.
6. Kleene Closure - The set of all strings over Σ is denoted by Σ^*. Clearly,

$$\Sigma^* = \cup_{i=0}^{\infty} \Sigma^i$$

Languages

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Example

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Example

1. The set of binary strings with an equal number of 0s and 1s.

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Example

1. The set of binary strings with an equal number of 0s and 1s.
2. Σ^*.

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Example

1. The set of binary strings with an equal number of 0s and 1s.
2. Σ^*.
3. The set of binary strings whose value is a prime.

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Example

1. The set of binary strings with an equal number of 0s and 1s.
2. Σ^*.
3. The set of binary strings whose value is a prime.
4. $\emptyset$.

Languages

Definition

Any set $L \subseteq \Sigma^*$ is called a language over Σ.

Example

1. The set of binary strings with an equal number of 0s and 1s.
2. Σ^*.
3. The set of binary strings whose value is a prime.
4. $\emptyset$.
5. $\{\epsilon\}$.

Problems

Problems

Definition

Give a language L and a string $w \in \Sigma^*$, decide whether $w \in L$.

Problems

Definition

Give a language L and a string $w \in \Sigma^*$, decide whether $w \in L$.

Example

Problems

Definition

Give a language L and a string $w \in \Sigma^*$, decide whether $w \in L$.

Example

Primality can be thought of as membership in the language L_p, where L_p is the set of all binary strings whose value is a prime.

Problems

Definition

Give a language L and a string $w \in \Sigma^*$, decide whether $w \in L$.

Example

Primality can be thought of as membership in the language L_p, where L_p is the set of all binary strings whose value is a prime. Answering the question may not always be easy.

Problems

Definition

Give a language L and a string $w \in \Sigma^*$, decide whether $w \in L$.

Example

Primality can be thought of as membership in the language L_p, where L_p is the set of all binary strings whose value is a prime. Answering the question may not always be easy.

Note

Languages and problems are two sides of the same coin.

Order of magnitude of functions

Order of magnitude of functions

Motivation

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

(i) *Additive and multiplicative constants do not matter in rate of growth.*

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

(i) *Additive and multiplicative constants do not matter in rate of growth.*

(ii) *The starting point of measurement does not matter.*

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

(i) *Additive and multiplicative constants do not matter in rate of growth.*

(ii) *The starting point of measurement does not matter.*

(iii) *We only care about functions from* $\Re_{\geq 0} \rightarrow \Re_{\geq 0}$.

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

(i) *Additive and multiplicative constants do not matter in rate of growth.*

(ii) *The starting point of measurement does not matter.*

(iii) *We only care about functions from* $\Re_{\geq 0} \rightarrow \Re_{\geq 0}$.

Example

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

(i) *Additive and multiplicative constants do not matter in rate of growth.*

(ii) *The starting point of measurement does not matter.*

(iii) *We only care about functions from* $\Re_{\geq 0} \rightarrow \Re_{\geq 0}$.

Example

(i) Which function grows faster: $100x^2$ or $\frac{1}{10^6}x^3$?

Order of magnitude of functions

Motivation

Order theory enables us to compare functions, just as the theory of arithmetic enables us to compare numbers.

In case of functions, we are interested in *rate of growth*, i.e., does function f grow at a faster rate than function g?

Note

(i) *Additive and multiplicative constants do not matter in rate of growth.*

(ii) *The starting point of measurement does not matter.*

(iii) *We only care about functions from* $\Re_{\geq 0} \rightarrow \Re_{\geq 0}$.

Example

(i) Which function grows faster: $100x^2$ or $\frac{1}{10^6}x^3$?

(ii) Which function grows faster: $x^2 - 10$ or $x + 10$?

Order of Magnitude (contd.)

Order of Magnitude (contd.)

Definition

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Definition

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = \Omega(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \geq c \cdot g(x)$.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = \Omega(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \geq c \cdot g(x)$.

Definition

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = \Omega(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \geq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = O(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \leq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = \Omega(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) \geq c \cdot g(x)$.

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = o(g)$, if there exist constants c and n_0 such that for all $n \geq n_0$, $f(x) < c \cdot g(x)$.

Order of Magnitude (contd.)

Order of Magnitude (contd.)

Definition

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = \Theta(g)$, if $f = O(g)$ and $g = O(f)$.

Order of Magnitude (contd.)

Definition

Let f and g be functions mapping non-negative reals to non-negative reals.

Then $f = \Theta(g)$, if $f = O(g)$ and $g = O(f)$.

Examples

Examples

Examples

Examples

Examples

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

(ii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

(ii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $f = \Omega(g)$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

(ii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $f = \Omega(g)$. Furthermore, $g = o(f)$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

(ii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $f = \Omega(g)$. Furthermore, $g = o(f)$.

(iii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

(ii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $f = \Omega(g)$. Furthermore, $g = o(f)$.

(iii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $g = O(f)$.

Examples

Examples

(i) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x^2 - 100$. $f = \Theta(g)$.

(ii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $f = \Omega(g)$. Furthermore, $g = o(f)$.

(iii) Let $f(x) = 2x^2 - 2$ and $g(x) = \frac{1}{100}x - 100$. $g = O(f)$. Furthermore, $g = o(f)$.

Test to determine order

Test to determine order

The limit test

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$.

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant,

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$,

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

(iii) If $l = \infty$,

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

(iii) If $l = \infty$, then $g = o(f)$.

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

(iii) If $l = \infty$, then $g = o(f)$.

Note

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x \to \infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

(iii) If $l = \infty$, then $g = o(f)$.

Note

If $\lim_{x \to \infty} f(x) = \infty$ and if $\lim_{x \to \infty} g(x) = \infty$, then,

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x\to\infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

(iii) If $l = \infty$, then $g = o(f)$.

Note

If $\lim_{x\to\infty} f(x) = \infty$ and if $\lim_{x\to\infty} g(x) = \infty$, then,

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = \lim_{x\to\infty} \frac{f'(x)}{g'(x)}$$

Test to determine order

The limit test

Let f and g denote two functions mapping non-negative reals to non-negative reals.

Let $l = \lim_{x\to\infty} \frac{f(x)}{g(x)}$. Then,

(i) If l is a positive constant, then $f = \Theta(g)$.

(ii) If $l = 0$, then $f = o(g)$.

(iii) If $l = \infty$, then $g = o(f)$.

Note

If $\lim_{x\to\infty} f(x) = \infty$ and if $\lim_{x\to\infty} g(x) = \infty$, then,

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = \lim_{x\to\infty} \frac{f'(x)}{g'(x)}$$

The above rule is called L'Hospital's rule.

Examples

Examples

Examples

Examples

(i) Show that $x = o(x^2)$.

Examples

Examples

(i) Show that $x = o(x^2)$.

(ii) Show that $x = o(x \log x)$.

Examples

Examples

(i) Show that $x = o(x^2)$.

(ii) Show that $x = o(x \log x)$.

(iii) Show that $\log x = o(x)$.

Some inequalities

Some inequalities

Useful relationships

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.
3. $n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n \cdot (1 + \Theta(\frac{1}{n}))$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.
3. $n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n \cdot (1 + \Theta(\frac{1}{n}))$.
4. $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.
3. $n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n \cdot (1 + \Theta(\frac{1}{n}))$.
4. $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.
5. $\ln(1 + x) = \sum_{i=1}^{\infty} (-1)^{i+1} \cdot \frac{x^i}{i}$, when $|x| < 1$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.
3. $n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n \cdot (1 + \Theta(\frac{1}{n}))$.
4. $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.
5. $\ln(1+x) = \sum_{i=1}^{\infty} (-1)^{i+1} \cdot \frac{x^i}{i}$, when $|x| < 1$.
6. $\lim_{n \to \infty} \frac{n^b}{a^n} = 0$, for all $a > 1$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.
3. $n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n \cdot (1 + \Theta(\frac{1}{n}))$.
4. $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.
5. $\ln(1 + x) = \sum_{i=1}^{\infty} (-1)^{i+1} \cdot \frac{x^i}{i}$, when $|x| < 1$.
6. $\lim_{n \to \infty} \frac{n^b}{a^n} = 0$, for all $a > 1$.
7. $a = b^{\log_b a}$.

Some inequalities

Useful relationships

1. $\log n! = \Theta(n \cdot \log n)$.
2. $n! = o(n^n), \omega(2^n)$.
3. $n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n \cdot (1 + \Theta(\frac{1}{n}))$.
4. $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.
5. $\ln(1 + x) = \sum_{i=1}^{\infty} (-1)^{i+1} \cdot \frac{x^i}{i}$, when $|x| < 1$.
6. $\lim_{n \to \infty} \frac{n^b}{a^n} = 0$, for all $a > 1$.
7. $a = b^{\log_b a}$.
8. $\lim_{n \to \infty} \frac{\log^b n}{n^a} = 0$, for all $a > 0$.

Quick tricks through calculus

Quick tricks through calculus

Bounding sums through integration

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function.

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function. Then,

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \leq \sum_{k=m}^{n} f(x) \leq \int_{m}^{n+1} f(x) \cdot dx.$$

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \leq \sum_{k=m}^{n} f(x) \leq \int_{m}^{n+1} f(x) \cdot dx.$$

2. Let f be a monotonically decreasing function.

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \leq \sum_{k=m}^{n} f(x) \leq \int_{m}^{n+1} f(x) \cdot dx.$$

2. Let f be a monotonically decreasing function. Then,

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \leq \sum_{k=m}^{n} f(x) \leq \int_{m}^{n+1} f(x) \cdot dx.$$

2. Let f be a monotonically decreasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \geq \sum_{k=m}^{n} f(x) \geq \int_{m}^{n+1} f(x) \cdot dx.$$

Quick tricks through calculus

Bounding sums through integration

1. Let f be a monotonically increasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \leq \sum_{k=m}^{n} f(x) \leq \int_{m}^{n+1} f(x) \cdot dx.$$

2. Let f be a monotonically decreasing function. Then,

$$\int_{m-1}^{n} f(x) \cdot dx \geq \sum_{k=m}^{n} f(x) \geq \int_{m}^{n+1} f(x) \cdot dx.$$

Exercise

Find upper and lowee bounds on $\sum_{i=1}^{n} \frac{1}{i}$.

Sample Space and Events

Sample Space and Events

Definition

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance,

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin.

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin. Then, $S = \{H,\ T\}$.

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin. Then, $S = \{H,\ T\}$.

(ii) Suppose that the experiment consists of tossing a die.

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin. Then, $S = \{H,\ T\}$.

(ii) Suppose that the experiment consists of tossing a die. Then, $S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$.

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin. Then, $S = \{H,\ T\}$.

(ii) Suppose that the experiment consists of tossing a die. Then, $S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$.

(iii) Suppose that the experiment consists of tossing two coins.

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin. Then, $S = \{H,\ T\}$.

(ii) Suppose that the experiment consists of tossing a die. Then, $S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$.

(iii) Suppose that the experiment consists of tossing two coins. Then, $S = \{HH,\ HT,\ TH,\ TT\}$.

Sample Space and Events

Definition

A random experiment is an experiment whose outcome is not known in advance, but belongs to a non-empty, non-singleton set called the sample space (usually denoted by S).

Example

(i) Suppose that the experiment consists of tossing a coin. Then, $S = \{H,\ T\}$.

(ii) Suppose that the experiment consists of tossing a die. Then, $S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$.

(iii) Suppose that the experiment consists of tossing two coins. Then, $S = \{HH,\ HT,\ TH,\ TT\}$.

Definition

Any subset of the sample space S is called an event.

Combining Events

Combining Events

Definition

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union)

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union) is defined as the event whose outcomes are in E or F;

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union) is defined as the event whose outcomes are in E or F; e.g., in the die tossing experiment, the union of the events $E = \{2,\ 4\}$ and $F = \{1\}$ is $\{1,\ 2,\ 4\}$.

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union) is defined as the event whose outcomes are in E or F; e.g., in the die tossing experiment, the union of the events $E = \{2,\ 4\}$ and $F = \{1\}$ is $\{1,\ 2,\ 4\}$.

Definition

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union) is defined as the event whose outcomes are in E or F; e.g., in the die tossing experiment, the union of the events $E = \{2,\ 4\}$ and $F = \{1\}$ is $\{1,\ 2,\ 4\}$.

Definition

Given two events E and F, the event EF

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union) is defined as the event whose outcomes are in E or F; e.g., in the die tossing experiment, the union of the events $E = \{2,\ 4\}$ and $F = \{1\}$ is $\{1,\ 2,\ 4\}$.

Definition

Given two events E and F, the event EF (intersection) is defined as the event whose outcomes are in E and F;

Combining Events

Definition

Given two events E and F, the event $E \cup F$ (union) is defined as the event whose outcomes are in E or F; e.g., in the die tossing experiment, the union of the events $E = \{2,\ 4\}$ and $F = \{1\}$ is $\{1,\ 2,\ 4\}$.

Definition

Given two events E and F, the event EF (intersection) is defined as the event whose outcomes are in E and F; e.g., in the die tossing experiment, the intersection of the events $E = \{1,\ 2,\ 3\}$ and $F = \{1\}$ is $\{1\}$.

Combining events (contd.)

Combining events (contd.)

Definition

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E;

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

If events E and F have no outcomes in common, then $EF = \emptyset$ and

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

If events E and F have no outcomes in common, then $EF = \emptyset$ and E and F are said to be *mutually exclusive*.

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

If events E and F have no outcomes in common, then $EF = \emptyset$ and E and F are said to be *mutually exclusive*. In this case, $P(EF) = 0$;

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

If events E and F have no outcomes in common, then $EF = \emptyset$ and E and F are said to be *mutually exclusive*. In this case, $P(EF) = 0$; in the single coin tossing experiment the events $\{H\}$ and $\{T\}$ are mutually exclusive.

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

If events E and F have no outcomes in common, then $EF = \emptyset$ and E and F are said to be *mutually exclusive*. In this case, $P(EF) = 0$; in the single coin tossing experiment the events $\{H\}$ and $\{T\}$ are mutually exclusive.

Note

Never forget that events are sets.

Combining events (contd.)

Definition

Given an event E, the event E^c (complement) denotes the event whose outcomes are in S, but not in E; e.g., in the die tossing experiment, the complement of the event $E = \{1,\ 2,\ 3\}$ is $\{4,\ 5,\ 6\}$.

Definition

If events E and F have no outcomes in common, then $EF = \emptyset$ and E and F are said to be *mutually exclusive*. In this case, $P(EF) = 0$; in the single coin tossing experiment the events $\{H\}$ and $\{T\}$ are mutually exclusive.

Note

Never forget that events are sets. This is particularly important when using logic to reason about them.

Defining Probabilities on Events

Defining Probabilities on Events

Assigning probabilities

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space.

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

(ii) $P(S) = 1$.

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

(ii) $P(S) = 1$.

(iii) If $E_1, E_2, \ldots, E_n$ are mutually exclusive events, then,

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

(ii) $P(S) = 1$.

(iii) If $E_1, E_2, \ldots, E_n$ are mutually exclusive events, then,

$$P(E_1 \cup E_2 \ldots E_n) = \sum_{i=1}^{n} P(E_i).$$

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

(ii) $P(S) = 1$.

(iii) If $E_1, E_2, \ldots, E_n$ are mutually exclusive events, then,

$$P(E_1 \cup E_2 \ldots E_n) = \sum_{i=1}^{n} P(E_i).$$

$P(E)$ is called the probability of event E.

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

(ii) $P(S) = 1$.

(iii) If $E_1, E_2, \ldots, E_n$ are mutually exclusive events, then,

$$P(E_1 \cup E_2 \ldots E_n) = \sum_{i=1}^{n} P(E_i).$$

$P(E)$ is called the probability of event E. The 2-tuple (S, P) is called a probability space.

Defining Probabilities on Events

Assigning probabilities

Let S denote a sample space. We assume that the number $P(E)$ is assigned to each event E in S, such that:

(i) $0 \leq P(E) \leq 1$.

(ii) $P(S) = 1$.

(iii) If $E_1, E_2, \ldots, E_n$ are mutually exclusive events, then,

$$P(E_1 \cup E_2 \ldots E_n) = \sum_{i=1}^{n} P(E_i).$$

$P(E)$ is called the probability of event E. The 2-tuple (S, P) is called a probability space. The above three conditions are called the axioms of probability theory.

Two Identities

Two Identities

Note

Two Identities

Note

(i) *Let E be an arbitrary event on the sample space S.*

Two Identities

Note

(i) *Let E be an arbitrary event on the sample space S. Then, $P(E) + P(E^c) = 1$.*

Two Identities

Note

(i) *Let E be an arbitrary event on the sample space S. Then, $P(E) + P(E^c) = 1$.*

(ii) *Let E and F denote two arbitrary events on the sample space S.*

Two Identities

Note

(i) *Let E be an arbitrary event on the sample space S. Then, $P(E) + P(E^c) = 1$.*

(ii) *Let E and F denote two arbitrary events on the sample space S. Then, $P(E \cup F) = P(E) + P(F) - P(EF)$.*

Two Identities

Note

(i) *Let E be an arbitrary event on the sample space S. Then, $P(E) + P(E^c) = 1$.*

(ii) *Let E and F denote two arbitrary events on the sample space S. Then, $P(E \cup F) = P(E) + P(F) - P(EF)$.*
What is $P(E \cup F)$, when E and F are mutually exclusive?

Two Identities

Note

(i) *Let E be an arbitrary event on the sample space S. Then, $P(E) + P(E^c) = 1$.*

(ii) *Let E and F denote two arbitrary events on the sample space S. Then, $P(E \cup F) = P(E) + P(F) - P(EF)$.*
What is $P(E \cup F)$, when E and F are mutually exclusive?
Let G be another event on S. What is $P(E \cup F \cup G)$?

Conditional Probability

Conditional Probability

Motivation

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads?

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Example

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Example

In the previously discussed coin tossing example, let E denote the event that both coins turn up heads and F denote the event that the first coin turns up heads.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Example

In the previously discussed coin tossing example, let E denote the event that both coins turn up heads and F denote the event that the first coin turns up heads. Accordingly, we are interested in $P(E \mid F)$.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Example

In the previously discussed coin tossing example, let E denote the event that both coins turn up heads and F denote the event that the first coin turns up heads. Accordingly, we are interested in $P(E \mid F)$. Observe that $P(F) = \frac{1}{2}$ and $P(EF) = \frac{1}{4}$.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Example

In the previously discussed coin tossing example, let E denote the event that both coins turn up heads and F denote the event that the first coin turns up heads. Accordingly, we are interested in $P(E \mid F)$. Observe that $P(F) = \frac{1}{2}$ and $P(EF) = \frac{1}{4}$. Hence, $P(E \mid F) = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}$.

Conditional Probability

Motivation

Consider the experiment of tossing two fair coins. What is the probability that both coins turn up heads? Now, assume that the first coin turns up heads. What is the probability that both coins turn up heads?

Definition

Let E and F denote two events on a sample space S. The conditional probability of E, given that the event F has occurred is denoted by $P(E \mid F)$ and is equal to $\frac{P(EF)}{P(F)}$, assuming $P(F) > 0$.

Example

In the previously discussed coin tossing example, let E denote the event that both coins turn up heads and F denote the event that the first coin turns up heads. Accordingly, we are interested in $P(E \mid F)$. Observe that $P(F) = \frac{1}{2}$ and $P(EF) = \frac{1}{4}$. Hence, $P(E \mid F) = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}$. Notice that $P(E) = \frac{1}{4} \neq P(E \mid F)$.

Independent Events

Independent Events

Definition

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Consider the experiment of tossing two fair dice.

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Consider the experiment of tossing two fair dice. Let F denote the event that the first die turns up 4.

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Consider the experiment of tossing two fair dice. Let F denote the event that the first die turns up 4. Let E_1 denote the event that the sum of the faces of the two dice is 6.

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Consider the experiment of tossing two fair dice. Let F denote the event that the first die turns up 4. Let E_1 denote the event that the sum of the faces of the two dice is 6. Let E_2 denote the event that the sum of the faces of the two dice is 7.

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Consider the experiment of tossing two fair dice. Let F denote the event that the first die turns up 4. Let E_1 denote the event that the sum of the faces of the two dice is 6. Let E_2 denote the event that the sum of the faces of the two dice is 7. Are E_1 and F independent?

Independent Events

Definition

Two events E and F on a sample space S are said to be independent, if the occurrence of one does not affect the occurrence of the other.
Mathematically,

$$P(E \mid F) = P(E).$$

Alternatively,

$$P(EF) = P(E) \cdot P(F)$$

Exercise

Consider the experiment of tossing two fair dice. Let F denote the event that the first die turns up 4. Let E_1 denote the event that the sum of the faces of the two dice is 6. Let E_2 denote the event that the sum of the faces of the two dice is 7. Are E_1 and F independent? How about E_2 and F?

Bayes' Formula

Bayes' Formula

Derivation

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S.

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive.

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$P(E) \quad =$$

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$P(E) = P(EF) + P(EF^c)$$

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$\begin{aligned} P(E) &= P(EF) + P(EF^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)P(F^c) \end{aligned}$$

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$\begin{aligned} P(E) &= P(EF) + P(EF^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)P(F^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)(1 - P(F)) \end{aligned}$$

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$\begin{aligned} P(E) &= P(EF) + P(EF^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)P(F^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)(1 - P(F)) \end{aligned}$$

Thus, the probability of an event E

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$\begin{aligned} P(E) &= P(EF) + P(EF^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)P(F^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)(1 - P(F)) \end{aligned}$$

Thus, the probability of an event E is the weighted average of the conditional probability of E, given that event F has occurred and the conditional probability of E, given that event F has not occurred,

Bayes' Formula

Derivation

Let E and F denote two arbitrary events on a sample space S. Clearly, $E = EF \cup EF^c$, where the events EF and EF^c are mutually exclusive. Now, observe that,

$$\begin{aligned} P(E) &= P(EF) + P(EF^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)P(F^c) \\ &= P(E \mid F)P(F) + P(E \mid F^c)(1 - P(F)) \end{aligned}$$

Thus, the probability of an event E is the weighted average of the conditional probability of E, given that event F has occurred and the conditional probability of E, given that event F has not occurred, each conditional probability being given as much weight as the probability of the event that it is conditioned on, has of occurring.

Random Variables

Random Variables

Motivation

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome,

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g.,

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7.

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or $\ldots$.

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Let X denote the random variable that is defined as the sum of two fair dice.

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Let X denote the random variable that is defined as the sum of two fair dice. What are the values that X can take?

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or $\ldots$.

Example

Let X denote the random variable that is defined as the sum of two fair dice. What are the values that X can take?

$$P\{X = 1\} \quad =$$

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Let X denote the random variable that is defined as the sum of two fair dice. What are the values that X can take?

$$P\{X = 1\} \quad = \quad 0$$

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Let X denote the random variable that is defined as the sum of two fair dice. What are the values that X can take?

$$\begin{aligned} P\{X = 1\} &= 0 \\ P\{X = 2\} &= \frac{1}{36} \end{aligned}$$

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Let X denote the random variable that is defined as the sum of two fair dice. What are the values that X can take?

$$\begin{aligned} P\{X = 1\} &= 0 \\ P\{X = 2\} &= \frac{1}{36} \\ &\vdots \end{aligned}$$

Random Variables

Motivation

In case of certain random experiments, we are not so much interested in the actual outcome, but in some function of the outcome, e.g., in the experiment of tossing two dice, we could be interested in knowing whether or not the the sum of the upturned faces is 7. We may not care whether the actual outcome is $(1, 6)$, $(6, 1)$, or ....

Example

Let X denote the random variable that is defined as the sum of two fair dice. What are the values that X can take?

$$\begin{aligned} P\{X = 1\} &= 0 \\ P\{X = 2\} &= \frac{1}{36} \\ &\vdots \\ P\{X = 12\} &= \frac{1}{36} \end{aligned}$$

The Bernoulli Random Variable

The Bernoulli Random Variable

Main idea

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes;

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes; one is labeled a “success” and the other a “failure”.

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes; one is labeled a “success” and the other a “failure”.

If we let the random variable X assume the value 1, if the experiment was a success and 0, if the experiment was a failure, then X is said to be a Bernoulli random variable.

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes; one is labeled a “success” and the other a “failure”.

If we let the random variable X assume the value 1, if the experiment was a success and 0, if the experiment was a failure, then X is said to be a Bernoulli random variable.

Assume that the probability that the experiment results in a success is p.

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes; one is labeled a “success” and the other a “failure”.

If we let the random variable X assume the value 1, if the experiment was a success and 0, if the experiment was a failure, then X is said to be a Bernoulli random variable.

Assume that the probability that the experiment results in a success is p.

The probability mass function of X is given by:

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes; one is labeled a “success” and the other a “failure”.

If we let the random variable X assume the value 1, if the experiment was a success and 0, if the experiment was a failure, then X is said to be a Bernoulli random variable.

Assume that the probability that the experiment results in a success is p.

The probability mass function of X is given by:

$$p(1) \quad = \quad P\{X = 1\} = p$$

The Bernoulli Random Variable

Main idea

Consider an experiment which has exactly two outcomes; one is labeled a "success" and the other a "failure".

If we let the random variable X assume the value 1, if the experiment was a success and 0, if the experiment was a failure, then X is said to be a Bernoulli random variable.

Assume that the probability that the experiment results in a success is p.

The probability mass function of X is given by:

$$\begin{aligned} p(1) &= P\{X = 1\} = p \\ p(0) &= P\{X = 0\} = 1 - p. \end{aligned}$$

The Binomial Random Variable

The Binomial Random Variable

Motivation

The Binomial Random Variable

Motivation

Consider an experiment which consists of n independent Bernoulli trials, with the probability of success in each trial being p.

The Binomial Random Variable

Motivation

Consider an experiment which consists of n independent Bernoulli trials, with the probability of success in each trial being p.

If X is the random variable that counts the number of successes in the n trials, then X is said to be a Binomial Random Variable.

The Binomial Random Variable

Motivation

Consider an experiment which consists of n independent Bernoulli trials, with the probability of success in each trial being p.

If X is the random variable that counts the number of successes in the n trials, then X is said to be a Binomial Random Variable.

The probability mass function of X is given by:

The Binomial Random Variable

Motivation

Consider an experiment which consists of n independent Bernoulli trials, with the probability of success in each trial being p.

If X is the random variable that counts the number of successes in the n trials, then X is said to be a Binomial Random Variable.

The probability mass function of X is given by:

$$p(i) = P\{X = i\} =$$

The Binomial Random Variable

Motivation

Consider an experiment which consists of n independent Bernoulli trials, with the probability of success in each trial being p.

If X is the random variable that counts the number of successes in the n trials, then X is said to be a Binomial Random Variable.

The probability mass function of X is given by:

$$p(i) = P\{X = i\} = C(n, i) \cdot p^i \cdot (1 - p)^{n-i}, \ i = 0, 1, 2, \ldots n$$

The Geometric Random Variable

The Geometric Random Variable

Motivation

The Geometric Random Variable

Motivation

Suppose that independent Bernoulli trials, each with probability p of success are performed until a success occurs.

The Geometric Random Variable

Motivation

Suppose that independent Bernoulli trials, each with probability p of success are performed until a success occurs.

If X is the random variable that counts the number of trials until the first success, then X is said to be a geometric random variable.

The Geometric Random Variable

Motivation

Suppose that independent Bernoulli trials, each with probability p of success are performed until a success occurs.

If X is the random variable that counts the number of trials until the first success, then X is said to be a geometric random variable.

The probability mass function of X is given by:

The Geometric Random Variable

Motivation

Suppose that independent Bernoulli trials, each with probability p of success are performed until a success occurs.

If X is the random variable that counts the number of trials until the first success, then X is said to be a geometric random variable.

The probability mass function of X is given by:

$$p(i) = P\{X = i\} =$$

The Geometric Random Variable

Motivation

Suppose that independent Bernoulli trials, each with probability p of success are performed until a success occurs.

If X is the random variable that counts the number of trials until the first success, then X is said to be a geometric random variable.

The probability mass function of X is given by:

$$p(i) = P\{X = i\} = (1-p)^{i-1} \cdot p, \ i = 1, 2, \ldots$$

Features of a random variable

Features of a random variable

Features

Features of a random variable

Features

Associated with each random variable are the following parameters:

Features of a random variable

Features

Associated with each random variable are the following parameters:

1. Probability mass function (pmt)

Features of a random variable

Features

Associated with each random variable are the following parameters:

1. Probability mass function (pmt) (Already discussed).

Features of a random variable

Features

Associated with each random variable are the following parameters:

1. Probability mass function (pmt) (Already discussed).
2. Cumulative distribution function or distribution function.

Features of a random variable

Features

Associated with each random variable are the following parameters:

1. Probability mass function (pmt) (Already discussed).
2. Cumulative distribution function or distribution function.
3. Expectation.

Features of a random variable

Features

Associated with each random variable are the following parameters:

1. Probability mass function (pmt) (Already discussed).
2. Cumulative distribution function or distribution function.
3. Expectation.
4. Variance.

Distribution Function

Distribution Function

Definition (Distribution Function)

Distribution Function

Definition (Distribution Function)

For a random variable X, the distribution function $F(\cdot)$ is defined for any real number b, $-\infty < b < \infty$, by

$$F(b) = P(X \leq b).$$

Expectation

Expectation

Definition (Expectation)

Expectation

Definition (Expectation)

Let X denote a discrete random variable with probability mass function $p(x)$.

Expectation

Definition (Expectation)

Let X denote a discrete random variable with probability mass function $p(x)$. The expected value of X, denoted by $E[X]$ is defined by:

$$E[X] = \sum_x x \cdot p(x).$$

Expectation

Definition (Expectation)

Let X denote a discrete random variable with probability mass function $p(x)$. The expected value of X, denoted by $E[X]$ is defined by:

$$E[X] = \sum_x x \cdot p(x).$$

Note

Expectation

Definition (Expectation)

Let X denote a discrete random variable with probability mass function $p(x)$. The expected value of X, denoted by $E[X]$ is defined by:

$$E[X] = \sum_x x \cdot p(x).$$

Note

$E[X]$ is the weighted average of the possible values that X can assume,

Expectation

Definition (Expectation)

Let X denote a discrete random variable with probability mass function $p(x)$. The expected value of X, denoted by $E[X]$ is defined by:

$$E[X] = \sum_x x \cdot p(x).$$

Note

$E[X]$ is the weighted average of the possible values that X can assume, each value being weighted by the probability that X assumes that value.

Variance and Covariance

Variance and Covariance

Definition (Variance)

The variance of a random variable X i(denoted by $Var(X)$ or σ^2) is given by

Variance and Covariance

Definition (Variance)

The variance of a random variable X i(denoted by $Var(X)$ or σ^2) is given by

$$E[(X - E[X])^2].$$

Variance and Covariance

Definition (Variance)

The variance of a random variable X i(denoted by $Var(X)$ or σ^2) is given by

$$E[(X - E[X])^2].$$

Definition (Covariance)

Given two (jointly distributed) random variables X and Y, the covariance of X and Y is defined as:

Variance and Covariance

Definition (Variance)

The variance of a random variable X i(denoted by $Var(X)$ or σ^2) is given by

$$E[(X - E[X])^2].$$

Definition (Covariance)

Given two (jointly distributed) random variables X and Y, the covariance of X and Y is defined as:

$$Cov(X, Y) = E[(X - E(X)) \cdot (Y - E(Y))].$$

Parameters of the important Random Variables

Parameters of the important Random Variables

Parameter table

Variable type	Expectation	Variance
Bernoulli	p	$p \cdot (1-p)$
Binomial	$n \cdot p$	$n \cdot p \cdot (1-p)$
Geometric	$\frac{1}{p}$	$\frac{1-p}{p^2}$

Parameters of the important Random Variables

Parameter table

Variable type	Expectation	Variance
Bernoulli	p	$p \cdot (1-p)$
Binomial	$n \cdot p$	$n \cdot p \cdot (1-p)$
Geometric	$\frac{1}{p}$	$\frac{1-p}{p^2}$

Exercise

Parameters of the important Random Variables

Parameter table

Variable type	Expectation	Variance
Bernoulli	p	$p \cdot (1-p)$
Binomial	$n \cdot p$	$n \cdot p \cdot (1-p)$
Geometric	$\frac{1}{p}$	$\frac{1-p}{p^2}$

Exercise

Find the parameters of the Poisson, Normal, Uniform and exponential random variables.

Expectation of the function of a random variable

Expectation of the function of a random variable

Theorem

Expectation of the function of a random variable

Theorem

If X is a random variable with pmf $p()$,

Expectation of the function of a random variable

Theorem

If X is a random variable with pmf $p()$, and $g()$ is any real-valued function, then,

Expectation of the function of a random variable

Theorem

If X is a random variable with pmf $p()$, and $g()$ is any real-valued function, then,

$$E[g(X)] =$$

Expectation of the function of a random variable

Theorem

If X is a random variable with pmf $p()$, and $g()$ is any real-valued function, then,

$$E[g(X)] = \sum_{x:\ p(x)>0} g(x) \cdot p(x)$$

Expectation of the function of a random variable

Theorem

If X is a random variable with pmf $p()$, and $g()$ is any real-valued function, then,

$$E[g(X)] = \sum_{x:\ p(x)>0} g(x) \cdot p(x)$$

Joint Distributions

Joint Distributions

Joint distribution functions

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

$$F(a,b) = P(X \leq a, Y \leq b),\ -\infty < a,b < \infty$$

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

$$F(a,b) = P(X \leq a, Y \leq b),\ -\infty < a,b < \infty$$

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

$$F(a,b) = P(X \leq a, Y \leq b),\ -\infty < a,b < \infty$$

The distribution of X (or Y) can be obtained from the joint distribution as follows:

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

$$F(a,b) = P(X \leq a, Y \leq b),\ -\infty < a,b < \infty$$

The distribution of X (or Y) can be obtained from the joint distribution as follows:

$$\begin{aligned} F_X(a) &= P(X \leq a) \\ &= P(X \leq a, Y \leq \infty) \\ &= F(a,\infty). \end{aligned}$$

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

$$F(a,b) = P(X \leq a, Y \leq b),\ -\infty < a, b < \infty$$

The distribution of X (or Y) can be obtained from the joint distribution as follows:

$$\begin{aligned} F_X(a) &= P(X \leq a) \\ &= P(X \leq a, Y \leq \infty) \\ &= F(a, \infty). \end{aligned}$$

Note

In case X and Y are discrete random variables, we can define the joint probability mass function as:

Joint Distributions

Joint distribution functions

For any two random variables X and Y, the joint cumulative distribution function is defined as:

$$F(a,b) = P(X \leq a, Y \leq b), \ -\infty < a, b < \infty$$

The distribution of X (or Y) can be obtained from the joint distribution as follows:

$$\begin{aligned} F_X(a) &= P(X \leq a) \\ &= P(X \leq a, Y \leq \infty) \\ &= F(a, \infty). \end{aligned}$$

Note

In case X and Y are discrete random variables, we can define the joint probability mass function as:

$$p(x,y) = P(X = x, \ Y = y).$$

Independent Random Variables

Independent Random Variables

Definition

Two random variables X and Y are said to be independent, if

Independent Random Variables

Definition

Two random variables X and Y are said to be independent, if

$$F(a,b) = F_X(a) \cdot F_Y(b), \ \forall a, b.$$

Independent Random Variables

Definition

Two random variables X and Y are said to be independent, if

$$F(a,b) = F_X(a) \cdot F_Y(b), \ \forall a, b.$$

When X and Y are discrete, the above condition reduces to:

Independent Random Variables

Definition

Two random variables X and Y are said to be independent, if

$$F(a,b) = F_X(a) \cdot F_Y(b), \ \forall a, b.$$

When X and Y are discrete, the above condition reduces to:

$$p(x,y) = p_x(x) \cdot p_y(y)$$

Linearity of Expectation

Linearity of Expectation

Proposition

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space.

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] =$$

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] = \sum_{i=1}^{n} a_i \cdot E[X_i]$$

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] = \sum_{i=1}^{n} a_i \cdot E[X_i]$$

Note

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] = \sum_{i=1}^{n} a_i \cdot E[X_i]$$

Note

Note that linearity of expectation holds even when the random variables are **not** *independent.*

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] = \sum_{i=1}^{n} a_i \cdot E[X_i]$$

Note

Note that linearity of expectation holds even when the random variables are **not** *independent. For random variables X_1 and X_2, $Var(X_1 + X_2) = Var(X_1) + Var(X_2)$, only if X_1 and X_2 are independent.*

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] = \sum_{i=1}^{n} a_i \cdot E[X_i]$$

Note

Note that linearity of expectation holds even when the random variables are **not** *independent. For random variables X_1 and X_2, $Var(X_1 + X_2) = Var(X_1) + Var(X_2)$, only if X_1 and X_2 are independent. More generally,*

Linearity of Expectation

Proposition

Let $X_1, X_2, \ldots, X_n$ denote n random variables, defined over some probability space. Let $a_1, a_2, \ldots, a_n$ denote n constants. Then,

$$E[\sum_{i=1}^{n} a_i \cdot X_i] = \sum_{i=1}^{n} a_i \cdot E[X_i]$$

Note

Note that linearity of expectation holds even when the random variables are **not** *independent. For random variables X_1 and X_2, $Var(X_1 + X_2) = Var(X_1) + Var(X_2)$, only if X_1 and X_2 are independent. More generally,*

$$Var(X_1 + X_2) = Var(X_1) + Var(X_2) + 2 \cdot Cov(X_1, X_2).$$

Concentration Inequalities

Concentration Inequalities

Tail bounds

Concentration Inequalities

Tail bounds

Consider the following problem:

Concentration Inequalities

Tail bounds

Consider the following problem: A fair coin is tossed n times. What is the probability that the number of heads is at least $\frac{3 \cdot n}{4}$?

Concentration Inequalities

Tail bounds

Consider the following problem: A fair coin is tossed n times. What is the probability that the number of heads is at least $\frac{3 \cdot n}{4}$? In general, the tail of a random X is the part of its pmf, that is away from its mean.

Concentration Inequalities

Tail bounds

Consider the following problem: A fair coin is tossed n times. What is the probability that the number of heads is at least $\frac{3 \cdot n}{4}$? In general, the tail of a random X is the part of its pmf, that is away from its mean.

Inequality	Known parameters	Tail bound
Markov	$X \geq 0, E[X]$	$P(X \geq a \cdot E[X]) \leq \frac{1}{a},\ a > 0$
Chebyshev	$E[X], Var(X)$	$P(\lvert X - E[X] \rvert \geq a \cdot E[X]) \leq \frac{Var(X)}{(a \cdot E[X])^2}, a > 0.$
Chernoff	X is binomial, $E[X]$	$P((X - E[X]) \geq \delta) \leq e^{-\frac{-2 \cdot \delta^2}{n}}, \delta > 0.$

Concentration Inequalities

Tail bounds

Consider the following problem: A fair coin is tossed n times. What is the probability that the number of heads is at least $\frac{3 \cdot n}{4}$? In general, the tail of a random X is the part of its pmf, that is away from its mean.

Inequality	Known parameters	Tail bound
Markov	$X \geq 0, E[X]$	$P(X \geq a \cdot E[X]) \leq \frac{1}{a},\ a > 0$
Chebyshev	$E[X], Var(X)$	$P(\lvert X - E[X] \rvert \geq a \cdot E[X]) \leq \frac{Var(X)}{(a \cdot E[X])^2}, a > 0.$
Chernoff	X is binomial, $E[X]$	$P((X - E[X]) \geq \delta) \leq e^{-\frac{-2 \cdot \delta^2}{n}}, \delta > 0.$

Exercise

Find the tail bounds for the coin tossing problem using all three techniques.

Groups

Groups

Definition

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity:

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.
2. Identity:

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.
2. Identity: There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.
2. Identity: There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. Inverse:

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.
2. Identity: There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. Inverse: Given $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$.

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.
2. Identity: There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. Inverse: Given $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$.

Example

Groups

Definition

A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.
2. Identity: There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. Inverse: Given $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$.

Example

$\mathcal{Z}$ with $+$ as the operator and 0 as the identity element.

Rings

Rings

Definition

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative:

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.
2. Additive commutative:

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.
2. Additive commutative: $a + b = b + a$, for all $a, b \in R$.

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.
2. Additive commutative: $a + b = b + a$, for all $a, b \in R$.
3. Additive identity:

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.
2. Additive commutative: $a + b = b + a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e + a = a + e = a$.

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.
2. Additive commutative: $a + b = b + a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e + a = a + e = a$.
4. Additive inverse:

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$.
2. Additive commutative: $a+b = b+a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e+a = a+e = a$.
4. Additive inverse: For every $a \in R$, there exists $-a \in R$ such that $a+(-a) = (-a)+a = e$.

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$.
2. Additive commutative: $a+b = b+a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e+a = a+e = a$.
4. Additive inverse: For every $a \in R$, there exists $-a \in R$ such that $a+(-a) = (-a)+a = e$.
5. Left and right distributivity:

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$.
2. Additive commutative: $a+b = b+a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e+a = a+e = a$.
4. Additive inverse: For every $a \in R$, there exists $-a \in R$ such that $a+(-a) = (-a)+a = e$.
5. Left and right distributivity: For all $a, b, c \in R$, we have, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$.
2. Additive commutative: $a+b = b+a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e+a = a+e = a$.
4. Additive inverse: For every $a \in R$, there exists $-a \in R$ such that $a+(-a) = (-a)+a = e$.
5. Left and right distributivity: For all $a, b, c \in R$, we have, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.
6. Multiplicative associativity: For all $a, b, c \in R$, we have, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$.
2. Additive commutative: $a+b = b+a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e+a = a+e = a$.
4. Additive inverse: For every $a \in R$, there exists $-a \in R$ such that $a+(-a) = (-a)+a = e$.
5. Left and right distributivity: For all $a, b, c \in R$, we have, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.
6. Multiplicative associativity: For all $a, b, c \in R$, we have, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Example

Rings

Definition

A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. Additive associative: $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$.
2. Additive commutative: $a+b = b+a$, for all $a, b \in R$.
3. Additive identity: There exists an element $e \in R$ such that for all $a \in R$, $e+a = a+e = a$.
4. Additive inverse: For every $a \in R$, there exists $-a \in R$ such that $a+(-a) = (-a)+a = e$.
5. Left and right distributivity: For all $a, b, c \in R$, we have, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.
6. Multiplicative associativity: For all $a, b, c \in R$, we have, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Example

$\mathcal{Z}$ under the usual addition and multiplication.

Fields

Fields

Definition

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative:

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.
3. Multiplicative identity:

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.
3. Multiplicative identity: There exists $1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in F$.

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.
3. Multiplicative identity: There exists $1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in F$.
4. Multiplicative inverse:

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.
3. Multiplicative identity: There exists $1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in F$.
4. Multiplicative inverse: If $a \in F$ and $a \neq 0$, there exists $b \in F$, such that $a \cdot b = b \cdot a = 1$.

Fields

Definition

A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:

1. $(F, +, \cdot)$ is a ring.
2. Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.
3. Multiplicative identity: There exists $1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in F$.
4. Multiplicative inverse: If $a \in F$ and $a \neq 0$, there exists $b \in F$, such that $a \cdot b = b \cdot a = 1$.

Example

The set $\Re$ with traditional addition and multiplication.

Bound Computation

Bound Computation

Upper and Lower bounds

Bound Computation

Upper and Lower bounds

1. Maximum/Minimum in an array.

Bound Computation

Upper and Lower bounds

1. Maximum/Minimum in an array.
2. Maximum and minimum in an array.

Bound Computation

Upper and Lower bounds

1. Maximum/Minimum in an array.
2. Maximum and minimum in an array.
3. Array sorting.

Bound Computation

Upper and Lower bounds

1. Maximum/Minimum in an array.
2. Maximum and minimum in an array.
3. Array sorting.
4. Matrix multiplication.

Problem types

Problem types

Three types of problems

Problem types

Three types of problems

1. The Königsberg bridge problem.

Problem types

Three types of problems

1. The Königsberg bridge problem.
2. The Hamilton Circuit problem.

Problem types

Three types of problems

1. The Königsberg bridge problem.
2. The Hamilton Circuit problem.
3. Playing Chess.

The path forward

The path forward

Roadmap

The path forward

Roadmap

1. Some problems permit insights.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.
3. The power of programming languages.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.
3. The power of programming languages.
4. Memory issues.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.
3. The power of programming languages.
4. Memory issues.
5. Coin tossing and adversary.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.
3. The power of programming languages.
4. Memory issues.
5. Coin tossing and adversary.
6. Arthur and Merlin.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.
3. The power of programming languages.
4. Memory issues.
5. Coin tossing and adversary.
6. Arthur and Merlin.
7. Holographic proofs.

The path forward

Roadmap

1. Some problems permit insights.
2. Some problems have short proofs.
3. The power of programming languages.
4. Memory issues.
5. Coin tossing and adversary.
6. Arthur and Merlin.
7. Holographic proofs.
8. Counting the number of solutions.