# Why is the Probability Space a Triple?

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

January 15, 2014

# Probability Space

## Definition

A probability space is a triple $(\Omega, \mathcal{F}, P)$ consisting of

- a set $\Omega$,
- a $\sigma$-field $\mathcal{F}$ of subsets of $\Omega$ and
- a probability measure $P$ on $(\Omega, \mathcal{F})$.

## Remarks

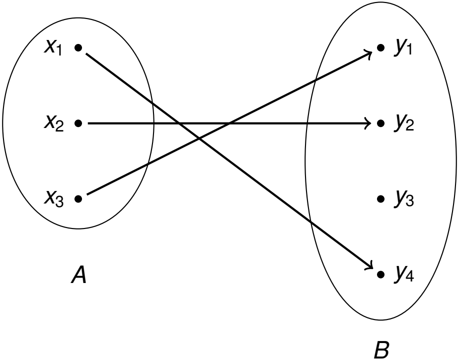
- When $\Omega$ is finite or countable, $\mathcal{F}$ can be $2^\Omega$ (all subsets can be events)
- If this always holds, then $\Omega$ uniquely specifies $\mathcal{F}$
- Then the probability space would be an ordered pair $(\Omega, P)$
- For uncountable $\Omega$, it may be impossible to define $P$ if $\mathcal{F} = 2^\Omega$
- We will see an example but first we need the following definitions
  - Countable and uncountable sets
  - Equivalence relations

# Countable and Uncountable Sets

# One-to-One Functions

## Definition (One-to-One function)

A function $f : A \to B$ is said to be a one-to-one mapping of $A$ into $B$ if $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$ and $x_1, x_2 \in A$.

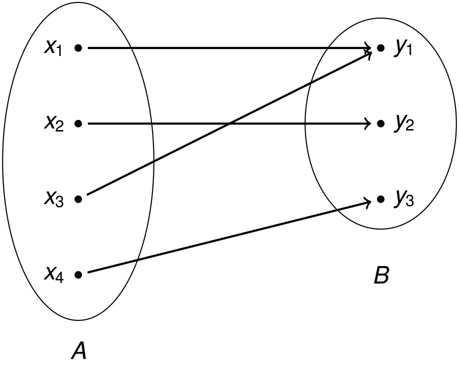



Also called an injective function

# Onto Functions

## Definition (Onto function)

A function $f : A \to B$ is said to be mapping $A$ onto $B$ if $f(A) = B$.

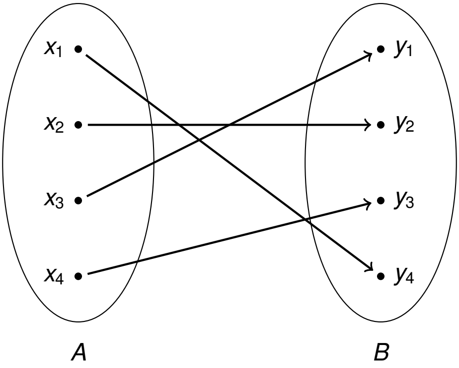



Also called a surjective function

# One-to-One Correspondence

## Definition (One-to-one correspondence)

A function $f : A \to B$ is said to be a one-to-one correspondence if it is a one-to-one and onto mapping from $A$ to $B$.




Also called a bijective function

# Countable Sets

## Definition

Sets $A$ and $B$ are said to have the same cardinal number if there exists a one-to-one correspondence $f : A \to B$.

## Definition (Countable Sets)

A set $A$ is said to be countable if there exists a one-to-one correspondence between $A$ and $\mathbb{N}$.

## Examples

- $\mathbb{N}$ is countable. Consider $f : \mathbb{N} \to \mathbb{N}$ defined as

$$f(x) = x$$

- $\mathbb{Z}$ is countable. Consider $f : \mathbb{Z} \to \mathbb{N}$ defined as

$$f(x) = \begin{cases} 2x + 1 & \text{if } x \geq 0 \\ -2x & \text{if } x < 0 \end{cases}$$

# More Examples of Countable Sets

$$
\begin{tikzcd}
(1,1) \arrow[r] & (2,1) \arrow[dl] & (3,1) \arrow[r] & (4,1) \arrow[dl] & (5,1) & \cdots \\
(1,2) \arrow[d] & (2,2) \arrow[ur] & (3,2) \arrow[dl] & (4,2) \arrow[ur] & (5,2) & \cdots \\
(1,3) \arrow[ur] & (2,3) \arrow[dl] & (3,3) \arrow[ur] & (4,3) & (5,3) & \cdots \\
(1,4) \arrow[d] & (2,4) \arrow[ur] & (3,4) & (4,4) & (5,4) & \cdots \\
(1,5) \arrow[ur] & (2,5) & (3,5) & (4,5) & (5,5) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{tikzcd}
$$

- Consider the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where $f(i, j)$ is equal to the number of pairs visited when $(i, j)$ is visited
- $\mathbb{N} \times \mathbb{N}$ is countable
- The same argument applies to any $A \times B$ where $A$ and $B$ are countable
- $\mathbb{Z} \times \mathbb{N}$ is countable $\implies$ $\mathbb{Q}$ is countable

# Reals are Uncountable

## Definition (Uncountable Sets)

A set is said to be uncountable if it is neither finite nor countable.

## Examples

- $[0, 1)$ is uncountable
- $\mathbb{R}$ is uncountable

# Equivalence Relations

# Binary Relations

## Definition (Binary Relation)

Given a set $X$, a binary relation $R$ is a subset of $X \times X$.

## Examples

- $X = \{1, 2, 3, 4\}, R = \{(1, 1), (2, 4)\}$
- $R = \left\{ (a, b) \in \mathbb{Z} \times \mathbb{Z} \,\middle|\, a - b \text{ is an even integer} \right\}$
- $R = \left\{ (A, B) \in 2^{\mathbb{N}} \times 2^{\mathbb{N}} \,\middle|\, \text{A bijection exists between } A \text{ and } B \right\}$

If $(a, b) \in R$, we write $a \sim_R b$ or just $a \sim b$.

# Equivalence Relations

## Definition (Equivalence Relation)

A binary relation $R$ on a set $X$ is said to be an equivalence relation on $X$ if for all $a, b, c \in X$ the following conditions hold

| | |
|---|---|
| Reflexive | $a \sim a$ |
| Symmetric | $a \sim b$ implies $b \sim a$ |
| Transitive | $a \sim b$ and $b \sim c$ imply $a \sim c$ |

## Examples

- $X = \{1, 2, 3, 4\}$, $R = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$
- $R = \left\{ (a, b) \in \mathbb{Z} \times \mathbb{Z} \middle| a - b \text{ is an even integer} \right\}$
- $R = \left\{ (a, b) \in \mathbb{Z} \times \mathbb{Z} \middle| a - b \text{ is a multiple of } 5 \right\}$
- Let $A$ be the set of people in the world. Are the following binary relations equivalence relations on $A$?
    - $a \sim b$ if $a$ and $b$ are friends
    - $a \sim b$ if $a$ and $b$ have an ancestor in common

# Equivalence Classes

## Definition (Equivalence Class)

Given an equivalence relation $R$ on $X$ and an element $x \in X$, the equivalence class of $x$ is the set of all $y \in X$ such that $x \sim y$.

## Examples

- $X = \{1, 2, 3, 4\}, R = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$
  Equivalence class of 1 is $\{1\}$.
- $R = \left\{ (a, b) \in \mathbb{Z} \times \mathbb{Z} \middle| a - b \text{ is an even integer} \right\}$
  Equivalence class of 0 is the set of all even integers.
  Equivalence class of 1 is the set of all odd integers.
- $R = \left\{ (a, b) \in \mathbb{Z} \times \mathbb{Z} \middle| a - b \text{ is a multiple of } 5 \right\}$. Equivalence classes?

## Theorem

*Given an equivalence relation, the collection of equivalence classes form a partition of $X$.*

# A Non-Measurable Set

# Choosing a Random Point in the Unit Interval

- Let $\Omega = [0, 1]$
- For $0 \le a \le b \le 1$, we want
$$P([a, b]) = P((a, b]) = P([a, b)) = P((a, b)) = b - a$$
- We want $P$ to be unaffected by shifting (with wrap-around)
$$P([0, 0.5]) = P([0.25, 0.75]) = P([0.75, 1] \cup [0, 0.25])$$
- In general, for each subset $A \subseteq [0, 1]$ and $0 \le r \le 1$
$$P(A \oplus r) = P(A)$$
where
$$A \oplus r = \{a + r | a \in A, a + r \le 1\} \cup \{a + r - 1 | a \in A, a + r > 1\}$$
- We want $P$ to be countably additive
$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$$
for disjoint subsets $A_1, A_2, \ldots$ of $[0, 1]$
- Can the definition of $P$ be extended to all subsets of $[0, 1]$?

# Building the Contradiction

- Suppose $P$ is defined for all subsets of $[0, 1]$
- Define an equivalence relation on $[0, 1]$ given by

$$x \sim y \iff x - y \text{ is rational}$$

- This relation partitions $[0, 1]$ into disjoint equivalence classes
- Let $H$ be a subset of $[0, 1]$ consisting of exactly one element from each equivalence class. Let $0 \in H$; then $1 \notin H$.
- $[0, 1)$ is contained in the union $\bigcup_{r \in [0,1) \cap \mathbb{Q}} (H \oplus r)$
- Since the sets $H \oplus r$ for $r \in [0, 1) \cap \mathbb{Q}$ are disjoint, by countable additivity

$$P([0, 1)) = \sum_{r \in [0,1) \cap \mathbb{Q}} P(H \oplus r)$$

- Shift invariance implies $P(H \oplus r) = P(H)$ which implies

$$1 = P([0, 1)) = \sum_{r \in [0,1) \cap \mathbb{Q}} P(H)$$

which is a contradiction

# Consequences of the Contradiction

- $P$ cannot be defined on all subsets of $[0, 1]$
- But the subsets it is defined on have to form a $\sigma$-field
- The $\sigma$-field of subsets of $[0, 1]$ on which $P$ can be defined without contradiction are called the measurable subsets
- That is why probability spaces are triples

Questions?