

Lecture 3: Random Variables

Wen Dingzhu

School of Information Science and Technology (SIST)
ShanghaiTech University

wendzh@shanghaitech.edu.cn

February 27, 2023



上海科技大学
ShanghaiTech University

Overview

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

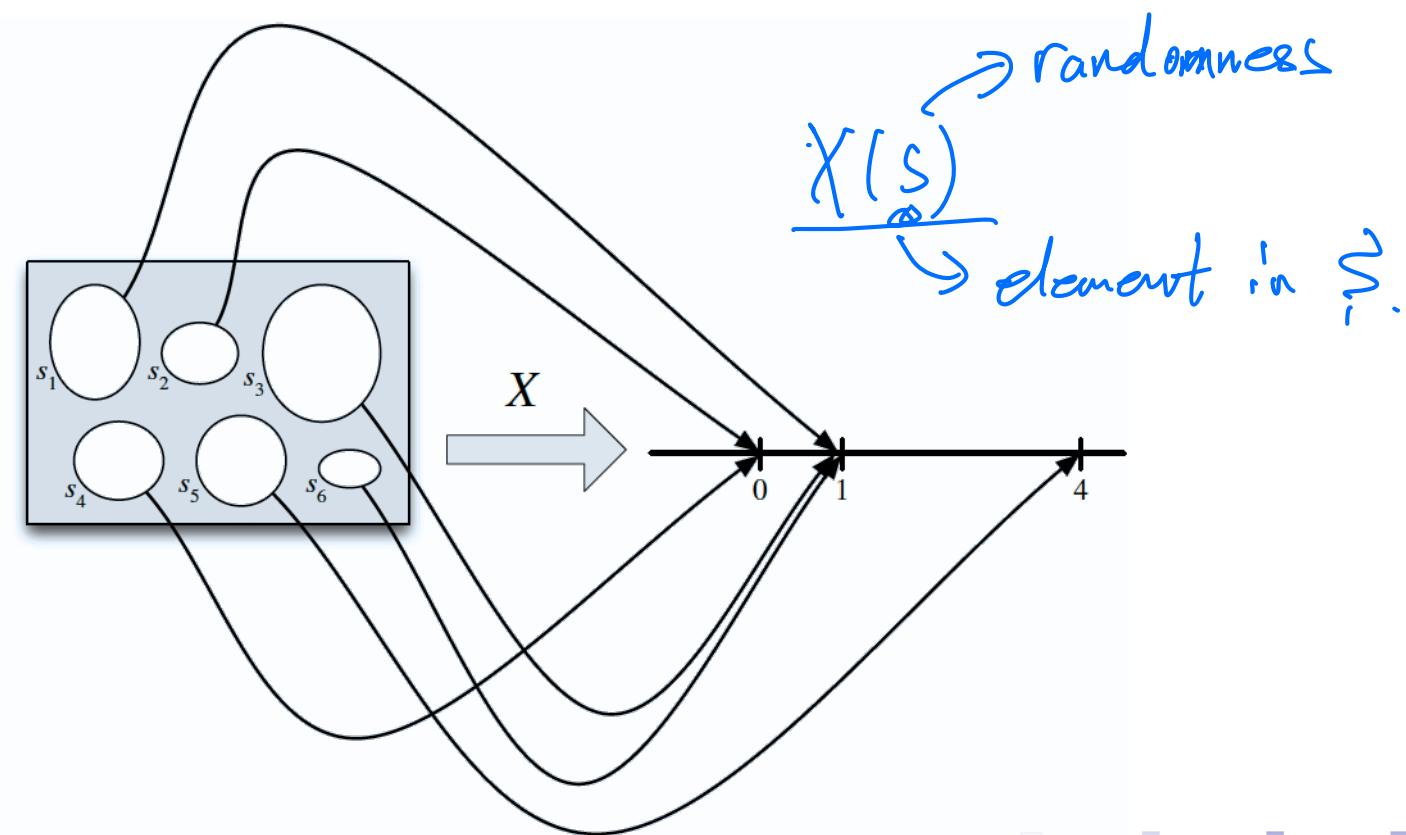
Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Definition of Random Variables

Definition

Given an experiment with sample space S , a *random variable* (r.v.) is a function from the sample space S to the real numbers R . It is common, but not required, to denote random variables by capital letters.



Example: Coin Tosses

Consider an experiment where we toss a fair coin twice. The sample space consists of four possible outcomes: $S = \{HH, HT, TH, TT\}$. Here are some random variables on this space (for practice, you can think up some of your own). Each r.v. is a numerical summary of some aspect of the experiment.

$$X \in \{0, 1, 2\}.$$

- X : the number of Heads. $X(HH) = 2$, $X(HT) = 1$, $X(TH) = 1$, $X(TT) = 0$.
- Y : the number of Tails. $Y(S) = 2 - X(S)$. $S \in S$.
- I : equals 1 if the first toss lands Heads and 0 otherwise.

$$I(HH) = I(HT) = 1, \quad I(TH) = I(TT) = 0.$$

Discrete Random Variable

Definition

A random variable X is said to be *discrete* if there is a finite list of values a_1, a_2, \dots, a_n or an infinite list of values a_1, a_2, \dots such that

$\sum_j P(X = a_j \text{ for some } j) = 1$. If X is a discrete r.v., then the finite or countably infinite set of values x such that $P(X = x) > 0$ is called the support of X .

Probability Mass Function

$$P_X(x) = P(X=x) = P(\{s | X(s)=x\}) .$$

Definition

The probability mass function (PMF) of a discrete r.v. X is the function p_X given by $p_X(x) = P(X = x)$. Note that this is positive if x is in the support of X , and 0 otherwise.

Example: Coin Tosses

$$X=2 \Leftrightarrow S=HH. P(X=2) = \frac{1}{4} = \underline{P_X(2)}$$

$$X=0, \Leftrightarrow S=TT \quad P(X=0) = \frac{1}{4} = \underline{P_X(0)}$$

$$X=1, \Leftrightarrow S=HT \text{ or } S=TH. \quad P(X=1) = \frac{1}{2} = \underline{P_X(1)}$$

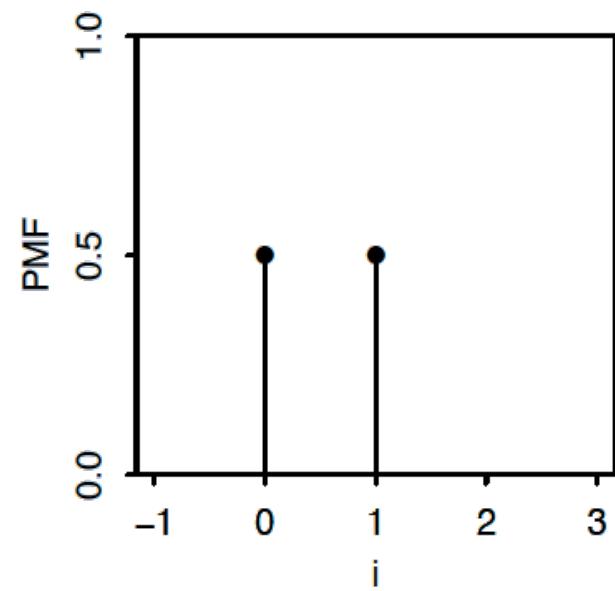
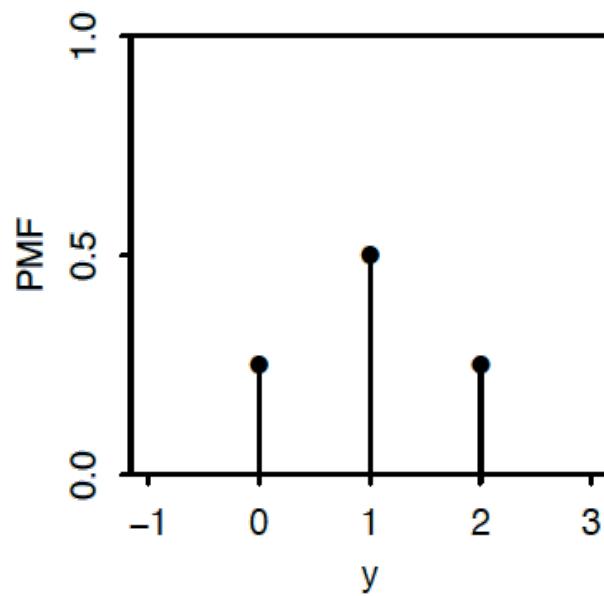
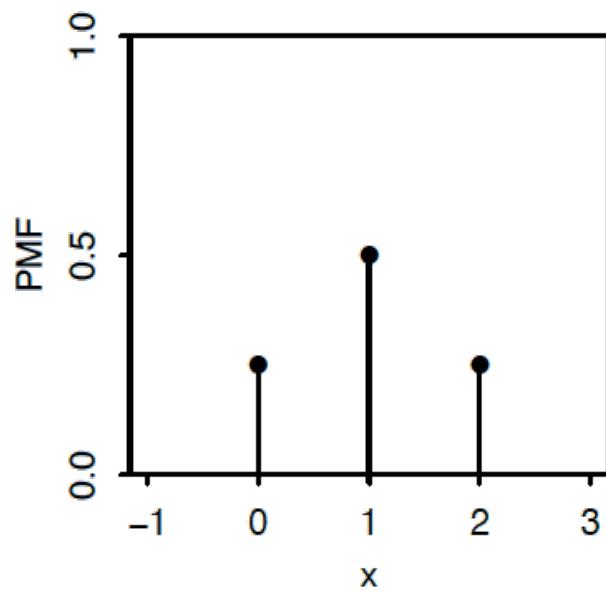
Consider an experiment where we toss a fair coin twice. The sample space consists of four possible outcomes: $\underline{S} = \{HH, HT, TH, TT\}$. Here are some random variables on this space (for practice, you can think up some of your own). Each r.v. is a numerical summary of some aspect of the experiment.

- X : the number of Heads.
- Y : the number of Tails. $Y = 2 - X$.
- I : equals 1 if the first toss lands Heads and 0 otherwise.

$$P_I(0) = P(I=0) = P(\{TH, TT\}) = \frac{1}{2}.$$

$$P_I(1) = P(I=1) = P(\{HH, HT\}) = \frac{1}{2}.$$

Example: Coin Tosses



Valid PMFs

Theorem

Let X be a discrete r.v. with support x_1, x_2, \dots (assume these values are distinct and, for notational simplicity, that the support is countably infinite; the analogous results hold if the support is finite). The PMF p_X of X must satisfy the following two criteria:

- Nonnegative: $p_X(x) > 0$ if $x = x_j$ for some j , and $p_X(x) = 0$ otherwise;
- Sums to 1: $\sum_{j=1}^{\infty} p_X(x_j) = 1$.

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Bernoulli Distribution

Definition

An r.v. X is said to have the Bernoulli distribution with parameter p if $P(X = 1) = p$ and $P(X = 0) = 1 - p$, where $0 < p < 1$. We write this as $X \sim \text{Bern}(p)$. The symbol \sim is read “is distributed as”.

Indicator Random Variable

Definition

The *indicator random variable* of an event A is the r.v. which equals 1 if A occurs and 0 otherwise. We will denote the indicator r.v. of A by I_A or $I(A)$. Note that $I_A \sim \text{Bern}(p)$ with $p = P(A)$.

Story: Bernoulli Trial

An experiment that can result in either a “success” or a “failure” (but not both) is called a *Bernoulli trial*. A Bernoulli random variable can be thought of as the *indicator of success* in a Bernoulli trial: it equals 1 if success occurs and 0 if failure occurs in the trial.

Story: Binomial Distribution

Suppose that n independent Bernoulli trials are performed, each with the same success probability p . Let X be the number of successes. The distribution of X is called the Binomial distribution with parameters n and p . We write $\underline{X} \sim \text{Bin}(n, p)$ to mean that X has the Binomial distribution with parameters n and p , where n is a positive integer and $0 < p < 1$.

$$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Binomial PMF

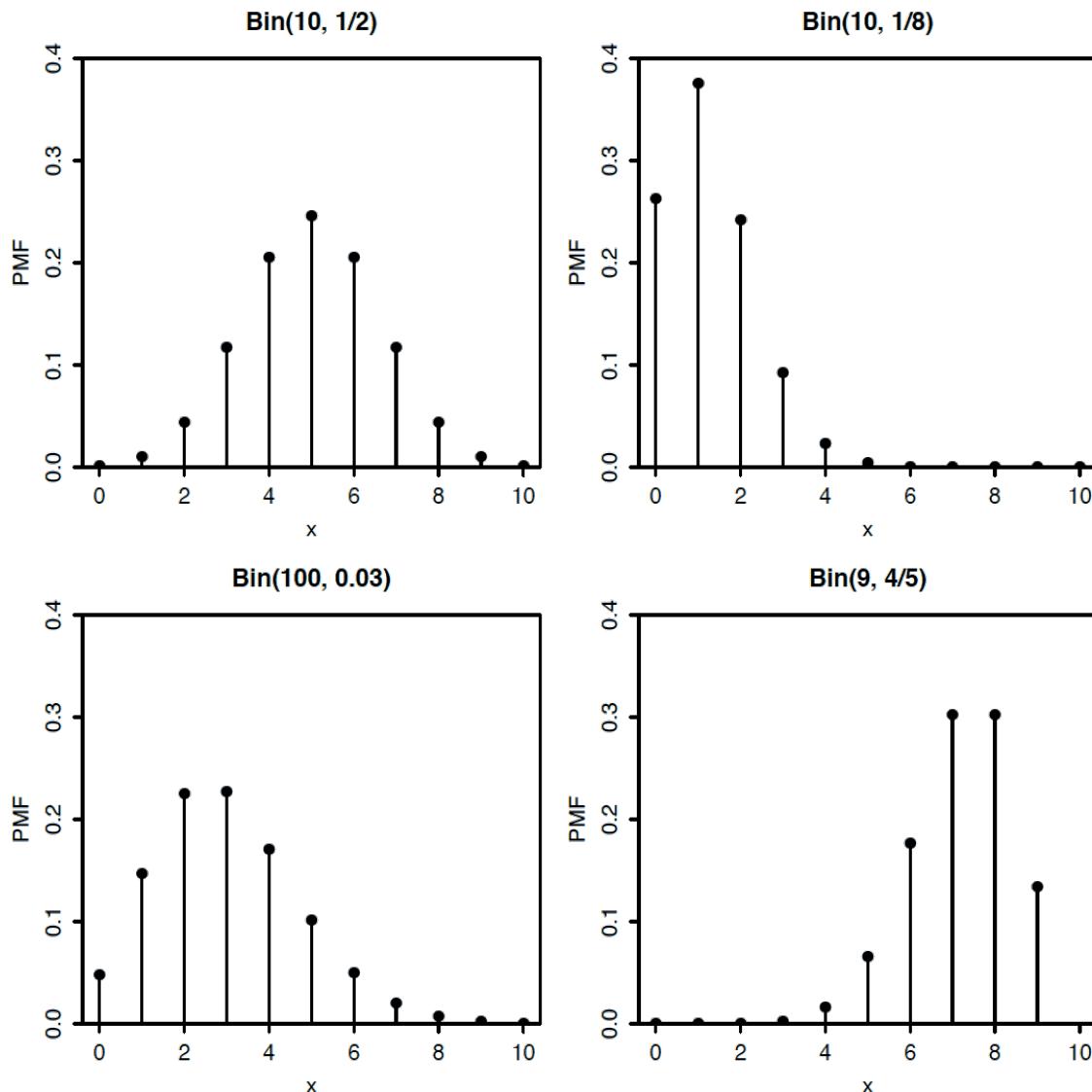
Theorem

If $X \sim \text{Bin}(n, p)$, then the PMF of X is

$$P(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$$

for $k = 0, 1, \dots, n$ (and $P(X = k) = 0$ otherwise).

Binomial PMF



Binomial PMF

$$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

$$Y = k \Rightarrow P(Y=n-k) = \binom{n}{n-k} p^{n-k} (1-p)^k$$

Theorem

Let $X \sim \text{Bin}(n, p)$, and $q = 1 - p$ (we often use q to denote the failure probability of a Bernoulli trial). Then $n - X \sim \text{Bin}(n, q)$.

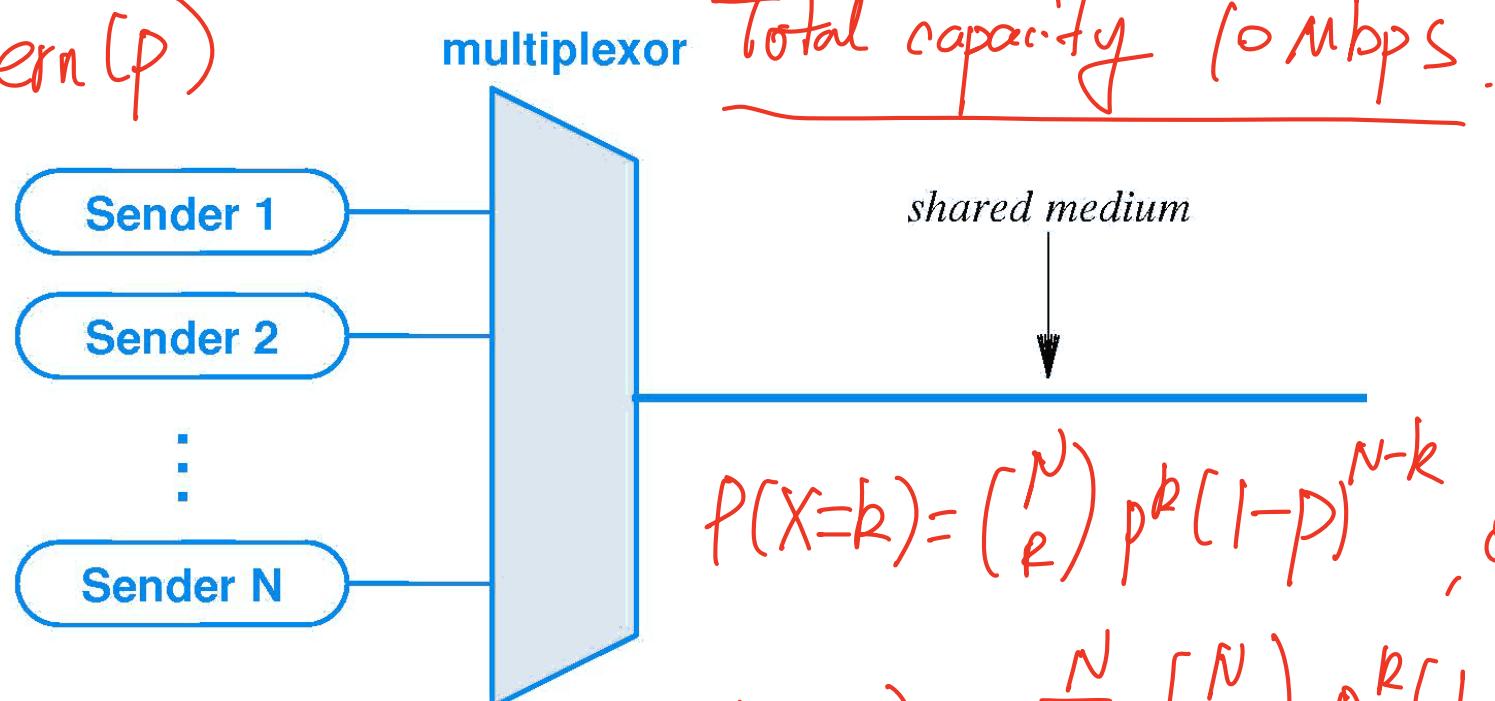
$$P(Y=k) = \binom{n}{k} q^k (1-q)^{n-k}$$

Example: Statistical Multiplexing

X : # of active senders at the same time -

each sender require $\frac{1}{n}$ Mbps
active prop. P .

$$X_i \sim \text{Bern}(p)$$

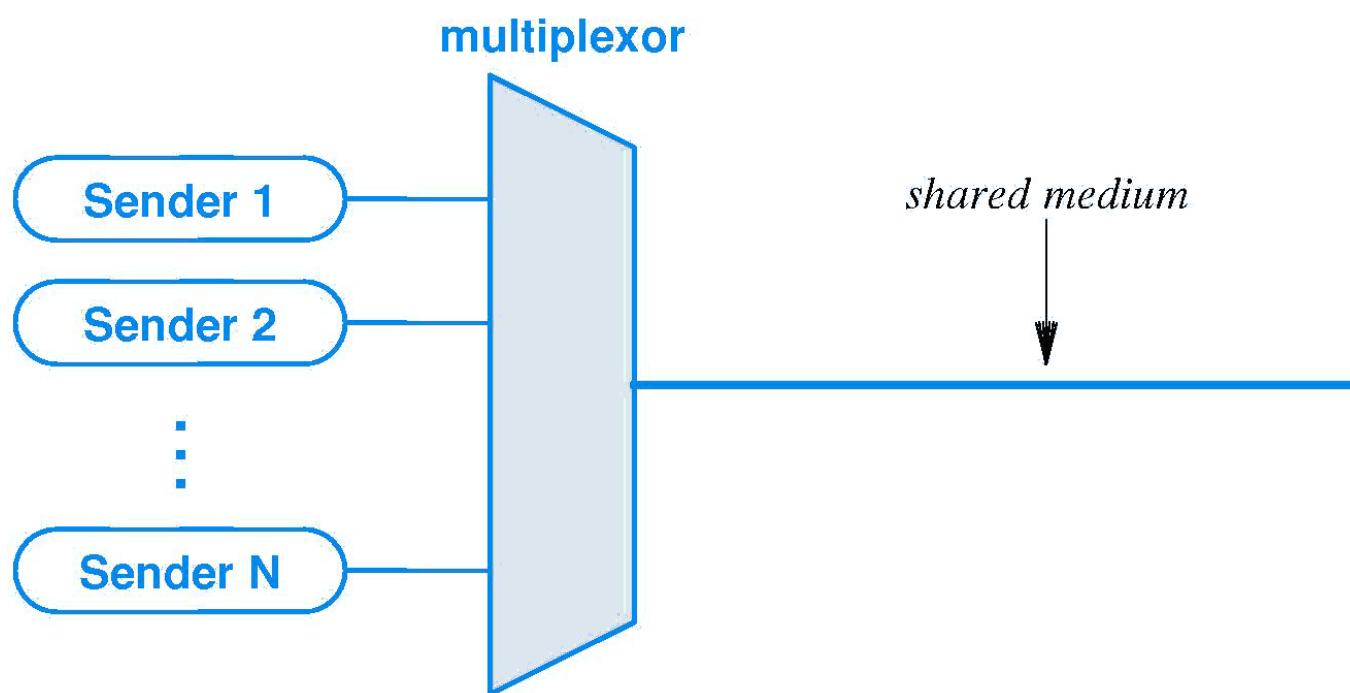


$$X = \sum_{i=1}^N X_i \sim \text{Bin}(N, p).$$

$$P(X=k) = \binom{N}{k} p^k (1-p)^{N-k}, \quad 0 \leq k \leq N.$$

$$P(X>0) = \sum_{k=1}^N \binom{N}{k} p^k (1-p)^{N-k}$$

Example: Statistical Multiplexing

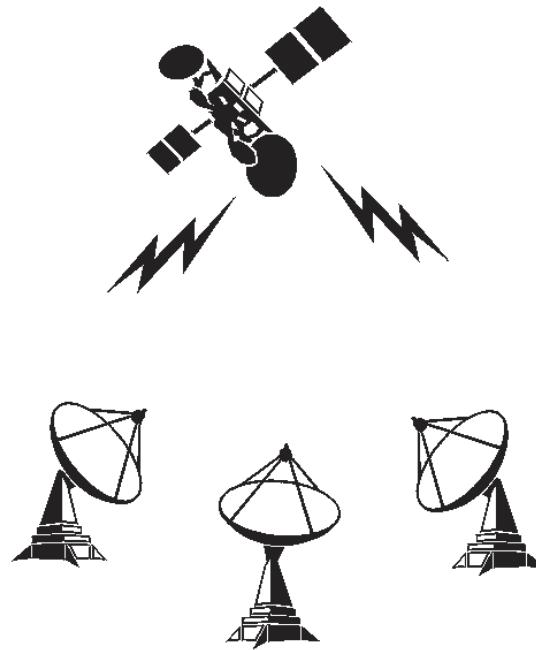


Example: Multiple Access (Aloha Protocol)

Wires + time -
slot



shared wireless



satellite

Example: Multiple Access (Aloha Protocol)

$$X = \sum_{i=1}^N X_i, \text{ # of devices transmit}$$

$$X \sim \text{Bin}(N, p).$$

$$X_i = \begin{cases} 1, & \text{i-th transmit} \\ 0, & \text{otherwise.} \end{cases}$$

$$X_i \sim \text{Bern}(p).$$

- N smart devices sharing a WiFi access point (e.g., in starbucks).
- ≥ 2 devices transmit simultaneously lead to collision.
- Aloha Protocol: proposed by Norman Abramson in the later 1960s.
- Each device transmits with probability p independently.
- What is the transmission rate (the number of successful transmissions per unit time)?

$$P(X=1) = \binom{N}{1} p (1-p)^{N-1} = N p (1-p)^{N-1} = \lambda(p), \text{ concave}$$

$$\lambda^*: \frac{d\lambda(p)}{dp} = 0 \Rightarrow p^* = \frac{1}{N} \Rightarrow \lambda^* = (1 - \frac{1}{N})^{N-1}, \quad N \rightarrow \infty, \lambda^* = e^{-1}$$

Example: Multiple Access (Aloha Protocol)

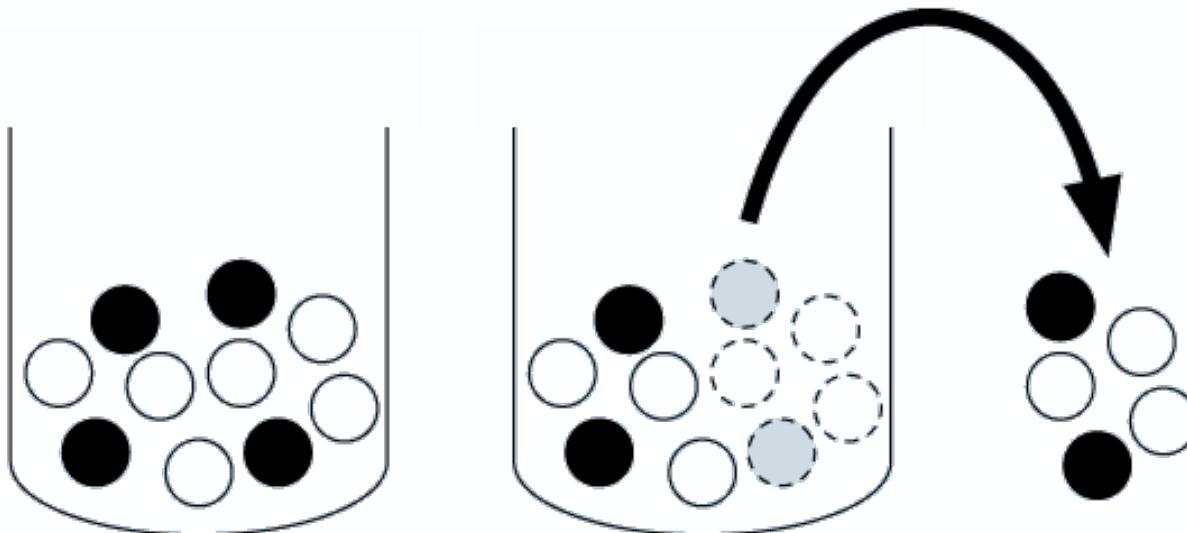
Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Urn Model

An urn is filled with w white and b black balls, then drawing n balls out of the urn

- with replacement: $\text{Bin}(n, \underline{w/(w+b)})$ distribution for the number of white balls obtained.
- without replacement: Hypergeometric distribution.



Story: Hypergeometric Distribution

$$X=k, \quad \binom{w}{k} \cdot \binom{b}{n-k}, \quad 0 \leq k \leq w.$$

Consider an urn with w white balls and b black balls. We draw n balls out of the urn at random without replacement, such that all $\binom{w+b}{n}$ samples are equally likely. Let X be the number of white balls in the sample. Then X is said to have the Hypergeometric distribution with parameters w , b , and n ; we denote this by $X \sim \text{HGeom}(w, b, n)$.

$$P(X=k) = \frac{\binom{w}{k} \cdot \binom{b}{n-k}}{\binom{w+b}{n}}$$

→ # of ways to choose
 k white balls.
 → total possible ways.

Hypergeometric PMF

Theorem

If $X \sim \text{HGeom}(w, b, n)$, then the PMF of X is

$$P(X = k) = \frac{\binom{w}{k} \binom{b}{n-k}}{\binom{w+b}{n}}$$

for integers k satisfying $0 \leq k \leq w$ and $0 \leq n - k \leq b$, and $P(X = k) = 0$ otherwise.

Identical Distribution

Theorem

The $\text{HGeom}(w, b, n)$ and $\text{HGeom}(n, w + b - n, w)$ distributions are identical. That is, if $X \sim \text{HGeom}(w, b, n)$ and $Y \sim \text{HGeom}(n, w + b - n, w)$, then X and Y have the same distribution.

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Story: Discrete Uniform Distribution

$$X_i = i, \quad 0 \leq i \leq 9.$$

$$C = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$P(X = X_i) = \frac{1}{10}.$$

Let C be a finite, nonempty set of numbers. Choose one of these numbers uniformly at random (i.e., all values in C are equally likely). Call the chosen number X . Then X is said to have the Discrete Uniform distribution with parameter C ; we denote this by $X \sim \text{DUnif}(C)$.

Zipf Distribution

- Zipf's Law & Zipf distribution: American linguist George Kingsley Zipf (1902-1950).
- Popularity distribution: popularity of the i^{th} most popular term is proportional to $1/i$.
- If $X \sim \text{Zipf}(\alpha > 0)$, then PMF of X is:

$$P(X = k) = \frac{1}{\sum_{j=1}^{\infty} \left(\frac{1}{j}\right)^{\alpha+1}}, k = 1, 2, \dots$$

$\sum_{k=1}^{\infty} P(X=k) = 1.$

Example of Zipf Distribution: Word Frequency



Examples of Zipf Distribution

- The world population lives in several large cities, a greater number of medium-sized cities, and a vast number of small towns.
- There are a few websites that get lots of hits, a greater number of websites that get a moderate number of hits, and a vast number of websites that hardly get any hits at all.
- A library has a few books that everyone wants to borrow (best sellers), a greater number of books that get borrowed occasionally (classics), and a vast number of books that hardly ever get borrowed.

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Definition



Definition

The cumulative distribution function (CDF) of an r.v. X is the function F_X given by $F_X(x) = P(X \leq x)$. When there is no risk of ambiguity, we sometimes drop the subscript and just write F (or some other letter) for a CDF.

$$P(X \leq 3) = P(X=1) + P(X=2)$$

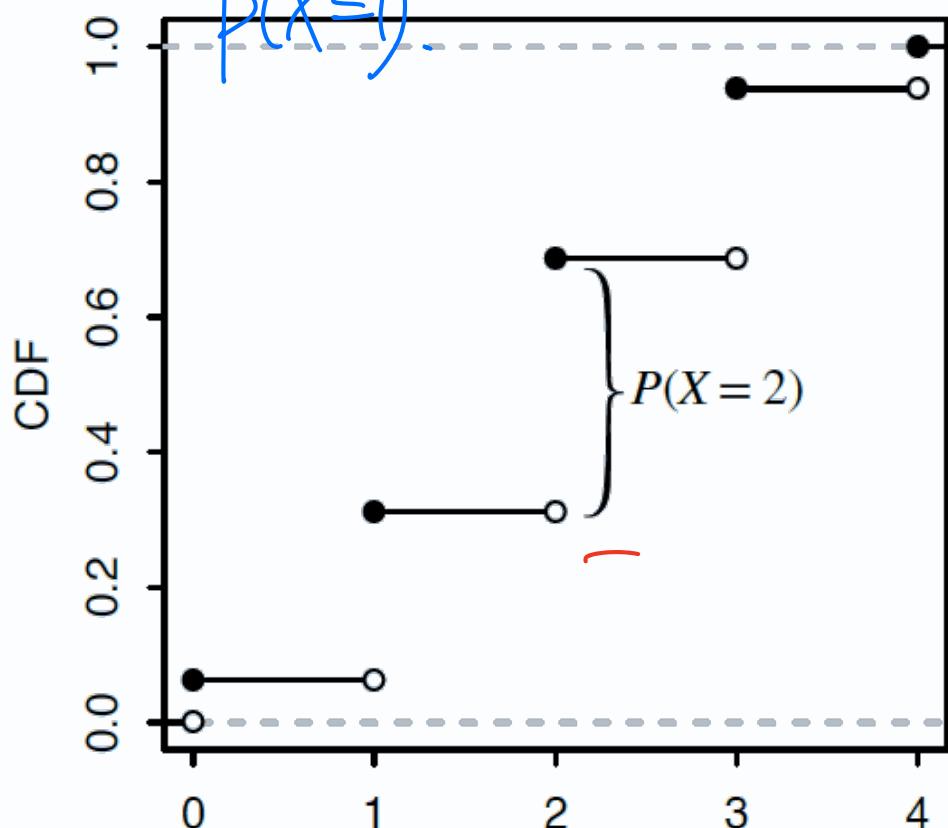
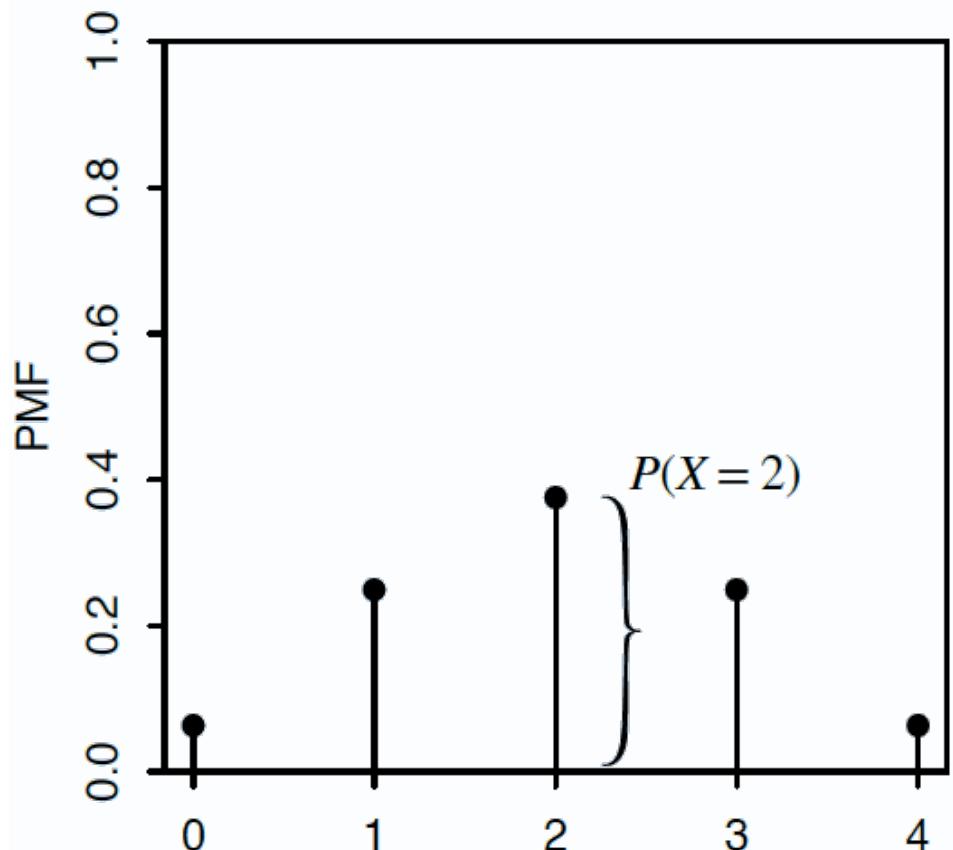
$$+ P(X=3)$$

Example

$$F(1.5) = P(X \leq 1.5) = P(X=0) + P(X=1)$$

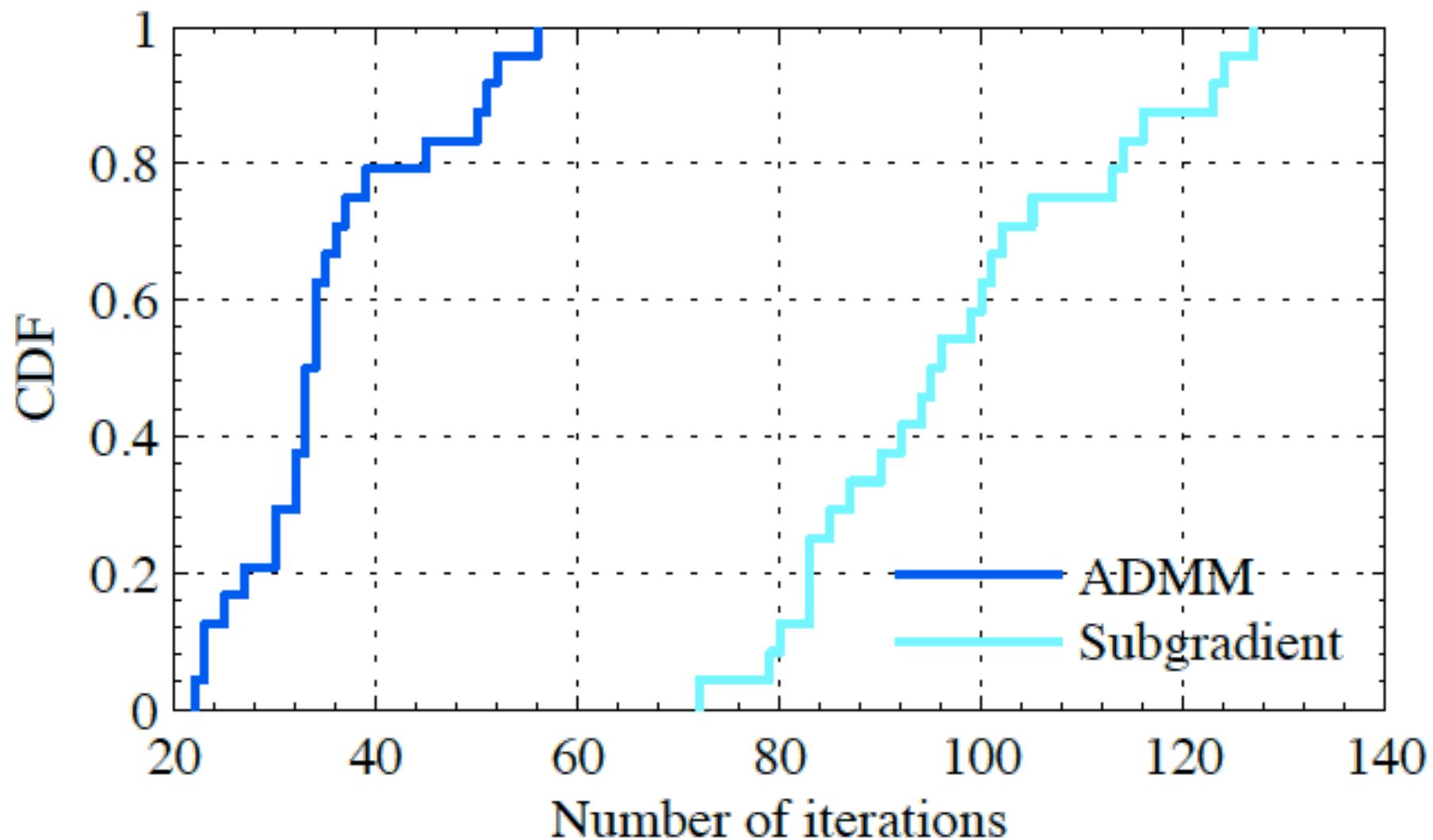
Let $X \sim \text{Bin}(4, 1/2)$, the PMF and CDF of X :

$$F(2) = F(1) + P(X=2).$$



$$F(2) = P(X \leq 2) = P(X=0) + P(X=1) + P(X=2).$$

Example



Valid CDFs

$$F(x_2) = F(x_1) + \underbrace{P(X_1 < X \leq x_2)}_{\geq 0}$$

Any CDF F has the following properties.

$$F(x_1) = P(X \leq x_1)$$

- Increasing: If $x_1 \leq x_2$, then $F(x_1) \leq F(x_2)$.
- Right-continuous: the CDF is continuous except possibly for having some jumps. Wherever there is a jump, the CDF is continuous from the right. That is, for any a , we have

$$F(x_1) = P(X \leq x_1)$$

$$F(a) = \lim_{x \rightarrow a^+} F(x). \quad (1)$$

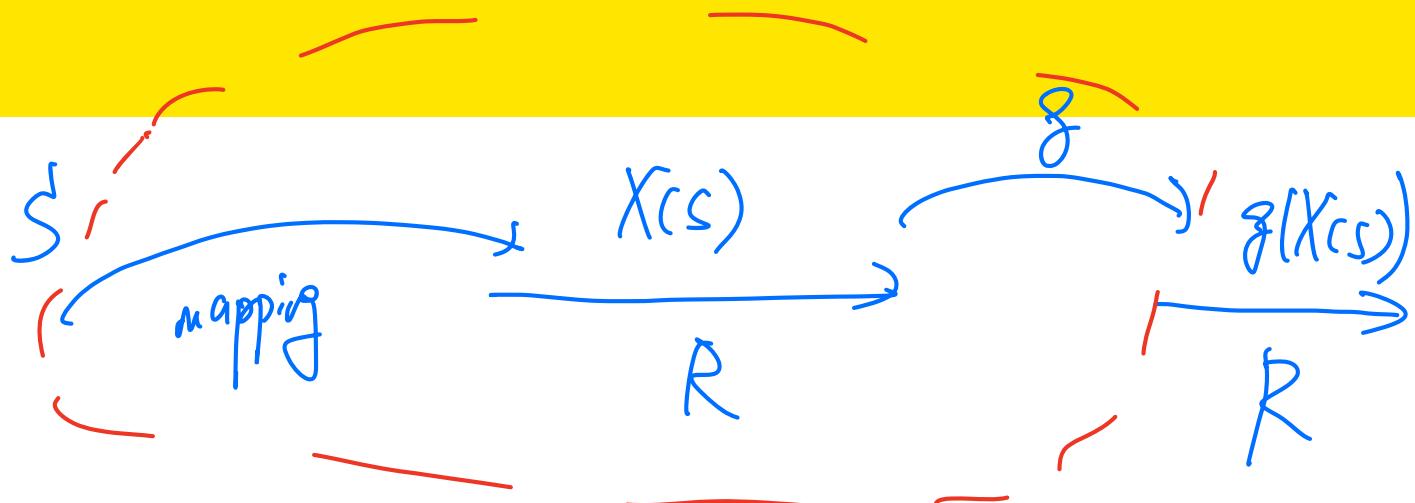
- Convergence to 0 and 1 in the limits:

$$\lim_{x \rightarrow -\infty} F(x) = 0 \text{ and } \lim_{x \rightarrow +\infty} F(x) = 1.$$

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Definition



Definition

For an experiment with sample space S , an r.v. X , and a function $g : \mathbb{R} \rightarrow \mathbb{R}$, $g(X)$ is the r.v. that maps s to $\underline{g(X(s))}$ for all $s \in S$.

PMF of $g(X)$

Theorem

Let X be a discrete r.v. and $g : \mathbb{R} \rightarrow \mathbb{R}$. Then the support of $g(X)$ is the set of all y such that $g(x) = y$ for at least one x in the support of X , and the PMF of $g(X)$ is

$$P(g(X) = y) = \sum_{x: g(x)=y} P(X = x)$$

for all y in the support of $g(X)$.

Example: Maximum of Two Die Rolls

$$\max(X, Y) = \{1, 2, 3, 4, 5, 6\}.$$

$$P[\max(X, Y) = 1] = P(X=1, Y=1) = P(X=1)P(Y=1) = \frac{1}{36}.$$

$$\begin{aligned} P[\max(X, Y) = 2] &= P(X=2, Y=1) + P(X=1, Y=2) + P(X=2, Y=2) \\ &= \frac{1}{12}. \end{aligned}$$

We roll two fair 6-sided dice. Let X be the number on the first die and Y the number on the second die. What is the PMF of $\max(X, Y)$.

$$P[\max(X, Y) = 3] = \frac{5}{36}, \quad P[\max(X, Y) = 4] = \frac{7}{36}.$$

$$P[\max(X, Y) = 5] = \frac{11}{36}, \quad P[\max(X, Y) = 6] = \frac{9}{36}.$$

Example: Sympathetic Magic

$$\textcircled{1} \quad Y = 2X, \quad P(Y=y) \neq 2P(X=x)$$

$$P(X=0) = \frac{1}{2}, \quad P(Y=g(x)=y) = \sum_{x: g(x)=y} P(X=x) = P(X=\frac{y}{2})$$

$$P(X=1) = \frac{1}{4}$$

$$P(X=2) = \frac{1}{4}$$

- Given an r.v. X , trying to get the PMF of $2X$ by multiplying the PMF of X by 2.

- Claiming that because X and Y have the same distribution, X must always equal Y , i.e., $P(X = Y) = 1$.

$$P(Y=0) = P(X=\frac{0}{2}) = \frac{1}{2}.$$

$$P(Y=1) = P(X=\frac{1}{2}) = 0$$

$$P(Y=2) = P(X=\frac{2}{2}) = \frac{1}{4}$$

$$P(Y=4) = P(X=\frac{4}{2}) = \frac{1}{4}$$

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Independence of Two R.V.s

$$P(X \leq x, Y \leq y) = P(X \leq x | Y \leq y) P(Y \leq y). \quad \text{H}_{x,y}.$$

Definition

Random variables X and Y are said to be *independent* if

$$\underbrace{P(X \leq x, Y \leq y)}_{\text{for all } x, y \in \mathbb{R}} = \underbrace{P(X \leq x)}_{\text{in the support of } X} \underbrace{P(Y \leq y)}_{\text{in the support of } Y}$$

for all $x, y \in \mathbb{R}$. In the discrete case, this is equivalent to the condition

$$P(X = x, Y = y) = P(X = x) P(Y = y)$$

for all x, y with x in the support of X and y in the support of Y .

Independence of Many R.V.s

Definition

Random variables X_1, \dots, X_n are *independent* if

$$P(X_1 \leq x_1, \dots, X_n \leq x_n) = P(X_1 \leq x_1) \cdots P(X_n \leq x_n)$$

for all $x_1, \dots, x_n \in \mathbb{R}$. For infinitely many r.v.s, we say that they are independent if every finite subset of the r.v.s is independent.

I.I.D.

We will often work with random variables that are independent and have the same distribution. We call such r.v.s independent and identically distributed, or i.i.d. for short.

- Independent & Identically Distributed.
- Independent & NOT Identically Distributed.
- Dependent & Identically Distributed.
- Dependent & NOT Identically Distributed.

Binomial Distribution

$$X = \sum_{i=1}^n X_i.$$

$$X_i = \begin{cases} 1, & P \\ 0, & 1-p. \end{cases}$$

Theorem

If $X \sim \text{Bin}(n, p)$, viewed as the number of successes in n independent Bernoulli trials with success probability p , then we can write

$X = X_1 + \cdots + X_n$ where the X_i are i.i.d. $\text{Bern}(p)$.

Binomial Distribution

Theorem

If $X \sim \text{Bin}(n, p)$, $Y \sim \text{Bin}(m, p)$, and X is independent of Y , then $X + Y \sim \text{Bin}(n + m, p)$.

Proof 1: LOTP

$X \sim \text{Bin}(n, p)$, $Y \sim \text{Bin}(m, p)$. X, Y independent
 $Z = X + Y = k$, $0 \leq k \leq n+m$.

$$\begin{aligned}
 P(Z=k) &\stackrel{\text{LOTP}}{=} \sum_{j=0}^k P(X+Y=k | X=j) P(X=j), \\
 &= \sum_{j=0}^k P(Y=k-j | X=j) P(X=j), \\
 &= \sum_{j=0}^k P(Y=k-j) P(X=j) \\
 &= \sum_{j=0}^k \binom{m}{k-j} p^{k-j} (1-p)^{m-k+j} \cdot \binom{n}{j} p^j (1-p)^{n-j} \\
 &= \boxed{\sum_{j=0}^k \binom{m}{k-j} \binom{n}{j} p^k (1-p)^{m+n-k}} = \boxed{\binom{m+n}{k} p^k (1-p)^{m+n-k}}
 \end{aligned}$$

Proof 2: Representation

$$X \sim \text{Bin}(n, p) \quad X = X_1 + \dots + X_n, \quad X_i \sim \text{Bern}(p), \quad (1 \leq i \leq n).$$

$$Y \sim \text{Bin}(m, p) \quad Y = Y_1 + \dots + Y_m, \quad Y_j \sim \text{Bern}(p), \quad (1 \leq j \leq m).$$

$$X+Y = \underbrace{(X_1 + \dots + X_n)}_{(m+n) \text{ independent Bern}(p)} + \underbrace{(Y_1 + \dots + Y_m)}$$

$$X+Y \sim \text{Bin}(n+m, p)$$

Proof 3: Story

X : # of success in n independent Bernoulli trials. (p)

y : # of - - - m - - - - - (P)

$$x+y \# \cdots \# n+m = \cdots = (p) = \cdots$$

$$X+Y \sim \text{Bin}(n+m, p).$$

Conditional Independence of R.V.s

Definition

Random variables X and Y are conditionally independent given an r.v. Z if for all $x, y \in \mathbb{R}$ and all z in the support of Z ,

$$P(X \leq x, Y \leq y | Z = z) = P(X \leq x | Z = z)P(Y \leq y | Z = z).$$

For discrete r.v.s, an equivalent definition is to require

$$P(X = x, Y = y | Z = z) = P(X = x | Z = z)P(Y = y | Z = z).$$

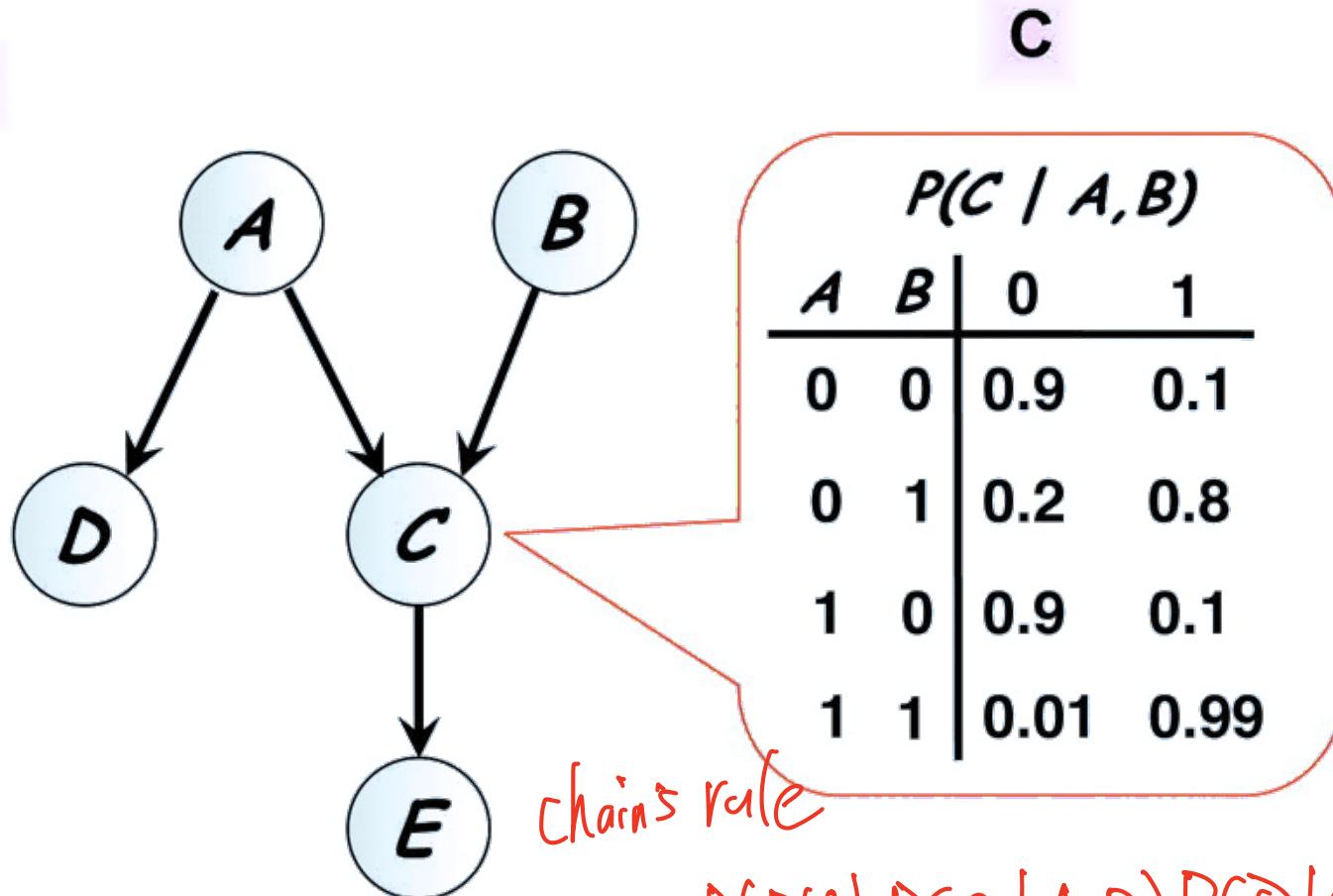
$\forall x, y, z$ in their support sets.

Conditional PMF

Definition

For any discrete r.v.s X and Z , the function $P(X = x | Z = z)$, when considered as a function of x for fixed z , is called the conditional PMF of X given $Z = z$.

Example: Bayesian Network



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

$\log[\quad] = \log[\quad] + \dots + \log[\quad]$

Example: Bayesian Network

- A probabilistic graphical model proposed by Judea Pearl in 1985.
- Represents a set of random variables and their conditional dependencies.
- Node: random variables
- Edge: conditional dependency
- Topology: a directed acyclic graph (DAG)
- Each node has a conditional probability table (CPT) with input from its parent nodes.
- Popular models for inference and learning.

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Connection

- Binomial \implies Hypergeometric: **conditioning**
- Hypergeometric \implies Binomial: **taking a limit**

Connection

$$\frac{P(Y=r-x | X=x) P(X=x)}{P(X+Y=r | X=x) P(X=x)}$$

$$\textcircled{1} \quad X+Y \sim \text{Bin}(n+m, p).$$

$$\textcircled{2} \quad P(X=x | X+Y=r) = \frac{P(X=x, X+Y=r)}{P(X+Y=r)} = \frac{P(X=x, Y=r-x)}{P(X+Y=r)} = \frac{P(X=x)P(Y=r-x)}{P(X+Y=r)}.$$

Theorem

If $X \sim \text{Bin}(n, p)$, $Y \sim \text{Bin}(m, p)$, and X is independent of Y , then the conditional distribution of X given $X + Y = r$ is HGeom(n, m, r).

$$= \frac{\binom{n}{x} p^x (1-p)^{n-x} \binom{m}{r-x} p^{r-x} (1-p)^{m-r+x}}{\binom{n+m}{r} p^r (1-p)^{n+m-r}} = \frac{\binom{n}{x} \binom{m}{r-x}}{\binom{n+m}{r}}$$

Connection

$N \rightarrow \infty$, equivalent to sampling with replacement.

Theorem

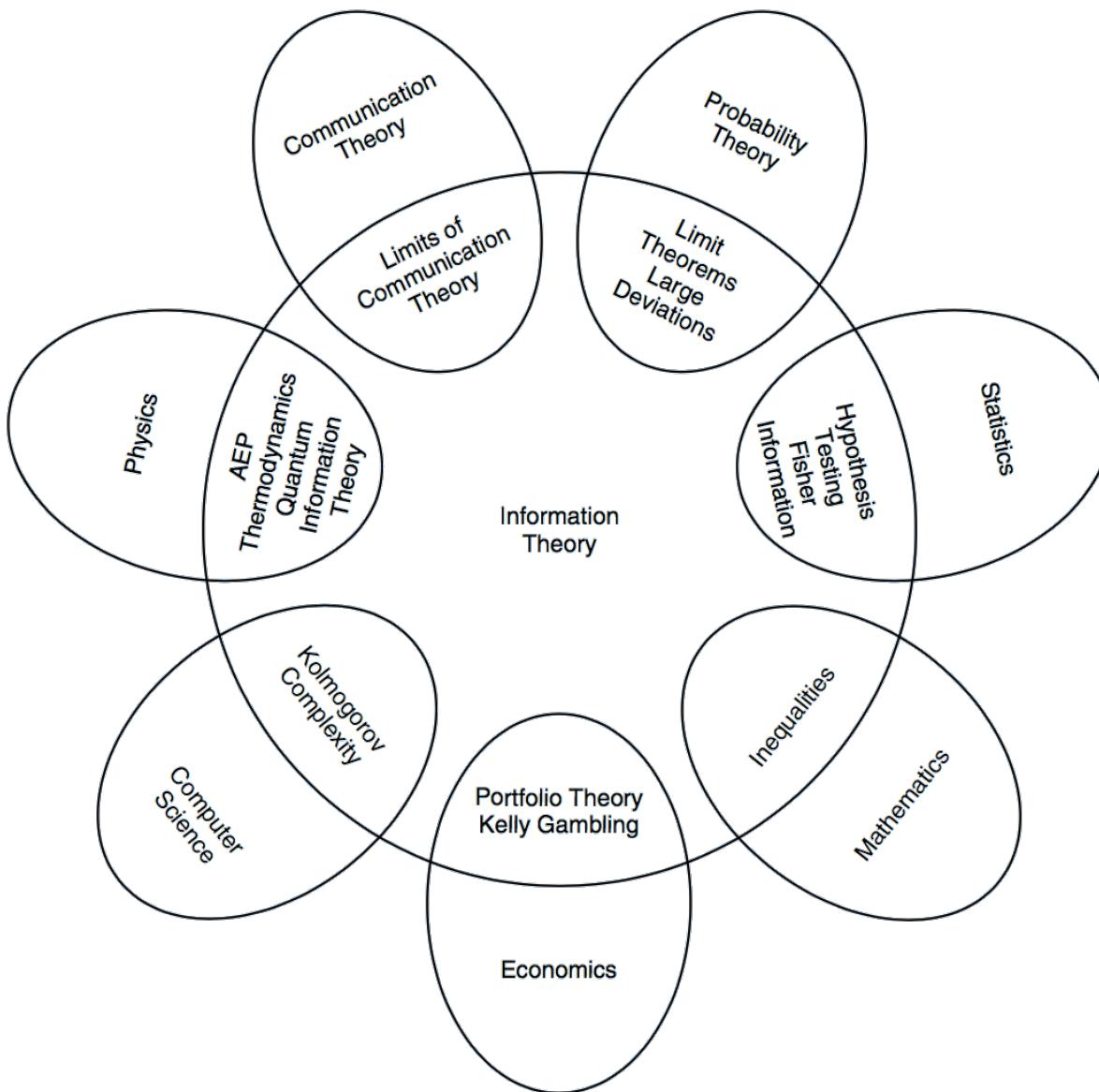
If $X \sim \text{HGeom}(w, b, n)$ and $N = w + b \rightarrow \infty$ such that $p = w/(w + b)$ remains fixed, then the PMF of X converges to the $\text{Bin}(n, p)$ PMF.

$$P(X=k) = \binom{n}{k} \left(\frac{w}{w+b}\right)^k \left(\frac{b}{w+b}\right)^{n-k}.$$

Outline

- 1 Random Variables
- 2 Bernoulli and Binomial
- 3 Hypergeometric
- 4 Discrete Uniform & Zipf Distribution
- 5 Cumulative Distribution Functions
- 6 Functions of Random Variables: Random Variables
- 7 Independence of R.V.s
- 8 Binomial & Hypergeometric
- 9 Information Theory & Entropy

Information Theory & Other Fields



Entropy

$$p = \frac{1}{2}, \quad H(X) = 1.$$

$$p = 1, \quad H(X) = 0.$$

$$p(x) = \begin{cases} 1, & p \\ 0, & 1-p \end{cases}$$

$$\begin{aligned} H(X) &= P \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p} \\ &= -p \log_2 p - (1-p) \log_2 (1-p). \end{aligned}$$

Definition

Given a random variable X with a probability mass function $p(x)$ and a support \mathcal{X} . The entropy of X is defined by

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log_2 p(x).$$

$$= \sum_{x \in \mathcal{X}} p(x) \log_2 \frac{1}{p(x)}.$$

Entropy of Discrete Uniform Distribution

- X has a uniform distribution over k outcomes.
- $p(x) = 1/k$.
- Then the entropy of X is

$$H(X) = - \sum_{x=1}^k p(x) \log_2 p(x) = - \sum_{x=1}^k \frac{1}{k} \log_2 \frac{1}{k} = \log_2 k.$$

Balance Puzzle

 k coins.

① one measurement $\log_2 3$. bit.

② k coins. $2k$ possible outcomes. $\log_2(2k)$. bit

You have 13 apparently identical gold coins. One of them is false but is virtually indistinguishable from the others. You also have a balance with two pans, but without weights. Accordingly, any measurement will tell you if the loaded pans weight the same or, if not, which weighs more. How many measurements are needed to find the false coin?

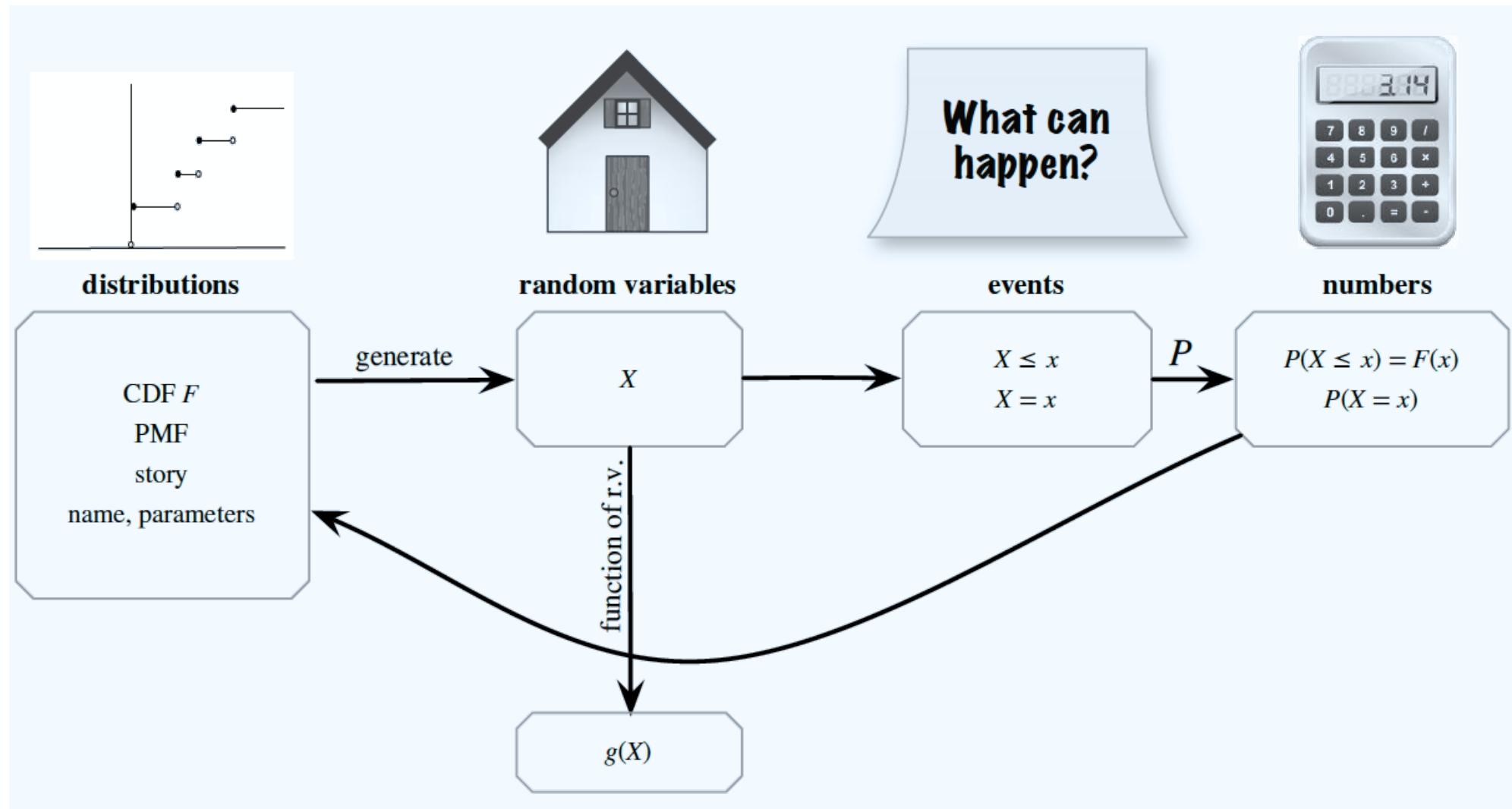
$$n \cdot \log_2 3 \geq \log_2(2k) \Rightarrow \underline{3^n \geq 2k} \rightarrow 3^n \geq 2k+1 \\ \Rightarrow k \leq \frac{3^n - 1}{2}$$

Solution

Entropy Bounds in General

Known	Goal	Maximum Coins for n weighings	Number of Weighings for c coins
Whether target coin is lighter or heavier than others	Identify coin	3^n	$\lceil \log_3(c) \rceil$
Target coin is different from others	Identify coin	$\frac{3^n - 1}{2}$ [1]	$\lceil \log_3(2c + 1) \rceil$
Target coin is different from others, or all coins are the same	Identify if unique coin exists, and whether it is lighter or heavier	$\frac{3^n - 1}{2} - 1$	$\lceil \log_3(2c + 3) \rceil$

Summary 1



References

- Chapter 3 of **BH**
- Chapter 2 of **BT**