

# Introduction to Artificial Intelligence

## Introduction to Probability

Andres Mendez-Vazquez

February 6, 2019

# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Outline

## 1 Basic Theory

### ● Intuitive Formulation

- Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Gerolamo Cardano: Gambling out of Darkness

## Gambling

Gambling shows our interest in quantifying the ideas of probability for millennia, but exact mathematical descriptions arose much later.

Gerolamo Cardano (16th century)

While gambling he developed the following rule!!!

Equal conditions

"The most fundamental principle of all in gambling is simply equal conditions, e.g. of opponents, of bystanders, of money, of situation, of the dice box and of the dice itself. To the extent to which you depart from that equity, if it is in your opponent's favour, you are a fool, and if in your own, you are unjust."

# Gerolamo Cardano: Gambling out of Darkness

## Gambling

Gambling shows our interest in quantifying the ideas of probability for millennia, but exact mathematical descriptions arose much later.

## Gerolamo Cardano (16th century)

While gambling he developed the following rule!!!

### Equal conditions

"The most fundamental principle of all in gambling is simply equal conditions, e.g. of opponents, of bystanders, of money, of situation, of the dice box and of the dice itself. To the extent to which you depart from that equity, if it is in your opponent's favour, you are a fool, and if in your own, you are unjust."

# Gerolamo Cardano: Gambling out of Darkness

## Gambling

Gambling shows our interest in quantifying the ideas of probability for millennia, but exact mathematical descriptions arose much later.

## Gerolamo Cardano (16th century)

While gambling he developed the following rule!!!

## Equal conditions

“The most fundamental principle of all in gambling is simply equal conditions, e.g. of opponents, of bystanders, of money, of situation, of the dice box and of the dice itself. To the extent to which you depart from that equity, if it is in your opponent's favour, you are a fool, and if in your own, you are unjust.”

# Gerolamo Cardano's Definition

## Probability

“If therefore, someone should say, I want an ace, a deuce, or a trey, you know that there are 27 favorable throws, and since the circuit is 36, the rest of the throws in which these points will not turn up will be 9; the odds will therefore be 3 to 1.”

## Meaning

Probability as a ratio of favorable to all possible outcomes!!! As long all events are equiprobable...

## This way!

$$P(\text{All favourable throws}) = \frac{\text{Number All favourable throws}}{\text{Number of All throws}} \quad (1)$$

# Gerolamo Cardano's Definition

## Probability

“If therefore, someone should say, I want an ace, a deuce, or a trey, you know that there are 27 favorable throws, and since the circuit is 36, the rest of the throws in which these points will not turn up will be 9; the odds will therefore be 3 to 1.”

## Meaning

Probability as a ratio of favorable to all possible outcomes!!! As long all events are equiprobable...

$$P(\text{All favourable throws}) = \frac{\text{Number All favourable throws}}{\text{Number of All throws}} \quad (1)$$



# Gerolamo Cardano's Definition

## Probability

"If therefore, someone should say, I want an ace, a deuce, or a trey, you know that there are 27 favorable throws, and since the circuit is 36, the rest of the throws in which these points will not turn up will be 9; the odds will therefore be 3 to 1."

## Meaning

Probability as a ratio of favorable to all possible outcomes!!! As long all events are equiprobable...

Thus, we get

$$P(\text{All favourable throws}) = \frac{\text{Number All favourable throws}}{\text{Number of All throws}} \quad (1)$$

# Intuitive Formulation

## Empiric Definition

Intuitively, the probability of an event  $A$  could be defined as:

$$P(A) = \lim_{n \rightarrow \infty} \frac{N(A)}{n}$$

Where  $N(A)$  is the number that event  $a$  happens in  $n$  trials.



# Intuitive Formulation

## Empiric Definition

Intuitively, the probability of an event  $A$  could be defined as:

$$P(A) = \lim_{n \rightarrow \infty} \frac{N(A)}{n}$$

Where  $N(A)$  is the number that event  $A$  happens in  $n$  trials.

## Example

Imagine you have three dices, then

- The total number of outcomes is  $6^3$
- If we have event  $A =$  all numbers are equal,  $|A| = 6$
- Then, we have that  $P(A) = \frac{6}{6^3} = \frac{1}{36}$



# Intuitive Formulation

## Empiric Definition

Intuitively, the probability of an event  $A$  could be defined as:

$$P(A) = \lim_{n \rightarrow \infty} \frac{N(A)}{n}$$

Where  $N(A)$  is the number that event  $a$  happens in  $n$  trials.

## Example

Imagine you have three dices, then

- The total number of outcomes is  $6^3$
- If we have event  $A =$  all numbers are equal,  $|A| = 6$
- Then, we have that  $P(A) = \frac{6}{6^3} = \frac{1}{36}$



# Intuitive Formulation

## Empiric Definition

Intuitively, the probability of an event  $A$  could be defined as:

$$P(A) = \lim_{n \rightarrow \infty} \frac{N(A)}{n}$$

Where  $N(A)$  is the number that event  $a$  happens in  $n$  trials.

## Example

Imagine you have three dices, then

- The total number of outcomes is  $6^3$
- If we have event  $A =$  all numbers are equal,  $|A| = 6$

• Then, we have that  $P(A) = \frac{6}{6^3} = \frac{1}{36}$



# Intuitive Formulation

## Empiric Definition

Intuitively, the probability of an event  $A$  could be defined as:

$$P(A) = \lim_{n \rightarrow \infty} \frac{N(A)}{n}$$

Where  $N(A)$  is the number that event  $A$  happens in  $n$  trials.

## Example

Imagine you have three dices, then

- The total number of outcomes is  $6^3$
- If we have event  $A =$  all numbers are equal,  $|A| = 6$
- Then, we have that  $P(A) = \frac{6}{6^3} = \frac{1}{36}$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
    - Axioms
    - Using Set Operations
      - Example
    - Finite and Infinite Space
    - Counting, Frequentist Approach
    - Independence
    - Repeated Trials
      - Cartesian Products
    - Unconditional and Conditional Probability
    - Conditional Probability
    - Independence
    - Law of Total Probability
    - Bayes Theorem
    - Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance

# Some Famous Examples

## Famous Coin Tosses

- Count of Buffon tossed a coin 4040 times. Heads appeared 2048 times.
- K. Pearson tossed a coin 12000 times and 24000 times.
  - ▶ The heads appeared 6019 times and 12012, respectively.

## Something to Note

- For these three tosses the relative frequencies of heads are 0.5049, 0.5016, and 0.5005.





# Some Famous Examples

## Famous Coin Tosses

- Count of Buffon tossed a coin 4040 times. Heads appeared 2048 times.
- K. Pearson tossed a coin 12000 times and 24000 times.
  - ▶ The heads appeared 6019 times and 12012, respectively.

## Something Notable

- For these three tosses the relative frequencies of heads are 0.5049, 0.5016, and 0.5005.



# Outline

## 1 Basic Theory

- Intuitive Formulation
- Famous Examples
- **Axioms**
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Axioms of Probability

## Axioms

Given a sample space  $S$  of events, we have that

- $0 \leq P(A)$  for  $A \subseteq S$
- $P(S) = 1$
- If  $A_1$  and  $A_2$  are mutually exclusive events (i.e.  $P(A_1 \cap A_2) = 0$ ), then:

$$P(A_1 \cup A_2) = P(A_1) + P(A_2)$$



# Axioms of Probability

## Axioms

Given a sample space  $S$  of events, we have that

- 1  $0 \leq P(A)$  for  $A \subseteq S$
- 2  $P(S) = 1$
- 3 If  $A_1$  and  $A_2$  are mutually exclusive events (i.e.  $P(A_1 \cap A_2) = 0$ ), then:

$$P(A_1 \cup A_2) = P(A_1) + P(A_2)$$



# Axioms of Probability

## Axioms

Given a sample space  $S$  of events, we have that

- 1  $0 \leq P(A)$  for  $A \subseteq S$
- 2  $P(S) = 1$

3 If  $A_1$  and  $A_2$  are mutually exclusive events (i.e.  $P(A_1 \cap A_2) = 0$ ), then:

$$P(A_1 \cup A_2) = P(A_1) + P(A_2)$$



# Axioms of Probability

## Axioms

Given a sample space  $S$  of events, we have that

- 1  $0 \leq P(A)$  for  $A \subseteq S$
- 2  $P(S) = 1$
- 3 If  $A_1$  and  $A_2$  are mutually exclusive events (i.e.  $P(A_1 \cap A_2) = 0$ ), then:

$$P(A_1 \cup A_2) = P(A_1) + P(A_2)$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
- Famous Examples
- Axioms
- **Using Set Operations**
- Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
- Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
- Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Events as Sets

For example, in a dice experiment

$$A = \{i \mid \text{with } i \text{ an even number}\}$$





# Events as Sets

For example, in a dice experiment

$$A = \{i \mid \text{with } i \text{ an even number}\}$$

Thus, we have the following set operations

- 1  $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- 2  $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- 3  $A^c = \{x \mid x \notin A\}$



# Events as Sets

For example, in a dice experiment

$$A = \{i \mid \text{with } i \text{ an even number}\}$$

Thus, we have the following set operations

- 1  $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- 2  $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- 3  $A^c = \{x \mid x \notin A\}$



# Events as Sets

For example, in a dice experiment

$$A = \{i \mid \text{with } i \text{ an even number}\}$$

Thus, we have the following set operations

- 1  $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- 2  $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- 3  $A^C = \{x \mid x \notin A\}$



# Therefore

We can use combinations

Of such events with the previous operations to describe random phenomenas

Set of all throws even and greater than 3

- $A = \{i | i \text{ is even}\}$
- $B = \{i | i > 3\}$

Then

$$A \cap B = \{i | i \text{ is even and } i > 3\}$$



# Therefore

We can use combinations

Of such events with the previous operations to describe random phenomenas

Set of all throws even and greater than 3

- $A = \{i | i \text{ is even}\}$
- $B = \{i | i > 3\}$

Then

$$A \cap B = \{i | i \text{ is even and } i > 3\}$$



Cinvestav

# Therefore

We can use combinations

Of such events with the previous operations to describe random phenomenas

Set of all throws even and greater than 3

- $A = \{i | i \text{ is even}\}$
- $B = \{i | i > 3\}$

Then

$$A \cap B = \{i | i \text{ is even and } i > 3\}$$



## Example

The Probability of the empty set is

$$P(S) = P(S \cup \emptyset) = P(S) + P(\emptyset)$$

Given that  $S \neq \emptyset$ , therefore

$$P(\emptyset) = 0$$



## Example

The Probability of the empty set is

$$P(S) = P(S \cup \emptyset) = P(S) + P(\emptyset)$$

Given that  $\overline{S} = \emptyset$ , therefore

$$P(\emptyset) = 0$$





# Examples

The union  $A \cup B$  of two events  $A$  and  $B$

It is an event that occurs if at least one of the events  $A$  or  $B$  occur

For mutually exclusive events:

$$P(A \cup B) = P(A) + P(B)$$



# Examples

The union  $A \cup B$  of two events  $A$  and  $B$

It is an event that occurs if at least one of the events  $A$  or  $B$  occur

For mutually exclusive events

$$P(A \cup B) = P(A) + P(B)$$



## Further

### In the General Case

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

in the case of the complement

$$P(A^c) = 1 - P(A)$$

Given that

$$P(S) = P(A^c) + P(A)$$



## Further

### In the General Case

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

### In the case of the complement

$$P(A^C) = 1 - P(A)$$

Given that

$$P(S) = P(A^C) + P(A)$$



## Further

### In the General Case

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

### In the case of the complement

$$P(A^C) = 1 - P(A)$$

### Given that

$$P(S) = P(A^C) + P(A)$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
- Famous Examples
- Axioms
- **Using Set Operations**
  - **Example**
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

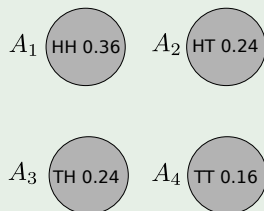
- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Example

## Setup

Throw a biased coin twice



We have the following event:

At least one head!!! Can you tell me which events are part of it?

What about this one?

Tail on first toss.

# Example

## Setup

Throw a biased coin twice

$A_1$  (HH 0.36)     $A_2$  (HT 0.24)

$A_3$  (TH 0.24)     $A_4$  (TT 0.16)

We have the following event

At least one head!!! Can you tell me which events are part of it?

What about this one?

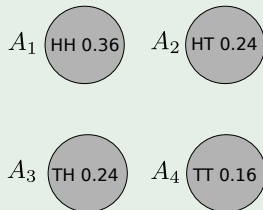
Tail on first toss.



# Example

## Setup

Throw a biased coin twice



We have the following event

At least one head!!! Can you tell me which events are part of it?

What about this one?

Tail on first toss.

# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- **Finite and Infinite Space**
  - Counting, Frequentist Approach
  - Independence
  - Repeated Trials
    - Cartesian Products
  - Unconditional and Conditional Probability
  - Conditional Probability
  - Independence
  - Law of Total Probability
  - Bayes Theorem
  - Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# We have that experiments in Probability are Defined as

## We have

- 1 The Set  $\mathcal{B}$  of all experimental outcomes
- 2 The Borel Field of all events of  $\mathcal{B}$
- 3 The Probability of Such Events

## Remarks about the Borel Field

- We use this field because we are given a way to measure infinite phenomena but Bounded.

## Therefore

- If you have a measure over a set  $\mathcal{B}$ , we would love to be able to measure:
  - ▶ The Union of such events
  - ▶ The Measure should be bounded.

# We have that experiments in Probability are Defined as

## We have

- 1 The Set  $\mathcal{B}$  of all experimental outcomes
- 2 The Borel Field of all events of  $\mathcal{B}$
- 3 The Probability of Such Events

## Remark about the Borel Field

- We use this field because we are given a way to measure infinite phenomena but Bounded.

## Measure

- If you have a measure over a set  $\mathcal{B}$ , we would love to be able to measure:
  - ▶ The Union of such events
  - ▶ The Measure should be bounded.

# We have that experiments in Probability are Defined as

## We have

- 1 The Set  $\mathcal{B}$  of all experimental outcomes
- 2 The Borel Field of all events of  $\mathcal{B}$
- 3 The Probability of Such Events

## Remark about the Borel Field

- We use this field because we are given a way to measure infinite phenomena but Bounded.

## Therefore

- If you have a measure over a set  $\mathcal{B}$ , we would love to be able to measure:
  - ▶ The Union of such events
  - ▶ The Measure should be bounded.

# Measuring Countable Spaces

If  $\mathcal{B} = \{A_1, A_2, \dots, A_N\}$

$$P(A_i) = p_i$$

Where

$$p_1 + p_2 + \dots + p_N = 1$$

Then, if you have  $B = \{A_1, \dots, A_k\}$  and  $k \leq N$

$$P(B) = \sum_{i=1}^k P(A_i)$$



# Measuring Countable Spaces

If  $\mathcal{B} = \{A_1, A_2, \dots, A_N\}$

$$P(A_i) = p_i$$

Where

$$p_1 + p_2 + \dots + p_N = 1$$

Then, if you have  $B = \{A_1, \dots, A_k\}$  and  $k \leq N$

$$P(B) = \sum_{i=1}^k P(A_i)$$



# Measuring Countable Spaces

If  $\mathcal{B} = \{A_1, A_2, \dots, A_N\}$

$$P(A_i) = p_i$$

Where

$$p_1 + p_2 + \dots + p_N = 1$$

Then, if you have  $B = A_1 \cup \dots \cup A_k$  and  $k \leq N$

$$P(B) = \sum_{i=1}^k P(A_i)$$





# In the Case of Equally Likely Events

We have that

$$p_i = \frac{1}{N}$$

Therefore

$$P(B) = \sum_{i=1}^k P(A_i) = \sum_{i=1}^k \frac{1}{N} = \frac{k}{N}$$



## In the Case of Equally Likely Events

We have that

$$p_i = \frac{1}{N}$$

Therefore

$$P(B) = \sum_{i=1}^k P(A_i) = \sum_{i=1}^k \frac{1}{N} = \frac{k}{N}$$



# The Real Line

## Here the Borel Sets

- It comes to save us...

### Something Notable

- In this case we are using events as intervals  $x_1 \leq x \leq x_2$
- And their finite Unions and Intersections

### For this, we define $\mathcal{B}$

The smallest Borel Field that includes half lines  $x \leq x_1$  with  $x_1 \in \mathbb{R}$ .



# The Real Line

## Here the Borel Sets

- It comes to save us...

## Something Notable

- In this case we are using events as intervals  $x_1 \leq x \leq x_2$
- And their finite Unions and Intersections

For this we claim:

The smallest Borel Field that includes half lines  $x \leq x_1$  with  $x_1 \in \mathbb{R}$ .



# The Real Line

## Here the Borel Sets

- It comes to save us...

## Something Notable

- In this case we are using events as intervals  $x_1 \leq x \leq x_2$
- And their finite Unions and Intersections

## For this, we define $\mathcal{B}$

The smallest Borel Field that includes half lines  $x \leq x_1$  with  $x_i \in \mathbb{R}$ .



# Important

This contains all the open and closed intervals, and all points

- This is not all possible subsets

These sets are not result of countable unions and intersections of intervals

- A Vitali set is a subset  $V$  of the interval  $[0, 1]$  of real numbers such that, for each real number  $r$ :
  - ▶ There is exactly one number  $v \in V$  such that  $v - r$  is a rational number

They do not describe experiments of interest

- These are of no interest for Probability



# Important

This contains all the open and closed intervals, and all points

- This is not all possible subsets

Those sets are not result of countable unions and intersections of intervals

- A Vitali set is a subset  $V$  of the interval  $[0, 1]$  of real numbers such that, for each real number  $r$ :
  - ▶ There is exactly one number  $v \in V$  such that  $v - r$  is a rational number

There are also some sets of no interest:

- These are of no interest for Probability



# Important

This contains all the open and closed intervals, and all points

- This is not all possible subsets

Those sets are not result of countable unions and intersections of intervals

- A Vitali set is a subset  $V$  of the interval  $[0, 1]$  of real numbers such that, for each real number  $r$ :
  - ▶ There is exactly one number  $v \in V$  such that  $v - r$  is a rational number

They do not describe experiments of interest

- These are of no interest for Probability





Therefore, we have

Assume that we have a function  $\alpha(x)$  such that

$$\int_{-\infty}^{\infty} \alpha(x) dx = 1 \text{ and } \alpha(x) \geq 0$$

We define that

$$P(x \leq x_1) = \int_{-\infty}^{x_1} \alpha(x) dx$$

Further, the survival function is defined as

$$P(x_1 \leq x \leq x_2) = \int_{x_1}^{x_2} \alpha(x) dx$$



Therefore, we have

Assume that we have a function  $\alpha(x)$  such that

$$\int_{-\infty}^{\infty} \alpha(x) dx = 1 \text{ and } \alpha(x) \geq 0$$

We define that

$$P(x \leq x_1) = \int_{-\infty}^{x_1} \alpha(x) dx$$

Further, the cumulative distribution function is defined as

$$P(x_1 \leq x \leq x_2) = \int_{x_1}^{x_2} \alpha(x) dx$$



Therefore, we have

Assume that we have a function  $\alpha(x)$  such that

$$\int_{-\infty}^{\infty} \alpha(x) dx = 1 \text{ and } \alpha(x) \geq 0$$

We define that

$$P(x \leq x_1) = \int_{-\infty}^{x_1} \alpha(x) dx$$

Further,  $x_1 \leq x \leq x_2$  is defined as

$$P(x_1 \leq x \leq x_2) = \int_{x_1}^{x_2} \alpha(x) dx$$



## Example

We have the following probability of emission of radioactive probabilities

$$\alpha(t) = ce^{-ct} I[t \geq 0] \text{ and } t \in \mathbb{R}$$

Therefore, the probability of being emitted in the interval  $(0, t_0]$

$$\int_0^{t_0} ce^{ct} dt = 1 - e^{-ct_0}$$



## Example

We have the following probability of emission of radioactive probabilities

$$\alpha(t) = ce^{-ct} I[t \geq 0] \text{ and } t \in \mathbb{R}$$

Therefore, the probability of being emitted in the interval  $(0, t_0)$

$$\int_0^{t_0} ce^{ct} dt = 1 - e^{-ct_0}$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- **Counting, Frequentist Approach**
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance

# We need to count!!!

## We have four main methods of counting

- 1 Ordered samples of size  $r$  with replacement
- 2 Ordered samples of size  $r$  without replacement
- 3 Unordered samples of size  $r$  without replacement
- 4 Unordered samples of size  $r$  with replacement



# We need to count!!!

## We have four main methods of counting

- 1 Ordered samples of size  $r$  with replacement
- 2 Ordered samples of size  $r$  without replacement
- 3 Unordered samples of size  $r$  without replacement
- 4 Unordered samples of size  $r$  with replacement





# We need to count!!!

## We have four main methods of counting

- 1 Ordered samples of size  $r$  with replacement
- 2 Ordered samples of size  $r$  without replacement
- 3 Unordered samples of size  $r$  without replacement
- 4 Unordered samples of size  $r$  with replacement



# We need to count!!!

## We have four main methods of counting

- 1 Ordered samples of size  $r$  with replacement
- 2 Ordered samples of size  $r$  without replacement
- 3 Unordered samples of size  $r$  without replacement
- 4 Unordered samples of size  $r$  with replacement



# Ordered samples of size $r$ with replacement

## Definition

The number of possible sequences  $(a_{i_1}, \dots, a_{i_r})$  for  $n$  different numbers is  $n \times n \times \dots \times n = n^r$

## Example

If you throw three dices you have  $6 \times 6 \times 6 = 216$



# Ordered samples of size $r$ with replacement

## Definition

The number of possible sequences  $(a_{i_1}, \dots, a_{i_r})$  for  $n$  different numbers is  $n \times n \times \dots \times n = n^r$

## Example

If you throw three dices you have  $6 \times 6 \times 6 = 216$



# Ordered samples of size $r$ without replacement

## Definition

The number of possible sequences  $(a_{i_1}, \dots, a_{i_r})$  for  $n$  different numbers is  $n \times n - 1 \times \dots \times (n - (r - 1)) = \frac{n!}{(n-r)!}$

## Example

The number of different numbers that can be formed if no digit can be repeated. For example, if you have 4 digits and you want numbers of size 3.



# Ordered samples of size $r$ without replacement

## Definition

The number of possible sequences  $(a_{i_1}, \dots, a_{i_r})$  for  $n$  different numbers is  $n \times n - 1 \times \dots \times (n - (r - 1)) = \frac{n!}{(n-r)!}$

## Example

The number of different numbers that can be formed if no digit can be repeated. For example, if you have 4 digits and you want numbers of size 3.



# Unordered samples of size $r$ without replacement

## Definition

Actually, we want the number of possible unordered sets.

However

We have  $\frac{n!}{(n-r)!}$  collections where we care about the order. Thus

$$\frac{n!}{(n-r)!} = \frac{n!}{r!(n-r)!} = \binom{n}{r} \quad (2)$$



# Unordered samples of size $r$ without replacement

## Definition

Actually, we want the number of possible unordered sets.

## However

We have  $\frac{n!}{(n-r)!}$  collections where we care about the order. Thus

$$\frac{n!}{(n-r)!} = \frac{n!}{r!(n-r)!} = \binom{n}{r} \quad (2)$$





# Unordered samples of size $r$ with replacement

## Definition

We want to find an unordered set  $\{a_{i_1}, \dots, a_{i_r}\}$  with replacement

Thus

$$\binom{n+r-1}{r} \quad (3)$$



# Unordered samples of size $r$ with replacement

## Definition

We want to find an unordered set  $\{a_{i_1}, \dots, a_{i_r}\}$  with replacement

Thus

$$\binom{n+r-1}{r} \quad (3)$$



## How? Use a digit trick for that

Change encoding by adding more signs

Imagine all the strings of three numbers with  $\{1, 2, 3\}$

We have

Old String	New String
111	$1+0,1+1,1+2=123$
112	$1+0,1+1,2+2=124$
113	$1+0,1+1,3+2=125$
122	$1+0,2+1,2+2=134$
123	$1+0,2+1,3+2=135$
133	$1+0,3+1,3+2=145$
222	$2+0,2+1,2+2=234$
223	$2+0,2+1,3+2=235$
233	$2+0,3+1,3+2=245$
333	$3+0,3+1,3+2=345$

## How? Use a digit trick for that

Change encoding by adding more signs

Imagine all the strings of three numbers with  $\{1, 2, 3\}$

We have

Old String	New String
111	$1+0,1+1,1+2=123$
112	$1+0,1+1,2+2=124$
113	$1+0,1+1,3+2=125$
122	$1+0,2+1,2+2=134$
123	$1+0,2+1,3+2=135$
133	$1+0,3+1,3+2=145$
222	$2+0,2+1,2+2=234$
223	$2+0,2+1,3+2=235$
233	$2+0,3+1,3+2=245$
333	$3+0,3+1,3+2=345$

# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- **Independence**
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Sometimes

We would like to model certain phenomena like

$$P(A_1, A_2, \dots, A_K)$$

The Problem is the complexity of calculating the joint distribution

We would like something simpler

Something like

$$P(A_1, A_2, \dots, A_K) = \text{Operation}_{i=1}^k P(A_i)$$



# Sometimes

We would like to model certain phenomena like

$$P(A_1, A_2, \dots, A_K)$$

The Problem is the complexity of calculating the joint distribution

We would like something simpler

Something like

$$P(A_1, A_2, \dots, A_K) = \text{Operation}_{i=1}^k P(A_i)$$



# Sometimes

We would like to model certain phenomena like

$$P(A_1, A_2, \dots, A_K)$$

The Problem is the complexity of calculating the joint distribution

We would like something simpler

Something like

$$P(A_1, A_2, \dots, A_K) = \text{Operation}_{i=1}^k P(A_i)$$





# Independence

## Definition

Two events  $A$  and  $B$  are independent if and only if

$$P(A, B) = P(A \cap B) = P(A)P(B)$$


## Example

We have two dices

Thus, we have all pairs  $(i, j)$  such that  $i, j = 1, 2, 3, \dots, 6$



# Example

We have two dices

Thus, we have all pairs  $(i, j)$  such that  $i, j = 1, 2, 3, \dots, 6$

We have the following events

- $A = \{\text{First dice } 1, 2 \text{ or } 3\}$
- $B = \{\text{First dice } 3, 4 \text{ or } 5\}$
- $C = \{\text{The sum of two faces is } 9\}$



# Example

We have two dices

Thus, we have all pairs  $(i, j)$  such that  $i, j = 1, 2, 3, \dots, 6$

We have the following events

- $A = \{\text{First dice } 1, 2 \text{ or } 3\}$
- $B = \{\text{First dice } 3, 4 \text{ or } 5\}$
- $C = \{\text{The sum of two faces is } 9\}$

So, we can do

Look at the board!!! Independence between  $A, B, C$



## Example

We have two dices

Thus, we have all pairs  $(i, j)$  such that  $i, j = 1, 2, 3, \dots, 6$

We have the following events

- $A = \{\text{First dice } 1, 2 \text{ or } 3\}$
- $B = \{\text{First dice } 3, 4 \text{ or } 5\}$
- $C = \{\text{The sum of two faces is } 9\}$

Now we can do

Look at the board!!! Independence between  $A, B, C$



## Example

We have two dices

Thus, we have all pairs  $(i, j)$  such that  $i, j = 1, 2, 3, \dots, 6$

We have the following events

- $A = \{\text{First dice } 1, 2 \text{ or } 3\}$
- $B = \{\text{First dice } 3, 4 \text{ or } 5\}$
- $C = \{\text{The sum of two faces is } 9\}$

So, we can do

Look at the board!!! Independence between  $A, B, C$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- **Repeated Trials**
  - Cartesian Products
  - Unconditional and Conditional Probability
  - Conditional Probability
  - Independence
  - Law of Total Probability
  - Bayes Theorem
  - Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- **Repeated Trials**
  - **Cartesian Products**
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



We have that

Given two sets  $\mathcal{A}$  and  $\mathcal{B}$

$$\mathcal{A} \times \mathcal{B} = \{(a, b) \mid a \in \mathcal{A} \text{ and } b \in \mathcal{B}\}$$

Example  $\mathcal{A} = \{a_1, a_2, a_3\}$  and  $\mathcal{B} = \{b_1, b_2\}$

$$\mathcal{A} \times \mathcal{B} = \{(a_1, b_1), (a_2, b_1), (a_3, b_1), (a_1, b_2), (a_2, b_2), (a_3, b_2)\}$$



We have that

Given two sets  $\mathcal{A}$  and  $\mathcal{B}$

$$\mathcal{A} \times \mathcal{B} = \{(a, b) \mid a \in \mathcal{A} \text{ and } b \in \mathcal{B}\}$$

Example  $\mathcal{A} = \{a_1, a_2, a_3\}$  and  $\mathcal{B} = \{b_1, b_2\}$

$$\mathcal{A} \times \mathcal{B} = \{(a_1, b_1), (a_2, b_1), (a_3, b_1), (a_1, b_2), (a_2, b_2), (a_3, b_2)\}$$



## Furthermore

If  $A \subseteq \mathcal{A}$  and  $B \subseteq \mathcal{B}$

$$C = A \times B$$

Look At the Board

- It is interesting!!!

Therefore,  $A \times B$  and  $A \times B$

$$A \times B = A \times B \cap A \times B$$



## Furthermore

If  $A \subseteq \mathcal{A}$  and  $B \subseteq \mathcal{B}$

$$C = A \times B$$

Look At the Board

- It is interesting!!!

Therefore,  $A \times B$  and  $A \times B$

$$A \times B = A \times B \cap A \times B$$



## Furthermore

If  $A \subseteq \mathcal{A}$  and  $B \subseteq \mathcal{B}$

$$C = A \times B$$

Look At the Board

- It is interesting!!!

Therefore,  $A \times B$  and  $\mathcal{A} \times \mathcal{B}$

$$A \times B = A \times \mathcal{B} \cap \mathcal{A} \times B$$



# Re-framing Independence

We have

- $P(A \times B) = P((a, b) | a \in A \text{ and } b \in B) = P(A)$
- $P(\mathcal{A} \times B) = P((a, b) | a \in \mathcal{A} \text{ and } b \in B) = P(B)$

Therefore, we can use our previous relation and assuming  $A \times B$  and  $\mathcal{A} \times B$  independent events

$$P(A \times B) = P(A \times B \cap \mathcal{A} \times B) = P(A)P(B)$$



# Re-framing Independence

We have

- $P(A \times \mathcal{B}) = P((a, b) | a \in A \text{ and } b \in \mathcal{B}) = P(A)$
- $P(\mathcal{A} \times B) = P((a, b) | a \in \mathcal{A} \text{ and } b \in B) = P(B)$

Therefore, we can use our previous relation and assuming  $A \times \mathcal{B}$  and  $\mathcal{A} \times B$  independent events

$$P(A \times B) = P(A \times \mathcal{B} \cap \mathcal{A} \times B) = P(A) P(B)$$



# We can use this to derive the Binomial Distribution

What???

We can do something quite interesting



Cinvestav



# First, we use a sequence of $n$ Bernoulli Trials

## We have this

- “Success” has a probability  $p$ .
- “Failure” has a probability  $1 - p$ .



# First, we use a sequence of $n$ Bernoulli Trials

## We have this

- “Success” has a probability  $p$ .
- “Failure” has a probability  $1 - p$ .

## Examples

- Toss a coin independently  $n$  times.
- Examine components produced on an assembly line.



# First, we use a sequence of $n$ Bernoulli Trials

## We have this

- “Success” has a probability  $p$ .
- “Failure” has a probability  $1 - p$ .

## Examples

- Toss a coin independently  $n$  times.
- Examine components produced on an assembly line.

We take  $S =$  all  $2^n$  ordered sequences of length  $n$ , with components 0 (failure) and 1 (success).



# First, we use a sequence of $n$ Bernoulli Trials

## We have this

- “Success” has a probability  $p$ .
- “Failure” has a probability  $1 - p$ .

## Examples

- Toss a coin independently  $n$  times.
- Examine components produced on an assembly line.

We take  $S =$  all  $2^n$  ordered sequences of length  $n$ , with components 0 (failure) and 1 (success).



# First, we use a sequence of $n$ Bernoulli Trials

## We have this

- “Success” has a probability  $p$ .
- “Failure” has a probability  $1 - p$ .

## Examples

- Toss a coin independently  $n$  times.
- Examine components produced on an assembly line.

## Now

We take  $S =$  all  $2^n$  ordered sequences of length  $n$ , with components **0 (failure)** and **1 (success)**.



# First

How do we represent such events?

We can use a sequence as

$$\langle a_1, a_2, \dots, a_n \rangle$$

With the following features

$$a_i \in S = \{0, 1\}$$



# First

How do we represent such events?

We can use a sequence as

$$\langle a_1, a_2, \dots, a_n \rangle$$

With the following features

$$a_i \in S = \{0, 1\}$$



# Meaning

We have one event  $A$

$$A = \text{Success} = 1$$

The Other Event  $A^c$

$$A^c = \text{Failure} = 0$$





# Meaning

We have one event  $A$

$$A = \textit{Success} = 1$$

The Other Event  $A^C$

$$A^C = \textit{Failure} = 0$$



Thus, taking a sample  $\omega$

$$\omega = 11 \cdots 10 \cdots 0 = \{0, 1\} \times \cdots \times \{0, 1\}$$

$k$  1's followed by  $n - k$  0's.



Thus, taking a sample  $\omega$

$$\omega = 11 \cdots 10 \cdots 0 = \{0, 1\} \times \cdots \times \{0, 1\}$$

$k$  1's followed by  $n - k$  0's.

We have then

$$\begin{aligned} P(\omega) &= P(A_1 \cap A_2 \cap \cdots \cap A_k \cap A_{k+1}^c \cap \cdots \cap A_n^c) \\ &= P(A_1) P(A_2) \cdots P(A_k) P(A_{k+1}^c) \cdots P(A_n^c) \\ &= p^k (1 - p)^{n-k} \end{aligned}$$



## Did you notice the following?

### After mapping the events through the probability

- We are losing the internal event structure

Which is not important, because

Events are mutually independent!!!

important

The number of such sample is the number of sets with  $k$  elements... or...

$$\binom{n}{k}$$



## Did you notice the following?

After mapping the events through the probability

- We are losing the internal event structure

Which is not important because

Events are mutually independent!!!

important!

The number of such sample is the number of sets with  $k$  elements... or...

$$\binom{n}{k}$$



## Did you notice the following?

After mapping the events through the probability

- We are losing the internal event structure

Which is not important because

Events are mutually independent!!!

Important

The number of such sample is the number of sets with  $k$  elements.... or...

$$\binom{n}{k}$$



# Therefore

We do not care where the 1's and 0's are

Thus all the probabilities are equal to  $p^k (1 - p)^{n-k}$

Thus, we are looking to sum all those probabilities of all those combinations of 1's and 0's

$$\sum_{k \text{ 1's}} p(\omega^k)$$

Then

$$\sum_{k \text{ 1's}} p(\omega^k) = \binom{n}{k} p^k (1-p)^{n-k}$$



Therefore

We do not care where the 1's and 0's are

Thus all the probabilities are equal to  $p^k (1 - p)^{n-k}$

Thus, we are looking to sum all those probabilities of all those combinations of 1's and 0's

$$\sum_{k \text{ 1's}} p (\omega^k)$$

$$\sum_{k \text{ 1's}} p (\omega^k) = \binom{n}{k} p (1 - p)^{n-k}$$





Therefore

We do not care where the 1's and 0's are

Thus all the probabilities are equal to  $p^k (1 - p)^{n-k}$

Thus, we are looking to sum all those probabilities of all those combinations of 1's and 0's

$$\sum_{k \text{ 1's}} p(\omega^k)$$

Then

$$\sum_{k \text{ 1's}} p(\omega^k) = \binom{n}{k} p^k (1 - p)^{n-k}$$



# Proving this is a probability

Sum of these probabilities is equal to 1

$$\sum_{k=0}^n \binom{n}{k} p (1-p)^{n-k} = (p + (1-p))^n = 1$$

The other is simple

$$0 \leq \binom{n}{k} p (1-p)^{n-k} \leq 1 \quad \forall k$$

This is known as

The Binomial probability function!!!



# Proving this is a probability

Sum of these probabilities is equal to 1

$$\sum_{k=0}^n \binom{n}{k} p (1-p)^{n-k} = (p + (1-p))^n = 1$$

The other is simple

$$0 \leq \binom{n}{k} p (1-p)^{n-k} \leq 1 \quad \forall k$$

This is known as

The Binomial probability function!!!



# Proving this is a probability

Sum of these probabilities is equal to 1

$$\sum_{k=0}^n \binom{n}{k} p (1-p)^{n-k} = (p + (1-p))^n = 1$$

The other is simple

$$0 \leq \binom{n}{k} p (1-p)^{n-k} \leq 1 \quad \forall k$$

This is known as

The Binomial probability function!!!



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- **Unconditional and Conditional Probability**
  - Conditional Probability
  - Independence
  - Law of Total Probability
  - Bayes Theorem
  - Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Unconditional Probability

## Definition

An **unconditional probability** is the probability of an event  $A$  prior to arrival of any evidence.



# Unconditional Probability

## Definition

An **unconditional probability** is the probability of an event  $A$  prior to arrival of any evidence.

## For Example

- $P(\text{Cavity}) = 0.1$  means that in the absence of any other information.  
▶ "There is a 10% chance that the patient is having a cavity"



# Unconditional Probability

## Definition

An **unconditional probability** is the probability of an event  $A$  prior to arrival of any evidence.

## For Example

- $P(\text{Cavity}) = 0.1$  means that in the absence of any other information.
  - ▶ **“There is a 10% chance that the patient is having a cavity”**





# Conditional Probability

## Definition

A **conditional probability** is the probability of one event if another event occurred.



# Conditional Probability

## Definition

A **conditional probability** is the probability of one event if another event occurred.

## For Example

- $P(\text{Cavity}/\text{Toothache}) = 0.8$  means that
  - ▶ "there is an 80% chance that the patient is having a cavity given that he is having a toothache"



# Conditional Probability

## Definition

A **conditional probability** is the probability of one event if another event occurred.

## For Example

- $P(\text{Cavity}/\text{Toothache}) = 0.8$  means that
  - ▶ “there is an 80% chance that the patient is having a cavity given that he is having a toothache”



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- **Conditional Probability**
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

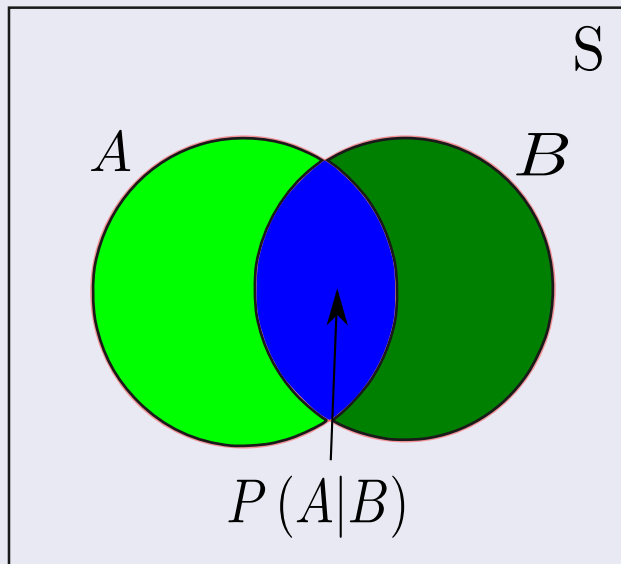
## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Basically

## Using Set Theory



However

We need a distribution!!!

$$\sum_{A \subseteq S} P(A) = 1$$

We then do the following

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$



However

We need a distribution!!!

$$\sum_{A \subseteq S} P(A) = 1$$

We then do the following

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$



Therefore

The conditional probability of  $A$  given  $B$  is written  $P(A|B)$

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A, B)}{P(B)}$$

with  $P(B) > 0$





We have that these are probabilities

First given  $0 < P(B)$  and  $0 \leq P(A \cap B)$

Then,

$$\frac{P(A, B)}{P(B)} \geq 0$$

Second, given if  $B \subseteq A$

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{P(B)}{P(B)} = 1$$

Third, given if  $A \subseteq B$

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{P(A)}{P(B)} \geq P(A) \geq 0$$

We have that this are probabilities

First given  $0 < P(B)$  and  $0 \leq P(A \cap B)$

Then,

$$\frac{P(A, B)}{P(B)} \geq 0$$

Second, given if  $B \subseteq A$

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{P(B)}{P(B)} = 1$$

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{P(A)}{P(B)} \geq P(A) \geq 0$$

We have that these are probabilities

First given  $0 < P(B)$  and  $0 \leq P(A \cap B)$

Then,

$$\frac{P(A, B)}{P(B)} \geq 0$$

Second, given if  $B \subseteq A$

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{P(B)}{P(B)} = 1$$

If  $A \subseteq B$

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{P(A)}{P(B)} \geq P(A) \geq 0$$

## Finally

We have that for  $A \cap B = \emptyset$

$$P(A \cup B | C) = \frac{P([A \cup B] \cap C)}{P(C)} = \frac{P([A \cap C] \cup [B \cap C])}{P(C)}$$

Then

$$P(A \cup B | C) = \frac{P(A \cap C) + P(B \cap C)}{P(C)} = \frac{P(A \cap C)}{P(C)} + \frac{P(B \cap C)}{P(C)}$$



## Finally

We have that for  $A \cap B = \emptyset$

$$P(A \cup B|C) = \frac{P([A \cup B] \cap C)}{P(C)} = \frac{P([A \cap C] \cup [B \cap C])}{P(C)}$$

Then

$$P(A \cup B|C) = \frac{P(A \cap C) + P(B \cap C)}{P(C)} = \frac{P(A \cap C)}{P(C)} + \frac{P(B \cap C)}{P(C)}$$



# Chain Rule

The probability that two events  $A$  and  $B$  will both occur is

$$P(A, B) = P(B)P(A|B) = P(A)P(B|A)$$

Flaw?

Any Ideas?



## Chain Rule

The probability that two events  $A$  and  $B$  will both occur is

$$P(A, B) = P(B)P(A|B) = P(A)P(B|A)$$

Flow?

Any Ideas?



Cinvestav

# Chain Rule

The probability that two events  $A$  and  $B$  will both occur is

$$P(A, B) = P(B)P(A|B) = P(A)P(B|A)$$

How?

Any Ideas?





# Therefore

This is also know

As the chain rule

Prove by induction

$$P(A_1, \dots, A_n) = P(A_n | A_{n-1} \dots A_1) P(A_{n-1} | A_{n-2} \dots A_1) \cdots P(A_2 | A_1) P(A_1)$$

Goal

Any idea?



# Therefore

This is also known

As the chain rule

Prove by induction

$$P(A_1, \dots, A_n) = P(A_n | A_{n-1} \dots A_1) P(A_{n-1} | A_{n-2} \dots A_1) \cdots P(A_2 | A_1) P(A_1)$$

Proof

Any idea?



Cinvestav

# Therefore

This is also know

As the chain rule

Prove by induction

$$P(A_1, \dots, A_n) = P(A_n | A_{n-1} \dots A_1) P(A_{n-1} | A_{n-2} \dots A_1) \cdots P(A_2 | A_1) P(A_1)$$

Proof

Any idea?



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- **Independence**
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Independence

If two events are independent

$$P(A|B) = P(A) \text{ and } P(B|A) = P(B).$$

Therefore, two events  $A$  and  $B$  are independent if

$$P(A, B) = P(A)P(B)$$



# Independence

If two events are independent

$$P(A|B) = P(A) \text{ and } P(B|A) = P(B).$$

Therefore, two events  $A$  and  $B$  are independent if

$$P(A, B) = P(A) P(B)$$



# Example

## Experiment

It involves a random draw from a standard deck of 52 playing cards.

Define events  $A$  and  $B$  to be

$A$  = The card is heart and  $B$  = The card is queen

Are the events independent?

How do we do it?



# Example

## Experiment

It involves a random draw from a standard deck of 52 playing cards.

Define events  $A$  and  $B$  to be

$A$  = The card is heart and  $B$  = The card is queen

Are the events independent?

How do we do it?





# Example

## Experiment

It involves a random draw from a standard deck of 52 playing cards.

Define events  $A$  and  $B$  to be

$A$  = The card is heart and  $B$  = The card is queen

Are the events independent?

How do we do it?



## Example

We have that

$$P(A, B) = \frac{1}{52}$$

But

$$P(A)P(B) = \frac{13}{52} \times \frac{4}{52}$$



## Example

We have that

$$P(A, B) = \frac{1}{52}$$

But

$$P(A)P(B) = \frac{13}{52} \times \frac{4}{52}$$



# What happens when you have independence in conditional setups?

## Conditional independence

$A$  and  $B$  are conditionally independent given  $C$  if and only if

$$P(A|B, C) = P(A|C)$$

## Example

$P(WetGrass|Season, Rain) = P(WetGrass|Rain)$ .



# What happens when you have independence in conditional setups?

## Conditional independence

$A$  and  $B$  are conditionally independent given  $C$  if and only if

$$P(A|B, C) = P(A|C)$$

## Example

$$P(\textit{WetGrass}|\textit{Season}, \textit{Rain}) = P(\textit{WetGrass}|\textit{Rain}).$$



## Example

Three cards are drawn from a deck

Find the probability of no obtaining a heart

We have

- 52 cards
- 39 of them not a heart

Define each of the draws

$A_i = \{\text{Card } i \text{ is not a heart}\}$  Then?



## Example

Three cards are drawn from a deck

Find the probability of no obtaining a heart

We have

- 52 cards
- 39 of them not a heart

Define each of the draws

$A_i = \{\text{Card } i \text{ is not a heart}\}$  Then?



## Example

Three cards are drawn from a deck

Find the probability of no obtaining a heart

We have

- 52 cards
- 39 of them not a heart

Define each of the draws

$A_i = \{\text{Card } i \text{ is not a heart}\}$  Then?





# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- **Law of Total Probability**
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



We have

### Definition

Events  $H_1, H_2, \dots, H_n$  form a partition of the sample space  $S$  if

- ① They are mutually exclusive  $H_i \cap H_j = \emptyset$  and  $i \neq j$
- ② Their union is the sample space  $S$ ,  $\bigcup_{i=1}^n H_i = S$



# We have

## Definition

Events  $H_1, H_2, \dots, H_n$  form a partition of the sample space  $S$  if

① They are mutually exclusive  $H_i \cap H_j = \emptyset$  and  $i \neq j$

② Their union is the sample space  $S$ ,  $\bigcup_{i=1}^n H_i = S$

The events  $H_1, H_2, \dots, H_n$  are usually called hypotheses

$$P(S) = P(H_1) + P(H_2) + \dots + P(H_n)$$



We have

### Definition

Events  $H_1, H_2, \dots, H_n$  form a partition of the sample space  $S$  if

- 1 They are mutually exclusive  $H_i \cap H_j = \emptyset$  and  $i \neq j$
- 2 Their union is the sample space  $S$ ,  $\cup_{i=1}^n H_i = S$

The events  $H_1, H_2, \dots, H_n$  are usually called hypotheses

$$P(S) = P(H_1) + P(H_2) + \dots + P(H_n)$$



We have

### Definition

Events  $H_1, H_2, \dots, H_n$  form a partition of the sample space  $S$  if

- 1 They are mutually exclusive  $H_i \cap H_j = \emptyset$  and  $i \neq j$
- 2 Their union is the sample space  $S$ ,  $\cup_{i=1}^n H_i = S$

The events  $H_1, H_2, \dots, H_n$  are usually called hypotheses

$$P(S) = P(H_1) + P(H_2) + \dots + P(H_n)$$



# Now

Let the event of interest  $A$  happens under any of the hypotheses  $H_i$

- With a known conditional probability  $P(A|H_i)$

Assume

- The probabilities of hypotheses  $H_1, \dots, H_n$  are known.

Total Probability Formula

$$P(A) = P(A|H_1)P(H_1) + \dots + P(A|H_n)P(H_n)$$



## Now

Let the event of interest  $A$  happens under any of the hypotheses  $H_i$

- With a known conditional probability  $P(A|H_i)$

Assume

- The probabilities of hypotheses  $H_1, \dots, H_n$  are known.

Total Probability Formula

$$P(A) = P(A|H_1)P(H_1) + \dots + P(A|H_n)P(H_n)$$



## Now

Let the event of interest  $A$  happens under any of the hypotheses  $H_i$

- With a known conditional probability  $P(A|H_i)$

Assume

- The probabilities of hypotheses  $H_1, \dots, H_n$  are known.

Total Probability Formula

$$P(A) = P(A|H_1)P(H_1) + \dots + P(A|H_n)P(H_n)$$





# Example

## Two-headed coin

Out of 100 coins one has heads on both sides.

One coin is chosen at random and flipped two times.

What is the probability to get

- Two heads?
- Two tails?



# Example

Two-headed coin

Out of 100 coins one has heads on both sides.

One coin is chosen at random and flipped two times

What is the probability to get

- Two heads?
- Two tails?



# Example

Two-headed coin

Out of 100 coins one has heads on both sides.

One coin is chosen at random and flipped two times

What is the probability to get

- 1 Two heads?
- 2 Two tails?



## Example

Let  $A$  be the event that two heads are obtained

Denote by  $H_1$  the event (hypothesis) that a fair coin was chosen.

## Example

Let  $A$  be the event that two heads are obtained

Denote by  $H_1$  the event (hypothesis) that a fair coin was chosen.

Now

The Hypothesis  $H_2 = H_1^C$  is the event that the two-headed coin was chosen.

## Example

Let  $A$  be the event that two heads are obtained

Denote by  $H_1$  the event (hypothesis) that a fair coin was chosen.

Now

The Hypothesis  $H_2 = H_1^C$  is the event that the two-headed coin was chosen.

Then, we have that

$$\begin{aligned} P(A) &= P(A|H_1)P(H_1) + P(A|H_2)P(H_2) \\ &= \frac{1}{4} \times \frac{99}{100} + 1 \times \frac{1}{100} \end{aligned}$$

$$= \frac{103}{400}$$

$$= 0.2575$$

## Example

Let  $A$  be the event that two heads are obtained

Denote by  $H_1$  the event (hypothesis) that a fair coin was chosen.

Now

The Hypothesis  $H_2 = H_1^C$  is the event that the two-headed coin was chosen.

Then, we have that

$$\begin{aligned} P(A) &= P(A|H_1)P(H_1) + P(A|H_2)P(H_2) \\ &= \frac{1}{4} \times \frac{99}{100} + 1 \times \frac{1}{100} \end{aligned}$$

$$= \frac{103}{400}$$

$$= 0.2575$$

## Example

Let  $A$  be the event that two heads are obtained

Denote by  $H_1$  the event (hypothesis) that a fair coin was chosen.

Now

The Hypothesis  $H_2 = H_1^C$  is the event that the two-headed coin was chosen.

Then, we have that

$$\begin{aligned}P(A) &= P(A|H_1)P(H_1) + P(A|H_2)P(H_2) \\ &= \frac{1}{4} \times \frac{99}{100} + 1 \times \frac{1}{100} \\ &= \frac{103}{400} \\ &= 0.2575\end{aligned}$$



## Example

Let  $A$  be the event that two heads are obtained

Denote by  $H_1$  the event (hypothesis) that a fair coin was chosen.

Now

The Hypothesis  $H_2 = H_1^C$  is the event that the two-headed coin was chosen.

Then, we have that

$$\begin{aligned}P(A) &= P(A|H_1)P(H_1) + P(A|H_2)P(H_2) \\ &= \frac{1}{4} \times \frac{99}{100} + 1 \times \frac{1}{100} \\ &= \frac{103}{400} \\ &= 0.2575\end{aligned}$$

What about the second one

Exercise

Answer: 0.2475



Cinvestav

# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- **Bayes Theorem**
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Bayes Theorem

## First

Let the event of interest  $A$  happens under any of hypotheses  $H_i$  with a known (conditional) probability  $P(A|H_i)$ .

## Assume

That the probabilities of hypotheses  $H_1, \dots, H_n$  are known (prior probabilities).

## Then

The conditional (posterior) probability of the hypothesis  $H_i$  given that  $A$  happened is

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A)}$$

# Bayes Theorem

## First

Let the event of interest  $A$  happens under any of hypotheses  $H_i$  with a known (conditional) probability  $P(A|H_i)$ .

## Assume

That the probabilities of hypotheses  $H_1, \dots, H_n$  are known (prior probabilities).

## Then

The conditional (posterior) probability of the hypothesis  $H_i$  given that  $A$  happened is

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A)}$$

# Bayes Theorem

## First

Let the event of interest  $A$  happens under any of hypotheses  $H_i$  with a known (conditional) probability  $P(A|H_i)$ .

## Assume

That the probabilities of hypotheses  $H_1, \dots, H_n$  are known (prior probabilities).

## Then

The conditional (posterior) probability of the hypothesis  $H_i$  given that  $A$  happened is

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A)}$$

Given the independence of the events

$H_1, H_2, \dots, H_n$  form a partition of the sample space  $S$

- Therefore

$$A = S \cap A = (H_1 \cup H_2 \cup \dots \cup H_n) \cap A$$

Therefore

$$A = \bigcup_{i=1}^n (H_i \cap A)$$



Given the independence of the events

$H_1, H_2, \dots, H_n$  form a partition of the sample space  $S$

- Therefore

$$A = S \cap A = (H_1 \cup H_2 \cup \dots \cup H_n) \cap A$$

Therefore

$$A = \cup_{i=1}^n (H_i \cap A)$$





# Where

We have

$$\begin{aligned}P(A) &= P(H_1 \cap A) + P(H_2 \cap A) + \cdots + P(H_n \cap A) \\ &= P(A|H_1)P(H_1) + \cdots + P(A|H_n)P(H_n)\end{aligned}$$



# Bayes Law of Total Probability

Therefore for an event  $H_i$

$$p(A, H_i) = P(A|H_i) P(H_i)$$

Then

$$P(H_i|A) = \frac{P(A, H_i)}{P(A)}$$



# Bayes Law of Total Probability

Therefore for an event  $H_i$

$$p(A, H_i) = P(A|H_i) P(H_i)$$

Then

$$P(H_i|A) = \frac{p(A, H_i)}{P(A)}$$



Thus

We have that

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A)}$$

Finally

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A|H_1) P(H_1) + \dots + P(A|H_n) P(H_n)}$$



Thus

We have that

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A)}$$

Finally

$$P(H_i|A) = \frac{P(A|H_i) P(H_i)}{P(A|H_1) P(H_1) + \cdots + P(A|H_n) P(H_n)}$$



## Another Interpretation

### One Version

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

## Another Interpretation

### One Version

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

### Where

- $P(A)$  is the **prior probability** or marginal probability of  $A$ .
  - ▶ It is "prior" in the sense that it does not take into account any information about  $B$ .
- $P(A|B)$  is the **conditional probability** of  $A$ , given  $B$ .
  - ▶ It is also called the posterior probability because it is derived from or depends upon the specified value of  $B$ .
- $P(B|A)$  is the **conditional probability** of  $B$  given  $A$ .
  - ▶ It is also called the likelihood.
- $P(B)$  is the **prior or marginal probability** of  $B$ , and acts as a normalizing constant.

## Another Interpretation

### One Version

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

### Where

- $P(A)$  is the **prior probability** or marginal probability of  $A$ .
  - ▶ It is "prior" in the sense that it does not take into account any information about  $B$ .
- $P(A|B)$  is the **conditional probability** of  $A$ , given  $B$ .
  - ▶ It is also called the posterior probability because it is derived from or depends upon the specified value of  $B$ .
- $P(B|A)$  is the conditional probability of  $B$  given  $A$ .
  - ▶ It is also called the likelihood.
- $P(B)$  is the prior or marginal probability of  $B$ , and acts as a normalizing constant.



## Another Interpretation

### One Version

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

### Where

- $P(A)$  is the **prior probability** or marginal probability of  $A$ .
  - ▶ It is "prior" in the sense that it does not take into account any information about  $B$ .
- $P(A|B)$  is the **conditional probability** of  $A$ , given  $B$ .
  - ▶ It is also called the posterior probability because it is derived from or depends upon the specified value of  $B$ .
- $P(B|A)$  is the **conditional probability** of  $B$  given  $A$ .
  - ▶ It is also called the likelihood.
- $P(B)$  is the prior or marginal probability of  $B$ , and acts as a normalizing constant.

## Another Interpretation

### One Version

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

### Where

- $P(A)$  is the **prior probability** or marginal probability of  $A$ .
  - ▶ It is "prior" in the sense that it does not take into account any information about  $B$ .
- $P(A|B)$  is the **conditional probability** of  $A$ , given  $B$ .
  - ▶ It is also called the posterior probability because it is derived from or depends upon the specified value of  $B$ .
- $P(B|A)$  is the **conditional probability** of  $B$  given  $A$ .
  - ▶ It is also called the likelihood.
- $P(B)$  is the **prior or marginal probability** of  $B$ , and acts as a normalizing constant.

# Example

## Setup

Throw two unbiased dice independently.

Let

- $A = \{\text{sum of the faces} = 8\}$
- $B = \{\text{faces are equal}\}$

Then calculate  $P(A|B)$ .

Look at the board



# Example

## Setup

Throw two unbiased dice independently.

## Let

- 1  $A = \{\text{sum of the faces} = 8\}$
- 2  $B = \{\text{faces are equal}\}$

Then calculate  $P(A|B)$ .

Look at the board



# Example

## Setup

Throw two unbiased dice independently.

## Let

- 1  $A = \{\text{sum of the faces} = 8\}$
- 2  $B = \{\text{faces are equal}\}$

Then calculate  $P(B|A)$

Look at the board



## Another Example

We have the following

Two coins are available, one unbiased and the other two headed

Assume

That you have a probability of  $\frac{3}{4}$  to choose the unbiased

## Another Example

We have the following

Two coins are available, one unbiased and the other two headed

Assume

That you have a probability of  $\frac{3}{4}$  to choose the unbiased

Events

- $A = \{\text{head comes up}\}$

## Another Example

We have the following

Two coins are available, one unbiased and the other two headed

Assume

That you have a probability of  $\frac{3}{4}$  to choose the unbiased

Events

- $A = \{\text{head comes up}\}$
- $B_1 = \{\text{Unbiased coin chosen}\}$
- $B_2 = \{\text{Biased coin chosen}\}$

► Find that if a head come up, find the probability that the two headed coin was chosen





## Another Example

We have the following

Two coins are available, one unbiased and the other two headed

Assume

That you have a probability of  $\frac{3}{4}$  to choose the unbiased

Events

- $A = \{\text{head comes up}\}$
- $B_1 = \{\text{Unbiased coin chosen}\}$
- $B_2 = \{\text{Biased coin chosen}\}$

► Find that if a head come up, find the probability that the two headed coin was chosen

# Another Example

We have the following

Two coins are available, one unbiased and the other two headed

Assume

That you have a probability of  $\frac{3}{4}$  to choose the unbiased

Events

- $A = \{\text{head comes up}\}$
- $B_1 = \{\text{Unbiased coin chosen}\}$
- $B_2 = \{\text{Biased coin chosen}\}$ 
  - ▶ Find that if a head come up, find the probability that the two headed coin was chosen

# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- **Application in Universal Hashing**

## 2 Random Variables

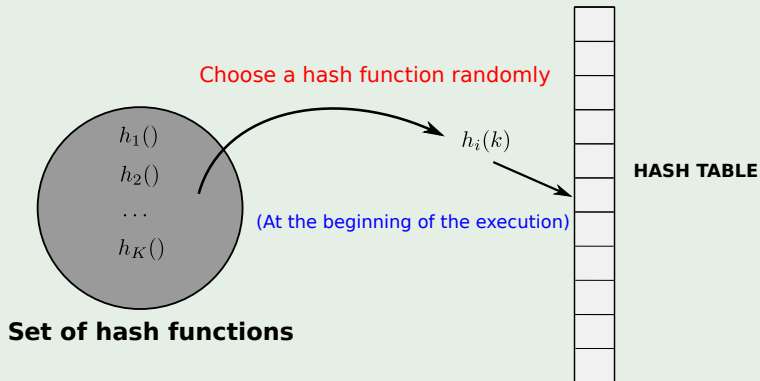
- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance

# Universal Hashing

## Example



# Definition of Universal Hash Functions

## Definition

Let  $H = \{h : U \rightarrow \{0, 1, \dots, m - 1\}\}$  be a family of hash functions.  $H$  is called a universal family if

$$\forall x, y \in U, x \neq y : \Pr_{h \in H}(h(x) = h(y)) \leq \frac{1}{m} \quad (4)$$

## Main result

With universal hashing the chance of collision between distinct keys  $k$  and  $l$  is no more than the  $\frac{1}{m}$  chance of collision if locations  $h(k)$  and  $h(l)$  were randomly and independently chosen from the set  $\{0, 1, \dots, m - 1\}$ .



# Definition of Universal Hash Functions

## Definition

Let  $H = \{h : U \rightarrow \{0, 1, \dots, m - 1\}\}$  be a family of hash functions.  $H$  is called a universal family if

$$\forall x, y \in U, x \neq y : \Pr_{h \in H}(h(x) = h(y)) \leq \frac{1}{m} \quad (4)$$

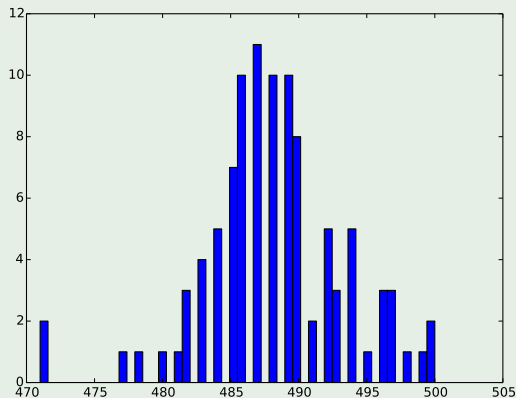
## Main result

With universal hashing the chance of collision between distinct keys  $k$  and  $l$  is no more than the  $\frac{1}{m}$  chance of collision if locations  $h(k)$  and  $h(l)$  were randomly and independently chosen from the set  $\{0, 1, \dots, m - 1\}$ .



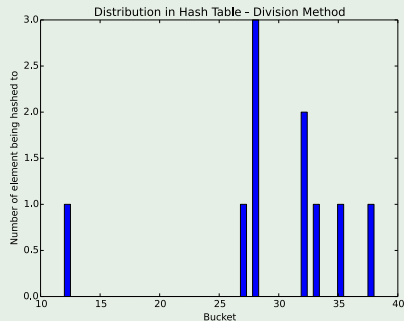
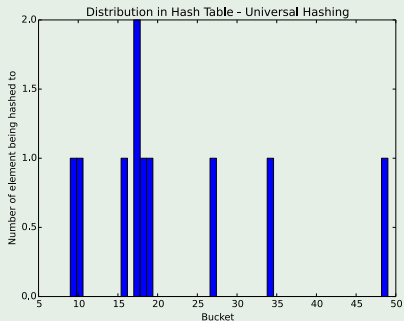
# Example of key distribution

Example, mean = 488.5 and dispersion = 5



# Example with 10 keys

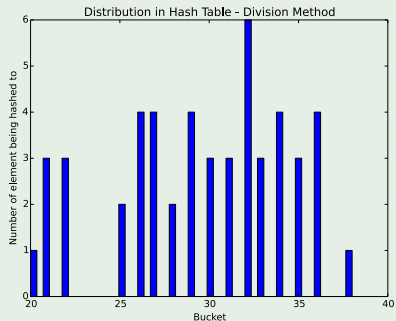
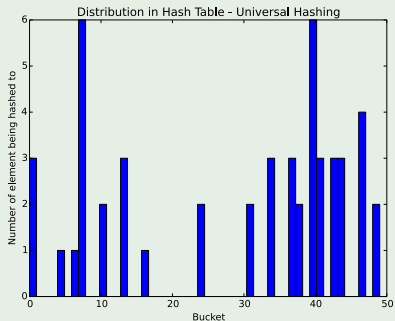
## Universal Hashing Vs Division Method





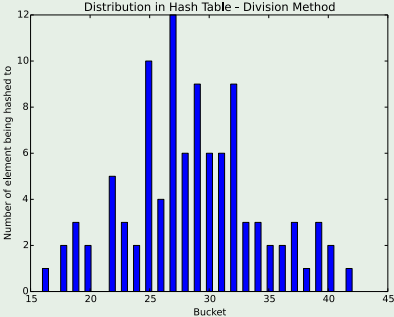
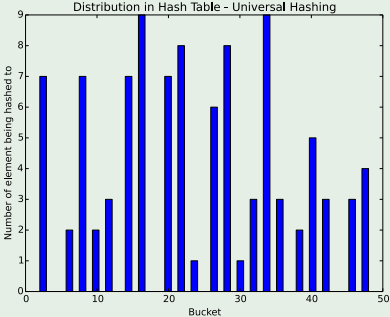
# Example with 50 keys

## Universal Hashing Vs Division Method



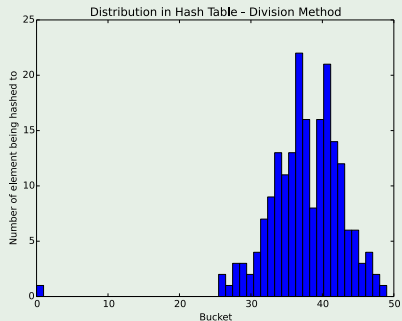
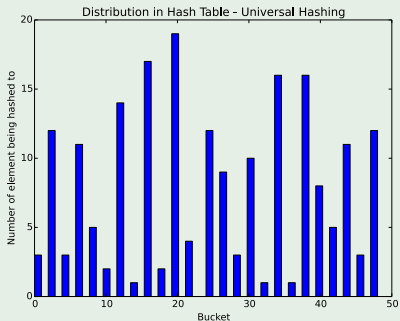
# Example with 100 keys

## Universal Hashing Vs Division Method



# Example with 200 keys

## Universal Hashing Vs Division Method



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- **Introduction**
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Random Variables

In many experiments,

It is easier to deal with a summary variable than with the original probability structure.



## Example

In an opinion poll, we ask 50 people whether agree or disagree with a certain issue

- Suppose we record a “1” for agree and “0” for disagree.

The sample space for this experiment has  $2^{50}$  elements

- Why?

Suppose we are only interested in the number of people who agree

- Define the variable  $X$  = number of “1” ’s recorded out of 50.
  - Easier to deal with this sample space (has only 51 elements).



## Example

In an opinion poll, we ask 50 people whether agree or disagree with a certain issue

- Suppose we record a “1” for agree and “0” for disagree.

The sample space for this experiment has  $2^{50}$  elements

- Why?

Suppose we are only interested in the number of people who agree

- Define the variable  $X$  = number of “1” ’s recorded out of 50.
  - Easier to deal with this sample space (has only 51 elements).



## Example

In an opinion poll, we ask 50 people whether agree or disagree with a certain issue

- Suppose we record a “1” for agree and “0” for disagree.

The sample space for this experiment has  $2^{50}$  elements

- Why?

Suppose we are only interested in the number of people who agree

- Define the variable  $X$  =number of “1” ’s recorded out of 50.
  - ▶ Easier to deal with this sample space (has only 51 elements).





Thus

It is necessary to define a function “random variable as follow”

$$X : S \rightarrow \mathbb{R}$$

Graphically



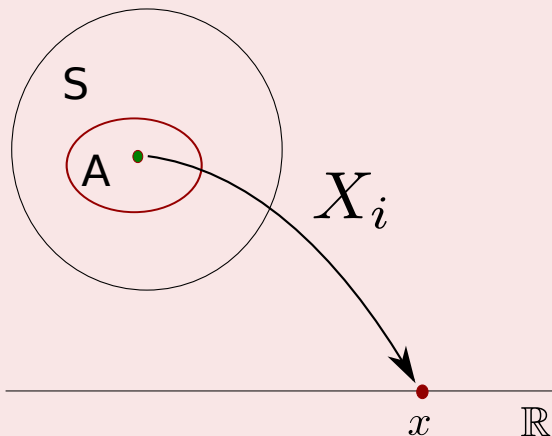
Cinvestav

Thus

It is necessary to define a function “random variable as follow”

$$X : S \rightarrow \mathbb{R}$$

Graphically



# Definition

## How?

What is the probability function of the random variable is being defined from the probability function of the original sample space?

### For this

- Suppose the sample space is  $S = \{s_1, s_2, \dots, s_n\}$

### Now

- Suppose the range of the random variable  $X = \langle x_1, x_2, \dots, x_m \rangle$



# Definition

## How?

What is the probability function of the random variable is being defined from the probability function of the original sample space?

## For this

- Suppose the sample space is  $S = \{s_1, s_2, \dots, s_n\}$

## Now

- Suppose the range of the random variable  $X = \langle x_1, x_2, \dots, x_m \rangle$



# Definition

## How?

What is the probability function of the random variable is being defined from the probability function of the original sample space?

## For this

- Suppose the sample space is  $S = \{s_1, s_2, \dots, s_n\}$

## Now

- Suppose the range of the random variable  $X = \langle x_1, x_2, \dots, x_m \rangle$



Then

We have that

- We observe  $X = x_i$  if and only if the outcome of the random experiment is an  $s \in S$  s.t.  $X(s) = x_j$

$$P(X = x_j) = P(s \in S | X(s) = x_j)$$



# Then

## We have that

- We observe  $X = x_i$  if and only if the outcome of the random experiment is an  $s \in S$  s.t.  $X(s) = x_j$

## Or

$$P(X = x_j) = P(s \in S | X(s) = x_j)$$



Therefore

If the events in  $S$  are disjoint

$$P(X = x_j) = \sum_{s \in S} P(s | X(s) = x_j)$$

Therefore, if we can decompose

We can easily see the relationship between Random Variables and The Events in  $S$





Therefore

If the events in  $S$  are disjoint

$$P(X = x_j) = \sum_{s \in S} P(s | X(s) = x_j)$$

Therefore if we can decompose  $S$

We can easily see the relationship between Random Variables and The Events in  $S$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- **Formal Definition**
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# We have

## Definition

- A Random Variable  $X$  is a process of assigning a number  $X(A)$  to every outcome  $A$ .

The resulting function must satisfy the the following two conditions

- The set  $\{X \leq x\}$  is an event for every  $x \in \mathbb{R}$ .
- The probability of the events  $\{X = \infty\}$  and  $\{X = -\infty\}$  equal zero:

$$P\{X = \infty\} = 0 \quad P\{X = -\infty\} = 0$$



# We have

## Definition

- A Random Variable  $X$  is a process of assigning a number  $X(A)$  to every outcome  $A$ .

The resulting function must satisfy the the following two conditions

- 1 The set  $\{X \leq x\}$  is an event for every  $x \in \mathbb{R}$ .
- 2 The probability of the events  $\{X = \infty\}$  and  $X = -\infty$  equal zero:

$$P\{X = \infty\} = 0 \quad P\{X = -\infty\} = 0$$



# Example

## Setup

Throw a coin 10 times, and let  $R$  be the number of heads.

Then

$S =$  all sequences of length 10 with components H and T

We have for

$\omega = \text{HHHHTTHTTTH} \Rightarrow R(\omega) = 6$



# Example

## Setup

Throw a coin 10 times, and let  $R$  be the number of heads.

## Then

$S$  = all sequences of length 10 with components H and T

We have for

$$\omega = \text{HHHHTTHTTH} \Rightarrow R(\omega) = 6$$



# Example

## Setup

Throw a coin 10 times, and let  $R$  be the number of heads.

## Then

$S$  = all sequences of length 10 with components H and T

## We have for

$\omega = \text{HHHHTTHTTH} \Rightarrow R(\omega) = 6$



# Example

## Setup

Let  $R$  be the number of heads in two independent tosses of a coin.

- Probability of head is .6

What are the probabilities?

$$\Omega = \{HH, HT, TH, TT\}$$

Thus, we can calculate

$$P(R=0), P(R=1), P(R=2)$$





# Example

## Setup

Let  $R$  be the number of heads in two independent tosses of a coin.

- Probability of head is .6

## What are the probabilities?

$$\Omega = \{HH, HT, TH, TT\}$$

Thus, we can calculate

$$P(R=0), P(R=1), P(R=2)$$



# Example

## Setup

Let  $R$  be the number of heads in two independent tosses of a coin.

- Probability of head is .6

## What are the probabilities?

$$\Omega = \{HH, HT, TH, TT\}$$

Thus, we can calculate

$$P(R = 0), P(R = 1), P(R = 2)$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- **Probability of a Random Variable**
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Note

If we are interested in a random variable  $X$

We want to know its probabilities

Basically

Measurement of such variables leads to measurements as

$$a \leq X \leq b$$

Therefore, we are looking at the following probabilities

$$P(s|a \leq X(s) \leq b)$$



# Note

If we are interested in a random variable  $X$

We want to know its probabilities

Basically

Measurement of such variables leads to measurements as

$$a \leq X \leq b$$

Therefore, we are looking at the following probabilities

$$P(s|a \leq X(s) \leq b)$$



## Note

If we are interested in a random variable  $X$

We want to know its probabilities

Basically

Measurement of such variables leads to measurements as

$$a \leq X \leq b$$

Therefore, we are looking at the following probabilities

$$P(s|a \leq X(s) \leq b)$$



Then

## Definition

- The distribution of a Random Variable  $X$  is the function

$$F_X(x) = P\{X \leq x\}$$

- ▶ Defined for all  $x \in \mathbb{R}$



Cinvestav

## Example

For example, if a coin is tossed independently  $n$  times

With:

- 1 Probability  $p$  of coming heads on a given toss.
- 2 And  $X$  is the number of heads

We have that

$$P(a \leq X(s) \leq b) = \sum_{k=a}^b \binom{n}{k} p^k (1-p)^{n-k}$$





# Example

For example, if a coin is tossed independently  $n$  times

With:

- 1 Probability  $p$  of coming heads on a given toss.
- 2 And  $X$  is the number of heads

We have that

$$P(a \leq X(s) \leq b) = \sum_{k=1}^b \binom{n}{k} p^k (1-p)^{n-k}$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- **Types of Random Variables**
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# We have Two Types of Random Variables

## Definition

The Random Variable  $X$  is said to be discrete if and only if the set of possible values of  $X$  is finite or countably infinite.

Then

if  $x_1, x_2, \dots$  are the values of  $X$  that belong to the range  $R$  of it,

$$P(X = x_1, X = x_2, \dots) = \sum_{x \in R} p_X(x)$$



# We have Two Types of Random Variables

## Definition

The Random Variable  $X$  is said to be discrete if and only if the set of possible values of  $X$  is finite or countably infinite.

## Then

If  $x_1, x_2, \dots$  are the values of  $X$  that belong to the range  $R$  of it,

$$P(X = x_1, X = x_2, \dots) = \sum_{x \in R} p_X(x)$$



# In the case of Continuous Random Variables

## Definition

A continuous random variable can assume a continuous range of values.

However, we would use something more formal for this

Using integrals.



# In the case of Continuous Random Variables

## Definition

A continuous random variable can assume a continuous range of values.

However, we would use something more formal for this

Using integrals.



# Examples

Random variable  $X$  has uniform  $U(a, b)$  distribution if its density is given by

$$f(x|a, b) = \begin{cases} \frac{1}{b-a} & a \leq x \leq b \\ 0 & \text{else} \end{cases}$$

For Example



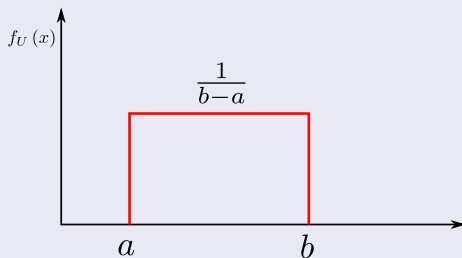
Cinvestav

# Examples

Random variable  $X$  has uniform  $U(a, b)$  distribution if its density is given by

$$f(x|a, b) = \begin{cases} \frac{1}{b-a} & a \leq x \leq b \\ 0 & \text{else} \end{cases}$$

For Example





# Example

## Bernoulli Distribution

Random variable  $X$  has Bernoulli  $\mathcal{B}er(p)$  distribution with parameter  $0 \leq p \leq 1$

if its probability mass function is given by

$$f(x|p) = p^x (1-p)^{1-x}, \quad x \in \{0, 1\}$$

What is the structure of the distribution?

Any idea?



## Example

### Bernoulli Distribution

Random variable  $X$  has Bernoulli  $\mathcal{Ber}(p)$  distribution with parameter  $0 \leq p \leq 1$

if its probability mass function is given by

$$f(x|p) = p^x (1-p)^{1-x}, \quad x \in \{0, 1\}$$

What is the structure of the distribution?

Any idea?



## Example

### Bernoulli Distribution

Random variable  $X$  has Bernoulli  $\mathcal{Ber}(p)$  distribution with parameter  $0 \leq p \leq 1$

if its probability mass function is given by

$$f(x|p) = p^x (1-p)^{1-x}, \quad x \in \{0, 1\}$$

What is the structure of the distribution

Any idea?



# Basic Properties

As you can imagine

They need to follow the rules of a probability.



Cinvestav

# Basic Properties

As you can imagine

They need to follow the rules of a probability.

The Probability sums to one

For the PMF and PDF

- $\sum_x f(x) = 1$
- $\int_{-\infty}^{\infty} f(x) dx = 1$



# Basic Properties

As you can imagine

They need to follow the rules of a probability.

The Probability sums to one

For the PMF and PDF

- $\sum_x f(x) = 1$

- $\int_{-\infty}^{\infty} f(x) dx = 1$



# Basic Properties

As you can imagine

They need to follow the rules of a probability.

The Probability sums to one

For the PMF and PDF

- $\sum_x f(x) = 1$
- $\int_{-\infty}^{\infty} f(x)dx = 1$



# The Probability

It can be “easily” calculated

- One of my ironies.

PMF

$$P_X(a < X < b) = \sum_{k=a}^b f_X(k).$$

PDF

$$P_X(a < X < b) = \int_a^b f_X(t) dt$$





# The Probability

It can be “easily” calculated

- One of my ironies.

PMF

$$F_X(a < X < b) = \sum_{k=a}^b f_X(k).$$

PDF

$$F_X(a < X < b) = \int_a^b f_X(t) dt$$



# The Probability

It can be “easily” calculated

- One of my ironies.

PMF

$$F_X(a < X < b) = \sum_{k=a}^b f_X(k).$$

PDF

$$F_X(a < X < b) = \int_a^b f_X(t)dt$$



## In the Continuous Case

We have

$$F_X(a < X < b) = F_X(b) - F_X(a)$$

Additionally, we have that for a single point

$$F_X(a < X < a) = F_X(a) - F_X(a) = 0$$



## In the Continuous Case

We have

$$F_X(a < X < b) = F_X(b) - F_X(a)$$

Additionally, we have that for a single point

$$F_X(a < X < a) = F_X(a) - F_X(a) = 0$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- **Distribution Functions**
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



## Now

We have some basic ideas about the descriptions of the Random Variables

We need to be more formal to connect our basic intuitions on continuous spaces.

## Now

### We have some basic ideas about the descriptions of the Random Variables

We need to be more formal to connect our basic intuitions on continuous spaces.

### Theorem

- Let  $f$  be a nonnegative real-valued function on  $\mathbb{R}$  with  $\int_{-\infty}^{\infty} f(x) dx = 1$ .
- There is a unique probability measure  $P$  defined in the Borel Subsets of  $\mathbb{R}$ .
- Such That

$$P(B) = \int_B f(x) dx$$

For all intervals  $B = (a, b]$

## Now

### We have some basic ideas about the descriptions of the Random Variables

We need to be more formal to connect our basic intuitions on continuous spaces.

### Theorem

- Let  $f$  be a nonnegative real-valued function on  $\mathbb{R}$  with  $\int_{-\infty}^{\infty} f(x) dx = 1$ .
- There is a unique probability measure  $P$  defined in the Borel Subsets of  $\mathbb{R}$ .
- Such That

$$P(B) = \int_B f(x) dx$$

For all intervals  $B = (a, b]$



## Now

### We have some basic ideas about the descriptions of the Random Variables

We need to be more formal to connect our basic intuitions on continuous spaces.

### Theorem

- Let  $f$  be a nonnegative real-valued function on  $\mathbb{R}$  with  $\int_{-\infty}^{\infty} f(x) dx = 1$ .
- There is a unique probability measure  $P$  defined in the Borel Subsets of  $\mathbb{R}$ .
- Such That

$$P(B) = \int_B f(x) dx$$

For all intervals  $B = (a, b]$

## Now

### We have some basic ideas about the descriptions of the Random Variables

We need to be more formal to connect our basic intuitions on continuous spaces.

### Theorem

- Let  $f$  be a nonnegative real-valued function on  $\mathbb{R}$  with  $\int_{-\infty}^{\infty} f(x) dx = 1$ .
- There is a unique probability measure  $P$  defined in the Borel Subsets of  $\mathbb{R}$ .
- Such That

$$P(B) = \int_B f(x) dx$$

For all intervals  $B = (a, b]$

# Therefore

## Definition

The random variable  $X$  is said to be absolutely continuous if and only if there is a non-negative function  $f = f_X$  defined over  $\mathbb{R}$  such that

$$F_X(x) = \int_{-\infty}^x f_X(t) dt$$

$f_X$  is called the Density function of  $X$  and  $F_X$  is called a Cumulative Density Function (CDF).



# Therefore

## Definition

The random variable  $X$  is said to be absolutely continuous if and only if there is a non-negative function  $f = f_X$  defined over  $\mathbb{R}$  such that

$$F_X(x) = \int_{-\infty}^x f_X(t) dt$$

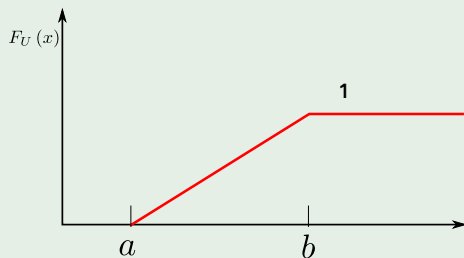
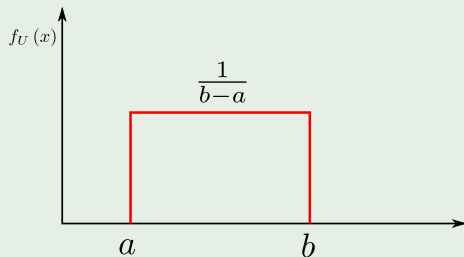
## Here

$f_X$  is called the Density function of  $X$  and  $F_X$  is called a Cumulative Density Function (CDF).



# Graphically

## Example uniform distribution



# Properties

## CDF's Properties

- $F_X(x) \geq 0$
- $F_X(x)$  is a non-decreasing function of  $X$ .

## Example

- If  $X$  is discrete, its CDF can be computed as follows:

$$F_X(x) = P(f(X) \leq x) = \sum_{k=1}^N P(X_k = p_k).$$



# Properties

## CDF's Properties

- $F_X(x) \geq 0$
- $F_X(x)$  is a non-decreasing function of  $X$ .

## Example

- If  $X$  is discrete, its CDF can be computed as follows:

$$F_X(x) = P(f(X) \leq x) = \sum_{k=1}^N P(X_k = p_k).$$



# Properties

## CDF's Properties

- $F_X(x) \geq 0$
- $F_X(x)$  in a non-decreasing function of  $X$ .

## Example

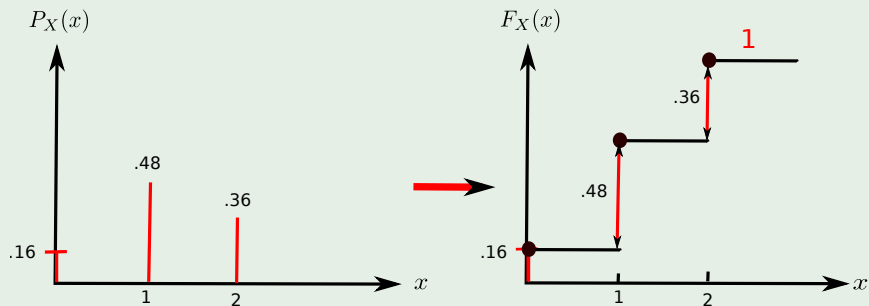
- If  $X$  is discrete, its CDF can be computed as follows:

$$F_X(x) = P(f(X) \leq x) = \sum_{k=1}^N P(X_k = p_k).$$





# Example on Discrete Function



# Derivative of Cumulative Density Function

## Continuous Function

If  $X$  is continuous, its CDF can be computed as follows:

$$F(x) = \int_{-\infty}^x f(t)dt.$$

### Remark:

Based in the fundamental theorem of calculus, we have the following equality.

$$f(x) = \frac{dF}{dx}(x)$$

### Note:

This particular  $p(x)$  is known as the Probability Distribution Function (PDF).

# Derivative of Cumulative Density Function

## Continuous Function

If  $X$  is continuous, its CDF can be computed as follows:

$$F(x) = \int_{-\infty}^x f(t)dt.$$

## Remark

Based in the fundamental theorem of calculus, we have the following equality.

$$f(x) = \frac{dF}{dx}(x)$$

## Note

This particular  $p(x)$  is known as the Probability Distribution Function (PDF).

# Derivative of Cumulative Density Function

## Continuous Function

If  $X$  is continuous, its CDF can be computed as follows:

$$F(x) = \int_{-\infty}^x f(t)dt.$$

## Remark

Based in the fundamental theorem of calculus, we have the following equality.

$$f(x) = \frac{dF}{dx}(x)$$

## Note

This particular  $p(x)$  is known as the Probability Distribution Function (PDF).

# Some Basic Properties of These Densities

## Conditional PMF/PDF

We have the conditional pdf:

$$p(y|x) = \frac{p(x, y)}{p(x)}.$$

From this, we have the general chain rule

$$p(x_1, x_2, \dots, x_n) = p(x_1|x_2, \dots, x_n)p(x_2|x_3, \dots, x_n)\dots p(x_n).$$

## Independence

If  $X$  and  $Y$  are independent, then:

$$p(x, y) = p(x)p(y).$$

# Some Basic Properties of These Densities

## Conditional PMF/PDF

We have the conditional pdf:

$$p(y|x) = \frac{p(x, y)}{p(x)}.$$

From this, we have the general chain rule

$$p(x_1, x_2, \dots, x_n) = p(x_1|x_2, \dots, x_n)p(x_2|x_3, \dots, x_n)\dots p(x_n).$$

## Independence

If X and Y are independent, then:

$$p(x, y) = p(x)p(y).$$

## Also the Law of Total Probability

Law of Total Probability is still working correctly

$$p(y) = \sum_x p(y|x)p(x).$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- **Function of Random Variables**
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance





# We have a common problem

Given a function  $g$

Describing a specific phenomena.

We can have a stochastic input

For example a Random Variable  $X_1$

Then, we have another random variable

$$X_2 = g(X_1)$$



# We have a common problem

Given a function  $g$

Describing a specific phenomena.

We can have a stochastic input

For example a Random Variable  $X_1$

Then we have another random variable

$$X_2 = g(X_1)$$



# We have a common problem

Given a function  $g$

Describing a specific phenomena.

We can have a stochastic input

For example a Random Variable  $X_1$

Then, we have another random variable

$$X_2 = g(X_1)$$



## Example

Let  $X_1$  a random variable such that  $X_2 = X_1^2$

What is the density function of  $X_2$ ?

For this, we need to express the event  $\{X_2 \leq y\}$

In terms of the random variable  $X_1$

Firstly, if  $y < 0$

Thus, we have that for  $y < 0$

$$F_2(y) = P(X_2 \leq y) = 0$$



## Example

Let  $X_1$  a random variable such that  $X_2 = X_1^2$

What is the density function of  $X_2$ ?

For this, we need to express the event  $\{X_2 \leq y\}$

In terms of the random variable  $X_1$

Firstly,

Thus, we have that for  $y < 0$

$$F_2(y) = P(X_2 \leq y) = 0$$



## Example

Let  $X_1$  a random variable such that  $X_2 = X_1^2$

What is the density function of  $X_2$ ?

For this, we need to express the event  $\{X_2 \leq y\}$

In terms of the random variable  $X_1$

First  $X_2 \geq 0$

Thus, we have that for  $y < 0$

$$F_2(y) = P(X_2 \leq y) = 0$$



Then

if  $y \geq 0$  then  $R_2 \leq y$

If and only if  $-\sqrt{y} \leq X_1 \leq \sqrt{y}$

Then

$$F(X_2 \leq y) = F(-\sqrt{y} \leq X_1 \leq \sqrt{y}) = \int_{-\sqrt{y}}^{\sqrt{y}} f_1(x) dx$$

If

$$f_1(x) = \begin{cases} 0 & \text{if } x < -1 \\ \frac{1}{2} & \text{if } -1 \leq x < 0 \\ \frac{1}{2} \exp\{-x\} & \text{if } 0 \leq x \end{cases}$$



Then

if  $y \geq 0$  then  $R_2 \leq y$

If and only if  $-\sqrt{y} \leq X_1 \leq \sqrt{y}$

Then

$$F(X_2 \leq y) = F(-\sqrt{y} \leq X_1 \leq \sqrt{y}) = \int_{-\sqrt{y}}^{\sqrt{y}} f_1(x) dx$$

$$f_1(x) = \begin{cases} 0 & \text{if } x < -1 \\ \frac{1}{2} & \text{if } -1 \leq x < 0 \\ \frac{1}{2} \exp\{-x\} & \text{if } 0 \leq x \end{cases}$$



Then

if  $y \geq 0$  then  $R_2 \leq y$

If and only if  $-\sqrt{y} \leq X_1 \leq \sqrt{y}$

Then

$$F(X_2 \leq y) = F(-\sqrt{y} \leq X_1 \leq \sqrt{y}) = \int_{-\sqrt{y}}^{\sqrt{y}} f_1(x) dx$$

If

$$f_1(x) = \begin{cases} 0 & \text{if } x < -1 \\ \frac{1}{2} & \text{if } -1 \leq x < 0 \\ \frac{1}{2} \exp\{-x\} & \text{if } 0 \leq x \end{cases}$$



We have then

if  $0 \leq y \leq 1$

$$F_2(y) = \int_{-\sqrt{y}}^{\sqrt{y}} f_1(x) dx$$

$$= \int_{-\sqrt{y}}^0 \frac{1}{2} dx + \int_0^{\sqrt{y}} \frac{1}{2} \exp\{-x\} dx$$

$$= \frac{1}{2} \sqrt{y} + \frac{1}{2} (1 - \exp\{-\sqrt{y}\})$$



We have then

if  $0 \leq y \leq 1$

$$\begin{aligned} F_2(y) &= \int_{-\sqrt{y}}^{\sqrt{y}} f_1(x) dx \\ &= \int_{-\sqrt{y}}^0 \frac{1}{2} dx + \int_0^{\sqrt{y}} \frac{1}{2} \exp\{-x\} dx \\ &= \frac{1}{2}\sqrt{y} + \frac{1}{2}(1 - \exp\{-\sqrt{y}\}) \end{aligned}$$

What is  $F_2(y)$ ?



We have then

if  $0 \leq y \leq 1$

$$\begin{aligned} F_2(y) &= \int_{-\sqrt{y}}^{\sqrt{y}} f_1(x) dx \\ &= \int_{-\sqrt{y}}^0 \frac{1}{2} dx + \int_0^{\sqrt{y}} \frac{1}{2} \exp\{-x\} dx \\ &= \frac{1}{2}\sqrt{y} + \frac{1}{2}(1 - \exp\{-\sqrt{y}\}) \end{aligned}$$

If  $y > 1$

What is  $F_2(y)$ ?



# Finally

For  $y < 0$

$$f_2(y) = \frac{dF_2(y)}{dy} = 0$$

For  $0 < y < 1$

$$f_2(y) = \frac{dF_2(y)}{dy} = \frac{1}{4\sqrt{y}} (1 + \exp\{-\sqrt{y}\})$$

For  $y > 1$

$$f_2(y) = \frac{dF_2(y)}{dy} = \frac{1}{4\sqrt{y}} \exp\{-\sqrt{y}\}$$



# Finally

For  $y < 0$

$$f_2(y) = \frac{dF_2(y)}{dy} = 0$$

For  $0 < y < 1$

$$f_2(y) = \frac{dF_2(y)}{dy} = \frac{1}{4\sqrt{y}} (1 + \exp\{-\sqrt{y}\})$$

For  $y > 1$

$$f_2(y) = \frac{dF_2(y)}{dy} = \frac{1}{4\sqrt{y}} \exp\{-\sqrt{y}\}$$



## Finally

For  $y < 0$

$$f_2(y) = \frac{dF_2(y)}{dy} = 0$$

For  $0 < y < 1$

$$f_2(y) = \frac{dF_2(y)}{dy} = \frac{1}{4\sqrt{y}} (1 + \exp\{-\sqrt{y}\})$$

For  $y > 1$

$$f_2(y) = \frac{dF_2(y)}{dy} = \frac{1}{4\sqrt{y}} \exp\{-\sqrt{y}\}$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- **Some Properties of the Distribution Functions**
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance





# The Situation Becomes Interesting

When you take into account two or more variables

Here, we have two random variables that are defined by a density function:

$$f_{X,Y}(x,y)$$

Therefore

We need to understand how these random variables interact.



# The Situation Becomes Interesting

When you take into account two or more variables

Here, we have two random variables that are defined by a density function:

$$f_{X,Y}(x, y)$$

Therefore

We need to understand how these random variables interact.



# Joint Distributions

Suppose we have a non-negative function real-valued function  $f$  in  $\mathbb{R}^2$

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) dx dy = 1$$

Now, if we define

$X_1(x, y)$  and  $X_2(x, y)$ , then

$$P((X_1, X_2) \in B) = P(B) = \int \int_B f(x, y) dx dy$$



# Joint Distributions

Suppose we have a non-negative function real-valued function  $f$  in  $\mathbb{R}^2$

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) dx dy = 1$$

Now, if we define

$X_1(x, y)$  and  $X_2(x, y)$ , then

$$P((X_1, X_2) \in B) = P(B) = \int \int_B f(x, y) dx dy$$



Therefore

The Joint Distribution Function is defined as

$$F(x, y) = \int_{-\infty}^x \int_{-\infty}^y f(u, v) \, du \, dv$$



## Example

Let

$$f(x, y) = \begin{cases} 1 & \text{if } 0 \leq x \leq 1 \text{ and } 0 \leq y \leq 1 \\ 0 & \text{elsewhere} \end{cases}$$

It looks like

The Unit Square in  $\mathbb{R}^2$



## Example

Let

$$f(x, y) = \begin{cases} 1 & \text{if } 0 \leq x \leq 1 \text{ and } 0 \leq y \leq 1 \\ 0 & \text{elsewhere} \end{cases}$$

It looks like

The Unit Square in  $\mathbb{R}^2$



Then

Assume the following random variables

$$X_1(x, y) = x \text{ and } X_2(x, y) = y.$$

Why don't we calculate the following probability? For

$$\frac{1}{2} \leq X_1 + X_2 \leq \frac{3}{2}$$

Therefore

$$\frac{1}{2} \leq x + y \leq \frac{3}{2}$$





Then

Assume the following random variables

$$X_1(x, y) = x \text{ and } X_2(x, y) = y.$$

Why don't we calculate the following probability? For

$$\frac{1}{2} \leq X_1 + X_2 \leq \frac{3}{2}$$

Therefore

$$\frac{1}{2} \leq x + y \leq \frac{3}{2}$$



Then

Assume the following random variables

$$X_1(x, y) = x \text{ and } X_2(x, y) = y.$$

Why don't we calculate the following probability? For

$$\frac{1}{2} \leq X_1 + X_2 \leq \frac{3}{2}$$

Therefore

$$\frac{1}{2} \leq x + y \leq \frac{3}{2}$$



# Look

We have the following

$$P \left\{ \frac{1}{2} \leq x + y \leq \frac{3}{2} \right\} = \int \int_B 1 dx dy$$

What is  $B$ ?

We can draw it!!!

Therefore

$$P \left\{ \frac{1}{2} \leq x + y \leq \frac{3}{2} \right\} = 1 - 2 \left( \frac{1}{8} \right)$$



# Look

We have the following

$$P \left\{ \frac{1}{2} \leq x + y \leq \frac{3}{2} \right\} = \int \int_B 1 dx dy$$

What is  $B$ ?

We can draw it!!!

Therefore

$$P \left\{ \frac{1}{2} \leq x + y \leq \frac{3}{2} \right\} = 1 - 2 \left( \frac{1}{8} \right)$$



# Look

We have the following

$$P \left\{ \frac{1}{2} \leq x + y \leq \frac{3}{2} \right\} = \int \int_B 1 dx dy$$

What is  $B$ ?

We can draw it!!!

Therefore

$$P \left\{ \frac{1}{2} \leq x + y \leq \frac{3}{2} \right\} = 1 - 2 \left( \frac{1}{8} \right)$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- **Some Properties of the Distribution Functions**
  - **Relations Between Joint and Individual Densities**

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# If we have a Joint Distribution

Can we get the Individual Distributions?

Actually, we have that we can integrate one of the variables.

For Example:

What if we have the following age-weight distributions

$X_1$ =Weight			
170-160	2	3	
160-150	4	5	
	20-25	25-30	$X_2$ =Age



# If we have a Joint Distribution

Can we get the Individual Distributions?

Actually, we have that we can integrate one of the variables.

For Example

What if we have the following age-weight distributions

$X_1$ =Weight			
170-160	<b>2</b>	<b>3</b>	
160-150	<b>4</b>	<b>5</b>	
	20-25	25-30	$X_2$ =Age





Therefore

## The Joint Distribution for two discrete variables

$$f(x, y) = P(X_1 = x, X_2 = y)$$

Then

$$\{X_1 = x\} = \{X_1 = x, X_2 = y_1\} \cup \{X_1 = x, X_2 = y_2\} \cup \dots$$

Remember

The events are independent!!!



Therefore

The Joint Distribution for two discrete variables

$$f(x, y) = P(X_1 = x, X_2 = y)$$

Then

$$\{X_1 = x\} = \{X_1 = x, X_2 = y_1\} \cup \{X_1 = x, X_2 = y_2\} \cup \dots$$

Remember

The events are independent!!!



Cinvestav

Therefore

The Joint Distribution for two discrete variables

$$f(x, y) = P(X_1 = x, X_2 = y)$$

Then

$$\{X_1 = x\} = \{X_1 = x, X_2 = y_1\} \cup \{X_1 = x, X_2 = y_2\} \cup \dots$$

Remember

The events are independent!!!



Therefore

We have the marginal distribution for  $X_1$

$$f_1(x) = P(X_1 = x) = \sum_y f(x, y)$$

Similarly

$$f_2(y) = P(X_2 = y) = \sum_x f(x, y)$$



Therefore

We have the marginal distribution for  $X_1$

$$f_1(x) = F(X_1 = x) = \sum_y f(x, y)$$

Similarly

$$f_2(y) = F(X_2 = y) = \sum_x f(x, y)$$



Therefore

We have

$$F(x_0 \leq X_1 \leq x_0 + dx_0) \approx f_1(x_0) dx_0$$

Basically



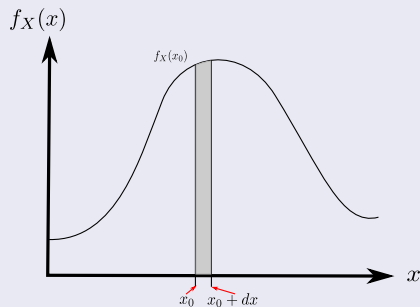
Cinvestav

Therefore

We have

$$F(x_0 \leq X_1 \leq x_0 + dx_0) \approx f_1(x_0) dx_0$$

Basically



Then

We have

$$\begin{aligned} F(x_0 \leq X_1 \leq x_0 + dx_0) &= F(x_0 \leq X_1 \leq x_0 + dx_0, -\infty < X_2 < \infty) \\ &= \int_{x_0}^{x_0+dx_0} dx \int_{-\infty}^{\infty} f(x, y) dy \\ &\approx dx_0 \int_{-\infty}^{\infty} f(x, y) dy \end{aligned}$$





Therefore

We have if  $f(x, y)$  is well behaved

$$f_1(x_0) dx_0 \approx dx_0 \int_{-\infty}^{\infty} f(x_0, y) dy$$

Then

$$f_1(x_0) \approx \int_{-\infty}^{\infty} f(x_0, y) dy$$



Therefore

We have if  $f(x, y)$  is well behaved

$$f_1(x_0) dx_0 \approx dx_0 \int_{-\infty}^{\infty} f(x_0, y) dy$$

Then

$$f_1(x_0) \approx \int_{-\infty}^{\infty} f(x_0, y) dy$$



In this way

We have

$$f_1(x) = \int_{-\infty}^{\infty} f(x, y) dy$$

Also

$$f_2(y) = \int_{-\infty}^{\infty} f(x, y) dx$$



In this way

We have

$$f_1(x) = \int_{-\infty}^{\infty} f(x, y) dy$$

Also

$$f_2(y) = \int_{-\infty}^{\infty} f(x, y) dx$$



## Example

Given

$$f(x, y) = \begin{cases} 8xy & 0 \leq y \leq x \leq 1 \\ 0 & \textit{elsewhere} \end{cases}$$

Then for  $0 \leq x \leq 1$

$$f_1(x) = \int_0^x 8xy dy = 4x^3$$

If  $y < 0$  or  $y > 1$

$$f_2(y) = 0$$



## Example

Given

$$f(x, y) = \begin{cases} 8xy & 0 \leq y \leq x \leq 1 \\ 0 & \textit{elsewhere} \end{cases}$$

Then for  $0 \leq x \leq 1$

$$f_1(x) = \int_0^x 8xy dy = 4x^3$$

If  $y > x$  or  $y < 0$

$$f_2(y) = 0$$



## Example

Given

$$f(x, y) = \begin{cases} 8xy & 0 \leq y \leq x \leq 1 \\ 0 & \textit{elsewhere} \end{cases}$$

Then for  $0 \leq x \leq 1$

$$f_1(x) = \int_0^x 8xy dy = 4x^3$$

If  $y < 0$  or  $y > 1$

$$f_2(y) = 0$$



Therefore

We have for  $0 \leq y \leq 1$

$$f_2(y) = \int_y^1 8xy dx = 4y(1 - y^2)$$





# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- **Introduction**
- Definition
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



# Expectation

## Imagine the following situation

You have the random variables  $R_1, R_2$  representing how long is a call and how much you pay for an international call

if  $0 \leq R_1 \leq 3(\text{minute})$   $R_2 = 10(\text{cents})$

if  $3 < R_1 \leq 6(\text{minute})$   $R_2 = 20(\text{cents})$

if  $6 < R_1 \leq 9(\text{minute})$   $R_2 = 30(\text{cents})$



# Expectation

## Imagine the following situation

You have the random variables  $R_1, R_2$  representing how long is a call and how much you pay for an international call

if  $0 \leq R_1 \leq 3(\text{minute})$   $R_2 = 10(\text{cents})$

if  $3 < R_1 \leq 6(\text{minute})$   $R_2 = 20(\text{cents})$

if  $6 < R_1 \leq 9(\text{minute})$   $R_2 = 30(\text{cents})$



Then

We have then the probabilities

$$P\{R_2 = 10\} = 0.6, P\{R_2 = 20\} = 0.25, P\{R_2 = 10\} = 0.15$$

If we observe  $N$  calls and  $N$  is very large

We can say that we have  $N \times 0.6$  calls and  $10 \times N \times 0.6$  the cost of those calls



Then

We have then the probabilities

$$P \{R_2 = 10\} = 0.6, P \{R_2 = 20\} = 0.25, P \{R_2 = 10\} = 0.15$$

If we observe  $N$  calls and  $N$  is very large

We can say that we have  $N \times 0.6$  calls and  $10 \times N \times 0.6$  the cost of those calls



# Expectation

## Similarly

- $\{R_2 = 20\} \implies 0.25N$  and total cost  $5N$
- $\{R_2 = 20\} \implies 0.15N$  and total cost  $4.5N$



# Expectation

## Similarly

- $\{R_2 = 20\} \implies 0.25N$  and total cost  $5N$
- $\{R_2 = 20\} \implies 0.15N$  and total cost  $4.5N$

We have then the probabilities

The total cost is  $6N + 5N + 4.5N = 15.5N$  or in average 15.5 cents per call



# Expectation

## Similarly

- $\{R_2 = 20\} \implies 0.25N$  and total cost  $5N$
- $\{R_2 = 20\} \implies 0.15N$  and total cost  $4.5N$

## We have then the probabilities

The total cost is  $6N + 5N + 4.5N = 15.5N$  or in average 15.5 cents per call





Then

The weighted average

$$\begin{aligned}\frac{10(0.6N) + 20(.25N) + 30(0.15N)}{N} &= 10(0.6) + 20(.25) + 30(0.15) \\ &= \sum_y yP\{R_2 = y\}\end{aligned}$$

Then

The Expected Value is a weighted average!!!



Cinvestav

Then

The weighted average

$$\begin{aligned}\frac{10(0.6N) + 20(.25N) + 30(0.15N)}{N} &= 10(0.6) + 20(.25) + 30(0.15) \\ &= \sum_y yP\{R_2 = y\}\end{aligned}$$

Then

The Expected Value is a weighted average!!!



# Then

John Cage

Assume

Given  $X$  a simple random variable i.e. a discrete random variable with a finite range!

We define the expectation of as

$$E(X) = \sum_x xP(X = x)$$

Given that you have a simple random variable

The sum is finite and there are not convergence problems.



Cinvestav

# Then

John Cage

Assume

Given  $X$  a simple random variable i.e. a discrete random variable with a finite range!

We define the expectation of as

$$E(X) = \sum_x xP(X = x)$$

Given that you have a simple random variable

The sum is finite and there are not convergence problems.



Cinvestav

# Then

John Cage

Assume

Given  $X$  a simple random variable i.e. a discrete random variable with a finite range!

We define the expectation of as

$$E(X) = \sum_x xP(X = x)$$

Given that you have a simple random variable

The sum is finite and there are not convergence problems.



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- **Definition**
- Properties
- Minimizing Distances
- Variance
- Definition of Variance



## Now

This expected function can be extended to random functions too

$$E(X_2) = E(g(X_1)) = \sum_x g(x) f_{X_1}(x)$$

In a similar way, it is possible to define for the continuous random variables

$$E(X_3) = \int_{-\infty}^{\infty} x f_{X_3}(x) dx$$

Similarly

$$E(g(X_3)) = \int_{-\infty}^{\infty} g(x) f_{X_3}(x) dx$$



Now

This expected function can be extended to random functions too

$$E(X_2) = E(g(X_1)) = \sum_x g(x) f_{X_1}(x)$$

In a similar way, it is possible to define for the continuous random variables

$$E(X_3) = \int_{-\infty}^{\infty} x f_{X_3}(x) dx$$

Similarly

$$E(g(X_3)) = \int_{-\infty}^{\infty} g(x) f_{X_3}(x) dx$$



Now

This expected function can be extended to random functions too

$$E(X_2) = E(g(X_1)) = \sum_x g(x) f_{X_1}(x)$$

In a similar way, it is possible to define for the continuous random variables

$$E(X_3) = \int_{-\infty}^{\infty} x f_{X_3}(x) dx$$

Similarly

$$E(g(X_3)) = \int_{-\infty}^{\infty} g(x) f_{X_3}(x) dx$$



## Example

### Normal Density Function

$$f_X(x) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{x^2}{2}\right\}$$

Then

$$E[X] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x \exp\left\{-\frac{x^2}{2}\right\} dx$$

Then

$$E[X] = -\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} d\left\{-\frac{x^2}{2}\right\}$$

## Example

### Normal Density Function

$$f_X(x) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{x^2}{2}\right\}$$

Then

$$E[X] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x \exp\left\{-\frac{x^2}{2}\right\} dx$$

Then

$$E[X] = -\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} d\left\{-\frac{x^2}{2}\right\}$$

## Example

### Normal Density Function

$$f_X(x) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{x^2}{2}\right\}$$

Then

$$E[X] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x \exp\left\{-\frac{x^2}{2}\right\} dx$$

Then

$$E[X] = -\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} d\left\{-\frac{x^2}{2}\right\}$$

# Finally

We have

$$E[X] = -\frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{x^2}{2}\right\} \Bigg|_{-\infty}^{\infty} = 0$$



# Example

Imagine the following

We have the following functions

●  $f(x) = e^{-x}, x \geq 0$

●  $g(x) = 0, x < 0$



# Example

Imagine the following

We have the following functions

$f(x) = e^{-x}, x \geq 0$

$g(x) = 0, x < 0$

Find

The expected Value



# Example

Imagine the following

We have the following functions

①  $f(x) = e^{-x}, x \geq 0$

②  $g(x) = 0, x < 0$

Find

The expected Value





# Example

Imagine the following

We have the following functions

①  $f(x) = e^{-x}, x \geq 0$

②  $g(x) = 0, x < 0$

Find

The expected Value



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- **Properties**
- Minimizing Distances
- Variance
- Definition of Variance



Then

Given a random variable  $X$ , and  $a, b, c$  constants

Then, for any functions  $g_1(x)$  and  $g_2(x)$  whose expectation exists

- ①  $E[ag_1(x) + bg_2(x) + c] = aE[g_1(x)] + bE[g_2(x)] + c$
- ② If  $g_1(x) \geq 0$  for all  $x$ , then  $E[g_1(x)] \geq 0$
- ③ If  $g_1(x) \geq g_2(x)$  for all  $x$ , then  $E[g_1(x)] \geq E[g_2(x)]$
- ④ If  $a \leq g_1(x) \leq b$  for all  $x$ , then  $a \leq E[g_1(x)] \leq b$



Then

Given a random variable  $X$ , and  $a, b, c$  constants

Then, for any functions  $g_1(x)$  and  $g_2(x)$  whose expectation exists

①  $E[ag_1(x) + bg_2(x) + c] = aE[g_1(x)] + bE[g_2(x)] + c$

② If  $g_1(x) \geq 0$  for all  $x$ , then  $E[g_1(x)] \geq 0$

③ If  $g_1(x) \geq g_2(x)$  for all  $x$ , then  $E[g_1(x)] \geq E[g_2(x)]$

④ If  $a \leq g_1(x) \leq b$  for all  $x$ , then  $a \leq E[g_1(x)] \leq b$



Then

Given a random variable  $X$ , and  $a, b, c$  constants

Then, for any functions  $g_1(x)$  and  $g_2(x)$  whose expectation exists

- 1  $E[ag_1(x) + bg_2(x) + c] = aE[g_1(x)] + bE[g_2(x)] + c$
- 2 If  $g_1(x) \geq 0$  for all  $x$ , then  $E[g_1(x)] \geq 0$
- 3 If  $g_1(x) \geq g_2(x)$  for all  $x$ , then  $E[g_1(x)] \geq E[g_2(x)]$
- 4 If  $a \leq g_1(x) \leq b$  for all  $x$ , then  $a \leq E[g_1(x)] \leq b$



Then

Given a random variable  $X$ , and  $a, b, c$  constants

Then, for any functions  $g_1(x)$  and  $g_2(x)$  whose expectation exists

- 1  $E[ag_1(x) + bg_2(x) + c] = aE[g_1(x)] + bE[g_2(x)] + c$
- 2 If  $g_1(x) \geq 0$  for all  $x$ , then  $E[g_1(x)] \geq 0$
- 3 If  $g_1(x) \geq g_2(x)$  for all  $x$ , then  $E[g_1(x)] \geq E[g_2(x)]$
- 4 If  $a \leq g_1(x) \leq b$  for all  $x$ , then  $a \leq E[g_1(x)] \leq b$



Then

Given a random variable  $X$ , and  $a, b, c$  constants

Then, for any functions  $g_1(x)$  and  $g_2(x)$  whose expectation exists

- 1  $E[ag_1(x) + bg_2(x) + c] = aE[g_1(x)] + bE[g_2(x)] + c$
- 2 If  $g_1(x) \geq 0$  for all  $x$ , then  $E[g_1(x)] \geq 0$
- 3 If  $g_1(x) \geq g_2(x)$  for all  $x$ , then  $E[g_1(x)] \geq E[g_2(x)]$
- 4 If  $a \leq g_1(x) \leq b$  for all  $x$ , then  $a \leq E[g_1(x)] \leq b$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- **Minimizing Distances**
- Variance
- Definition of Variance





# Minimizing Distances

## Observation

The expected value of a Random Variable has an important property!!!

### One can see that

The interpretation of  $E[X]$  as a good guess for  $X$

### Suppose the following

We measure the distance between a random variable  $X$  and a constant  $b$  by  $(X - b)^2$

- The closer the  $b$  is to  $X$ , the smaller the quantity is!!!



# Minimizing Distances

## Observation

The expected value of a Random Variable has an important property!!!

## One can be seen as

The interpretation of  $E[X]$  as a good guess for  $X$

Suppose the following:

We measure the distance between a random variable  $X$  and a constant  $b$  by  $(X - b)^2$

- The closer the  $b$  is to  $X$ , the smaller the quantity is!!!



# Minimizing Distances

## Observation

The expected value of a Random Variable has an important property!!!

## One can be seen as

The interpretation of  $E[X]$  as a good guess for  $X$

## Suppose the following

We measure the distance between a random variable  $X$  and a constant  $b$  by  $(X - b)^2$

- The closer the  $b$  is to  $X$ , the smaller the quantity is!!!



Then

We can then determine the value of  $b$

$$\begin{aligned} E(X - b)^2 &= E(X - EX + EX - b)^2 \\ &= E((X - EX) + (EX - b))^2 \\ &= E(X - EX)^2 + (EX - b)^2 + \dots \\ &= 2E((X - EX)(EX - b)) \end{aligned}$$



Then

We can then determine the value of  $b$

$$\begin{aligned} E(X - b)^2 &= E(X - EX + EX - b)^2 \\ &= E((X - EX) + (EX - b))^2 \\ &= E(X - EX)^2 + (EX - b)^2 + \dots \\ &= 2E((X - EX)(EX - b)) \end{aligned}$$



Then

We can then determine the value of  $b$

$$\begin{aligned} E(X - b)^2 &= E(X - EX + EX - b)^2 \\ &= E((X - EX) + (EX - b))^2 \\ &= E(X - EX)^2 + (EX - b)^2 + \dots \\ &= 2E((X - EX)(EX - b)) \end{aligned}$$



Then

We can then determine the value of  $b$

$$\begin{aligned} E(X - b)^2 &= E(X - EX + EX - b)^2 \\ &= E((X - EX) + (EX - b))^2 \\ &= E(X - EX)^2 + (EX - b)^2 + \dots \\ &= 2E((X - EX)(EX - b)) \end{aligned}$$



We notice the following

We have

$$E((X - EX)(EX - b)) = (EX - b)E(X - EX) = 0$$

Then

$$E(X - b)^2 = E(X - EX)^2 + (EX - b)^2$$

What if we choose  $b = EX$ ?

$$\min_b E(X - b)^2 = E(X - EX)^2$$





We notice the following

We have

$$E((X - EX)(EX - b)) = (EX - b)E(X - EX) = 0$$

Then

$$E(X - b)^2 = E(X - EX)^2 + (EX - b)^2$$

What if we choose  $b = EX$ ?

$$\min_b E(X - b)^2 = E(X - EX)^2$$



We notice the following

We have

$$E((X - EX)(EX - b)) = (EX - b)E(X - EX) = 0$$

Then

$$E(X - b)^2 = E(X - EX)^2 + (EX - b)^2$$

What if we choose  $b = EX$

$$\min_b E(X - b)^2 = E(X - EX)^2$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- **Variance**
- Definition of Variance



# First, the central moments

## Definition

For each integer  $n$ , the  $n^{\text{th}}$  moment of  $X$ ,  $m_n$ , is

$$m_n = E[X^n]$$

The  $n^{\text{th}}$  central moment of  $X$  is

$$\mu_n = E[(X - \mu)^n]$$

where

$$\mu = \mu_n = EX$$



# First, the central moments

## Definition

For each integer  $n$ , the  $n^{\text{th}}$  moment of  $X$ ,  $m_n$ , is

$$m_n = E[X^n]$$

The  $n^{\text{th}}$  central moment of  $X$  is

$$\mu_n = E[X - \mu]^n$$

where

$$\mu = \mu_n = EX$$



# First, the central moments

## Definition

For each integer  $n$ , the  $n^{\text{th}}$  moment of  $X$ ,  $m_n$ , is

$$m_n = E[X^n]$$

The  $n^{\text{th}}$  central moment of  $X$  is

$$\mu_n = E[X - \mu]^n$$

Where

$$\mu = \mu_n = EX$$



# Outline

## 1 Basic Theory

- Intuitive Formulation
  - Famous Examples
- Axioms
- Using Set Operations
  - Example
- Finite and Infinite Space
- Counting, Frequentist Approach
- Independence
- Repeated Trials
  - Cartesian Products
- Unconditional and Conditional Probability
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes Theorem
- Application in Universal Hashing

## 2 Random Variables

- Introduction
- Formal Definition
- Probability of a Random Variable
- Types of Random Variables
- Distribution Functions
- Function of Random Variables
- Some Properties of the Distribution Functions
  - Relations Between Joint and Individual Densities

## 3 Expected Value

- Introduction
- Definition
- Properties
- Minimizing Distances
- Variance
- **Definition of Variance**



Then

### Definition

The Variance of a Random Variable  $X$  is its second central moment

$$\text{Var } X = E[X - EX]^2$$

Then

- The standard deviation is simply  $\sigma = \sqrt{\text{Var}(X)}$ .



Cinvestav



Then

### Definition

The Variance of a Random Variable  $X$  is its second central moment

$$\text{Var } X = E[X - EX]^2$$

Then

- The standard deviation is simply  $\sigma = \sqrt{\text{Var}(X)}$ .



# Now

The variance gives a measure of the degree of spread around its mean

Then, we have two cases

A large variance

In such case  $X$  is more variable

At the extreme

- If  $Var X = E(X - EX)^2 = 0$ , then  $X = EX$  with probability 1.
  - ▶ No Variation!!!



# Now

The variance gives a measure of the degree of spread around its mean

Then, we have two cases

A large variance

In such case  $X$  is more variable

At the extreme

- If  $Var X = E(X - EX)^2 = 0$ , then  $X = EX$  with probability 1.
  - ▶ No Variation!!!



# Now

The variance gives a measure of the degree of spread around its mean

Then, we have two cases

A large variance

In such case  $X$  is more variable

At the extreme

- If  $Var X = E(X - EX)^2 = 0$ , then  $X = EX$  with probability 1.
  - ▶ No Variation!!!



# Example

## Exponential Variance

Let  $X$  have the exponential( $\lambda$ ) distribution.

We know that  $E[X] = 1/\lambda$ .



## Example

### Exponential Variance

Let  $X$  have the exponential( $\lambda$ ) distribution.

We know that  $EX = \lambda$

$$\begin{aligned} \text{Var } X &= E(X - \lambda)^2 \\ &= \int_0^{\infty} (x - \lambda)^2 \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx \\ &= \int_0^{\infty} (x^2 - 2x\lambda + \lambda^2) \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx \end{aligned}$$



# Example

## Exponential Variance

Let  $X$  have the exponential( $\lambda$ ) distribution.

We know that  $EX = \lambda$

$$\text{Var } X = E(X - \lambda)^2$$

$$= \int_0^{\infty} (x - \lambda)^2 \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx$$

$$= \int_0^{\infty} (x^2 - 2x\lambda + \lambda^2) \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx$$



# Example

## Exponential Variance

Let  $X$  have the exponential( $\lambda$ ) distribution.

We know that  $EX = \lambda$

$$\begin{aligned} \text{Var } X &= E(X - \lambda)^2 \\ &= \int_0^{\infty} (x - \lambda)^2 \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx \\ &= \int_0^{\infty} (x^2 - 2x\lambda + \lambda^2) \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx \end{aligned}$$





# Example

## Exponential Variance

Let  $X$  have the exponential( $\lambda$ ) distribution.

We know that  $EX = \lambda$

$$\begin{aligned} \text{Var } X &= E(X - \lambda)^2 \\ &= \int_0^{\infty} (x - \lambda)^2 \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx \\ &= \int_0^{\infty} (x^2 - 2x\lambda + \lambda^2) \frac{1}{\lambda} \exp\left\{-\frac{x}{\lambda}\right\} dx \end{aligned}$$



## Further

We can use integration by parts to find the variance

$$\int u dv = uv - \int v du$$

Please try to calculate it

Answer:  $\text{Var } X = \lambda^2$



## Further

We can use integration by parts to find the variance

$$\int u dv = uv - \int v du$$

Please, try to calculate it

Answer:  $\text{Var } X = \lambda^2$



# About the Possible Linearity

We have

If  $X$  is a random variable with finite variance, then for any constants  $a$  and  $b$

$$\text{Var} (aX + b) = a^2 \text{Var} X$$

Alternative formula for the variance

$$\text{Var} X = EX^2 - (EX)^2$$

Work

At the White Board



Cinvestav

# About the Possible Linearity

We have

If  $X$  is a random variable with finite variance, then for any constants  $a$  and  $b$

$$\text{Var} (aX + b) = a^2 \text{Var} X$$

Alternative formula for the variance

$$\text{Var} X = EX^2 - (EX)^2$$

Whiteboard

At the White Board



Cinvestav

# About the Possible Linearity

## We have

If  $X$  is a random variable with finite variance, then for any constants  $a$  and  $b$

$$\text{Var} (aX + b) = a^2 \text{Var} X$$

## Alternative formula for the variance

$$\text{Var} X = EX^2 - (EX)^2$$

## Proof

At the White Board

