

Lecture 1: Probability and Counting

Wen Dingzhu

School of Information Science and Technology (SIST)
ShanghaiTech University

wendzh@shanghaitech.edu.cn

January 30, 2023



上海科技大学
ShanghaiTech University

Overview

- 1 Probabilistic Model
- 2 Naive Definition of Probability & Counting
- 3 Other Non-Axiomatic Definitions of Probability
- 4 Axiomatic Definition of Probability

Outline

1 Probabilistic Model

2 Naive Definition of Probability & Counting

3 Other Non-Axiomatic Definitions of Probability

4 Axiomatic Definition of Probability

Set $A = \{a, b, c, d\} = \{b, a, d, c\}$.

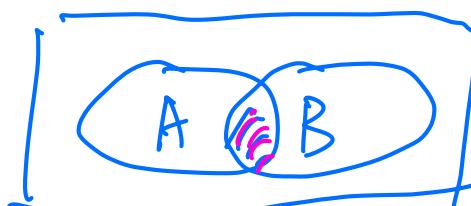
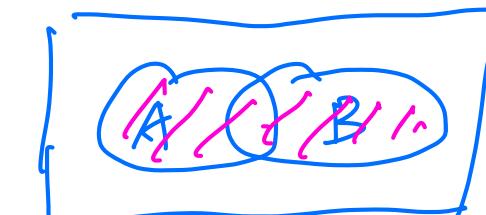
确定性 $a \in A$ or $a \notin A$. 无序性

互异性

$a \neq b, b \neq c, c \neq d, d \neq a$

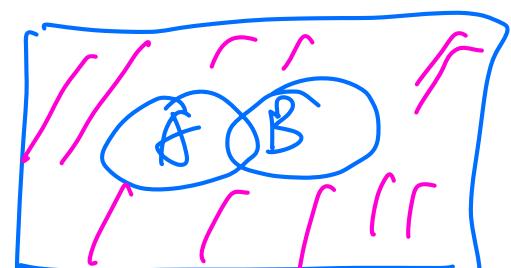
A set is a collection of objects. Given two sets A, B , key concepts include

- empty set: \emptyset
- A is a *subset* of B : $A \subseteq B$
- union of A and B : $A \cup B$
- intersection of A and B : $A \cap B$
- complement of A : A^c
- *De Morgan's laws*:

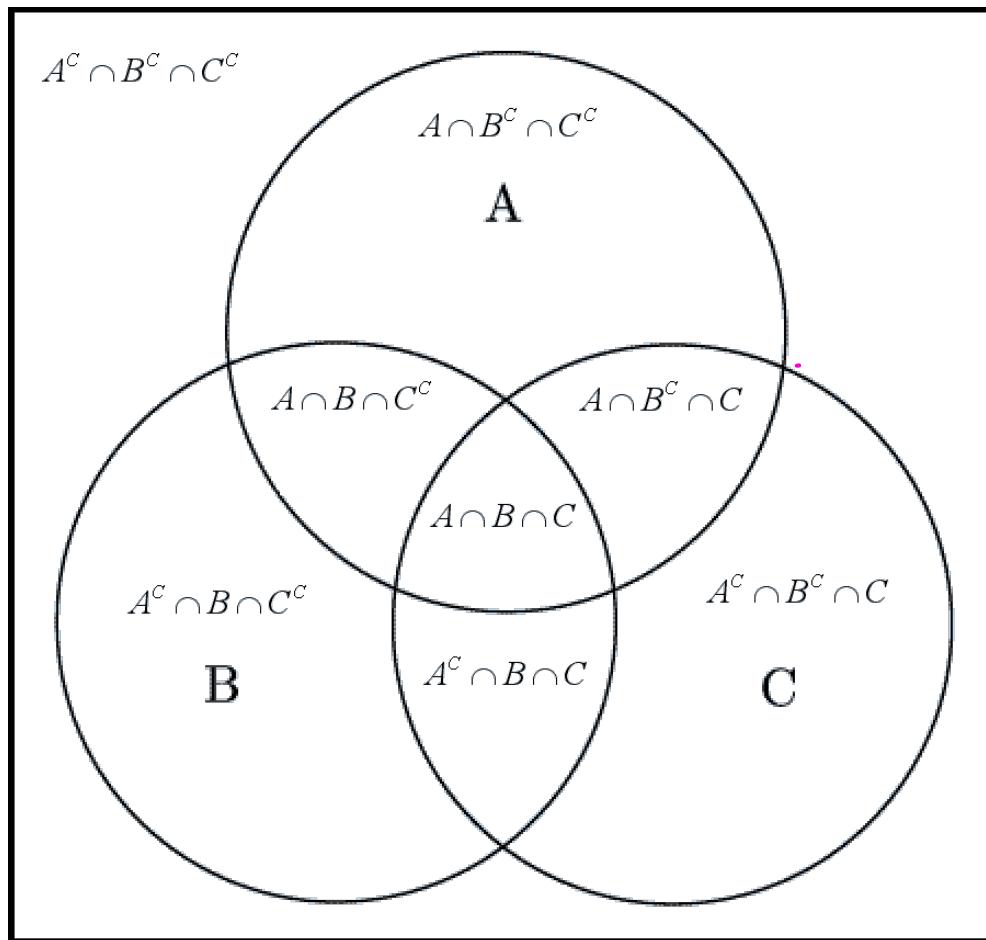


$$(A \cup B)^c = A^c \cap B^c,$$

$$(A \cap B)^c = A^c \cup B^c$$



Venn Diagram

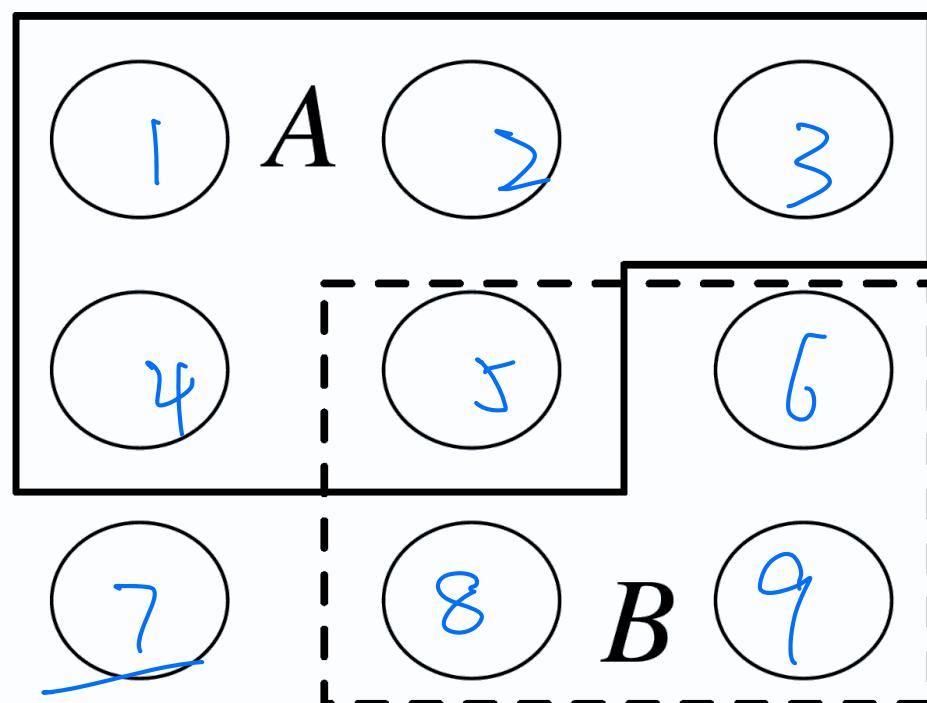


Sample Space & Event

$\{H, T\}$, $\{HH, HT, TH, TT\}$

- The sample space S of [an experiment] the set of all possible outcomes of the experiment.
- An event A is a subset of the sample space S .
- A occurred if the actual outcome is in A .

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



$$A = \{1, 2, 3, 4, 5\}$$

$$B = \{5, 6, 7, 8, 9\}$$

$$A \cap B = \{5\}$$

Example: Coin flips

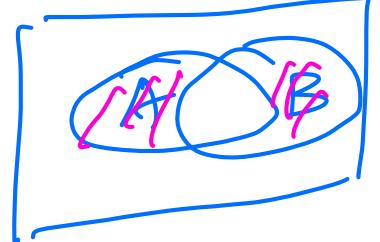
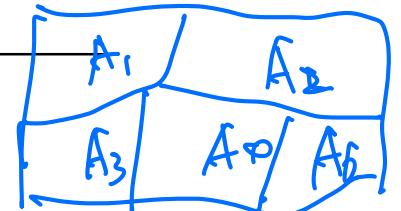
$$s_i \neq j \in \{0, 1\}.$$

A coin is flipped 10 times. Writing Heads as 1 and Tails as 0. Then

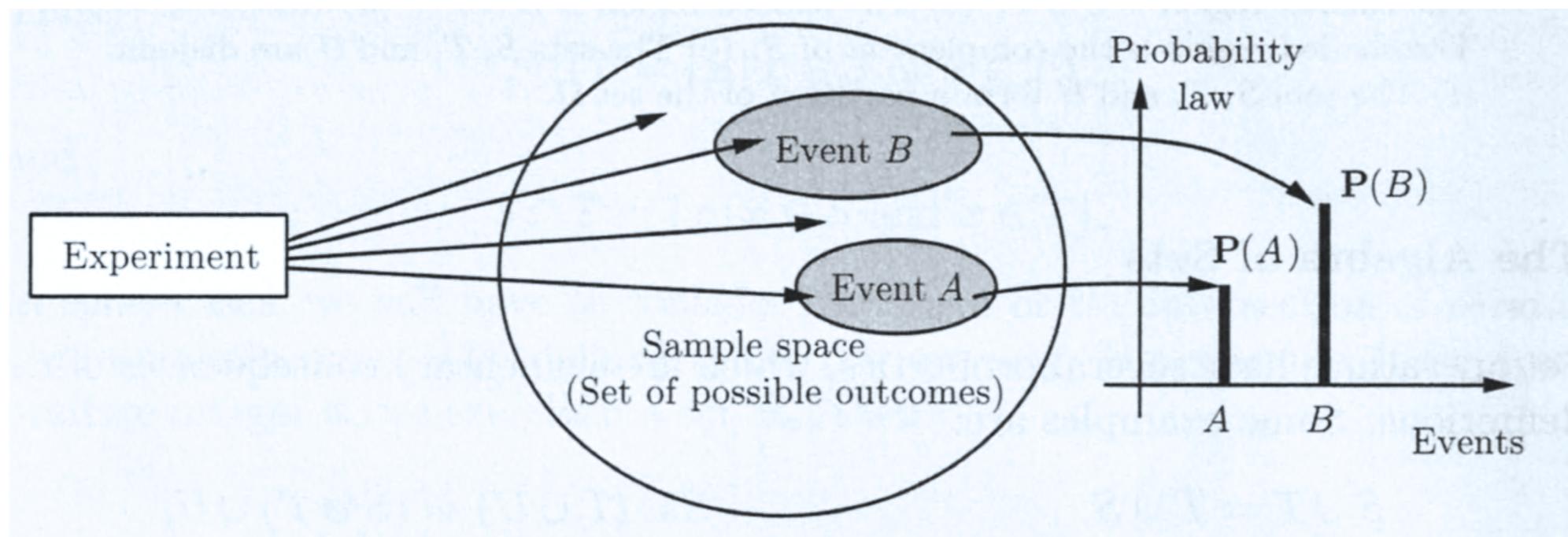
- An outcome is a sequence $(s_1, s_2, \dots, s_{10})$ with $s_j \in \{0, 1\}$ ✓
- The sample space: the set of all such sequences. $\{(s_1, s_2, \dots, s_{10})\}$
- A_j : the event that the j^{th} flip is Head. $\{(\dots, s_j = 1, \dots)\}$
- B : the event that at least one flip was Head. $(B = \bigcup_{j=1}^{10} A_j)$
- C : the event that all the flips were Heads. $(C = \bigcap_{j=1}^{10} A_j)$
- D : the event that there were at least two consecutive Heads.
 $(D = \bigcup_{j=1}^9 (A_j \cap A_{j+1}))$

Translation Between English & Sets

English	Sets
<i>Events and occurrences</i>	
sample space	S
<u>s</u> is a possible outcome	$s \in S$
<u>A</u> is an event	$\underline{A} \subseteq S$
A occurred	$s_{\text{actual}} \in A$
something must happen	$s_{\text{actual}} \in S$
<i>New events from old events</i>	
A or B (inclusive)	$A \cup B$
A and B	$A \cap B$
not A	A^c
A or B , but not both	$(A \cap B^c) \cup (A^c \cap B)$
at least one of A_1, \dots, A_n	$A_1 \cup \dots \cup A_n$
all of A_1, \dots, A_n	$A_1 \cap \dots \cap A_n$
<i>Relationships between events</i>	
<u>A</u> implies <u>B</u>	$A \subseteq B$
<u>A</u> and <u>B</u> are <u>mutually exclusive</u>	$A \cap B = \emptyset$
A_1, \dots, A_n are a <u>partition</u> of <u>S</u>	$A_1 \cup \dots \cup A_n = S, A_i \cap A_j = \emptyset \text{ for } i \neq j$

Probabilistic Model



Outline

- 1 Probabilistic Model
- 2 Naive Definition of Probability & Counting
- 3 Other Non-Axiomatic Definitions of Probability
- 4 Axiomatic Definition of Probability

Naive Definition of Probability

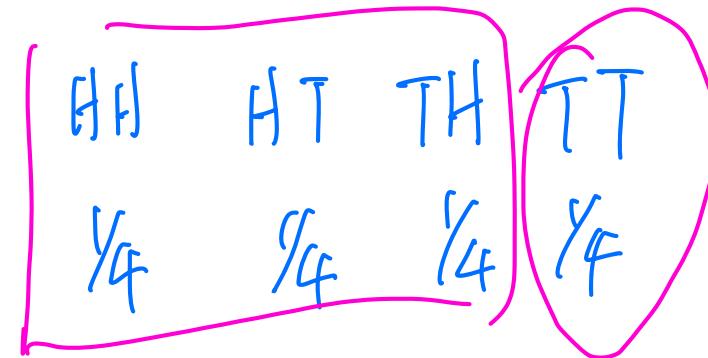
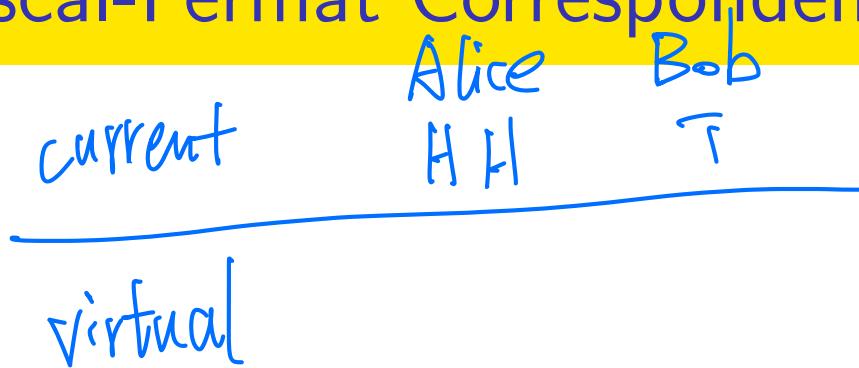
- Assumption 1: finite sample space
- Assumption 2: all outcomes occur equally likely

Definition

Let A be an event for an experiment with a finite sample space S . The naive probability of A is

$$P_{\text{naive}}(A) = \frac{|A|}{|S|} = \frac{\text{number of outcomes favorable to } A}{\text{total number of outcomes in } S}.$$

Pascal-Fermat Correspondence: Unfinished Game



Alice and Bob play a game with a pot of \$40, where the one wins three tosses of a fair coin will get the whole pot. On each round, Alice chooses heads, Bob chooses tails. But for some reason they have to abandon the game after three rounds, with Alice ahead, 2 to 1. How do they divide the pot?

$$\} : |$$

Solution

Basic Counting

- **Sampling:** sampling from a set means choosing an element (draw a sample) or multiple elements (draw samples) from that set.
- **With Replacement & Without Replacement:** put each element(object) back or not after each draw. Or “repetition is allowed or not”.
- **Ordered & Unordered:** ordering matters or not.

Basic Counting

- Ordered Sampling with Replacement
- Ordered Sampling without Replacement
- Unordered Sampling without Replacement
- Unordered Sampling with Replacement

Basic Counting

Choose k elements from a set with n elements (choose k objects out of n distinguishable objects), the number of possible ways:

	Order Matters	Order Not Matter
with replacement		
without replacement		

Basic Counting

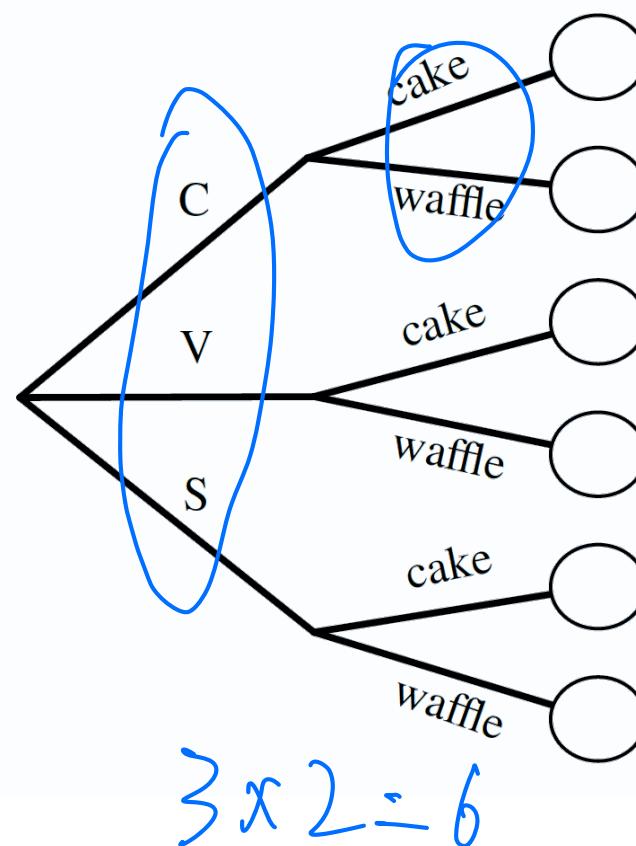
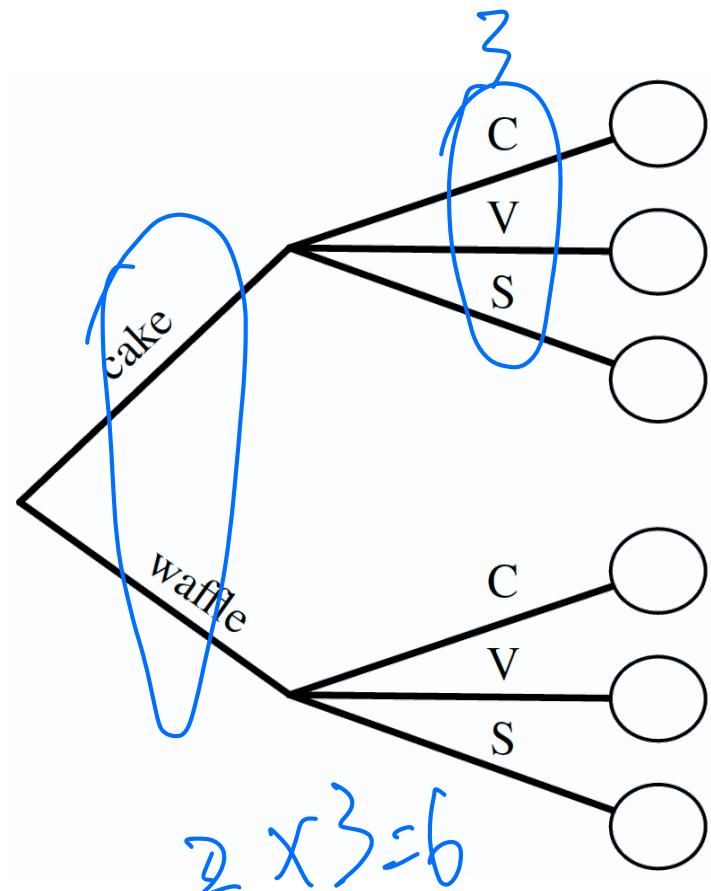
Choose k elements from a set with n elements (choose k objects out of n distinguishable objects), the number of possible ways:

	Order Matters	Order Not Matter
with replacement	? n^k	
without replacement	? A_n^k	C_n^k

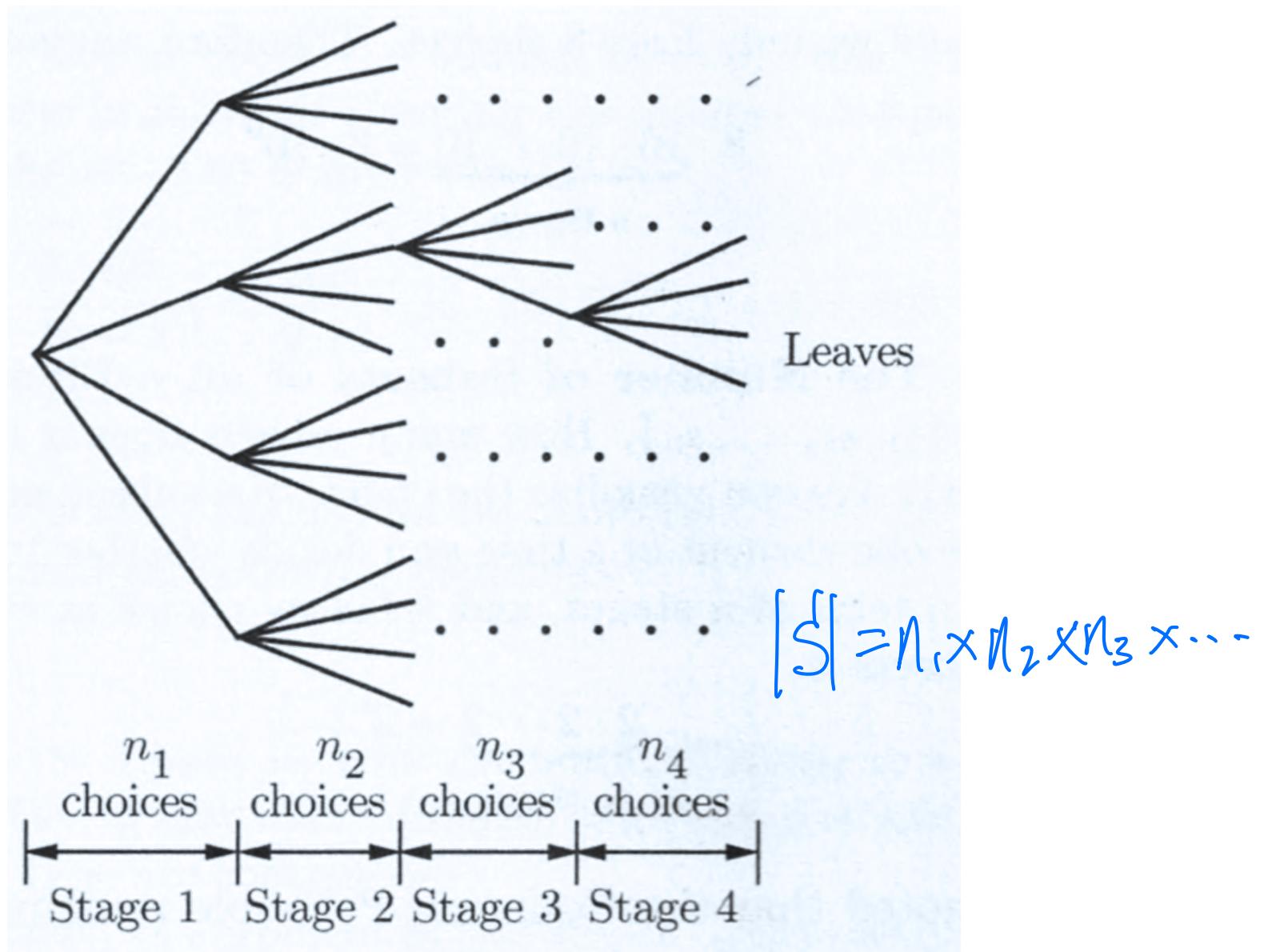
Multiplication Rule

You buy an ice cream cone with several choices:

- cone: cake or waffle
- flavor: chocolate, vanilla, or strawberry



Multiplication Rule in General



Ordered Sampling With Replacement

$$\begin{matrix} 1 & 2 & 3 & \dots & k \\ n \times n \times n \times \dots \times n & & & & n^k \end{matrix}$$

Theorem

Consider n objects in a set and making k choices from them, one at a time with replacement (i.e., choosing a certain object does not preclude it from being chosen again). Then there are n^k possible outcomes.

Ordered Sampling Without Replacement

$$\begin{array}{ll}
 k > n, & 0 \\
 k = n, & 1 \\
 k < n, & \begin{matrix} 1 & 2 & 3 & \dots & k \\ n \times (n-1) \times (n-2) \times \dots \times (n-k+1) \end{matrix}
 \end{array}$$

Theorem

Consider n objects in a set and making k choices from them, one at a time without replacement (i.e., choosing a certain object preclude it from being chosen again). Then there are $\underline{n(n-1)\cdots(n-k+1)}$ possible outcomes for $k \leq n$ (and 0 possibilities for $k > n$). When $k = n$, there are $\underline{n!}$ possible outcomes, each outcome is called a “permutation” of such n objects.

$$\frac{n!}{(n-k)!}$$

Example: Birthday Problem

$$k \geq 366, \quad P(A) = 1$$

$$k \leq 365 \quad 1 - \frac{A_{365}^k}{365^k}$$

There are k people in a room. Assume each person's birthday is equally likely to be any of the 365 days of the year (we exclude February 29), and that people's birthdays are independent (we assume there are no twins in the room). What is the probability that two or more people in the group have the same birthday?

event A = " ≥ 2 people have the same birthday".

A^c = "no one shares a same birthday"

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

Solution of Birthday Problem

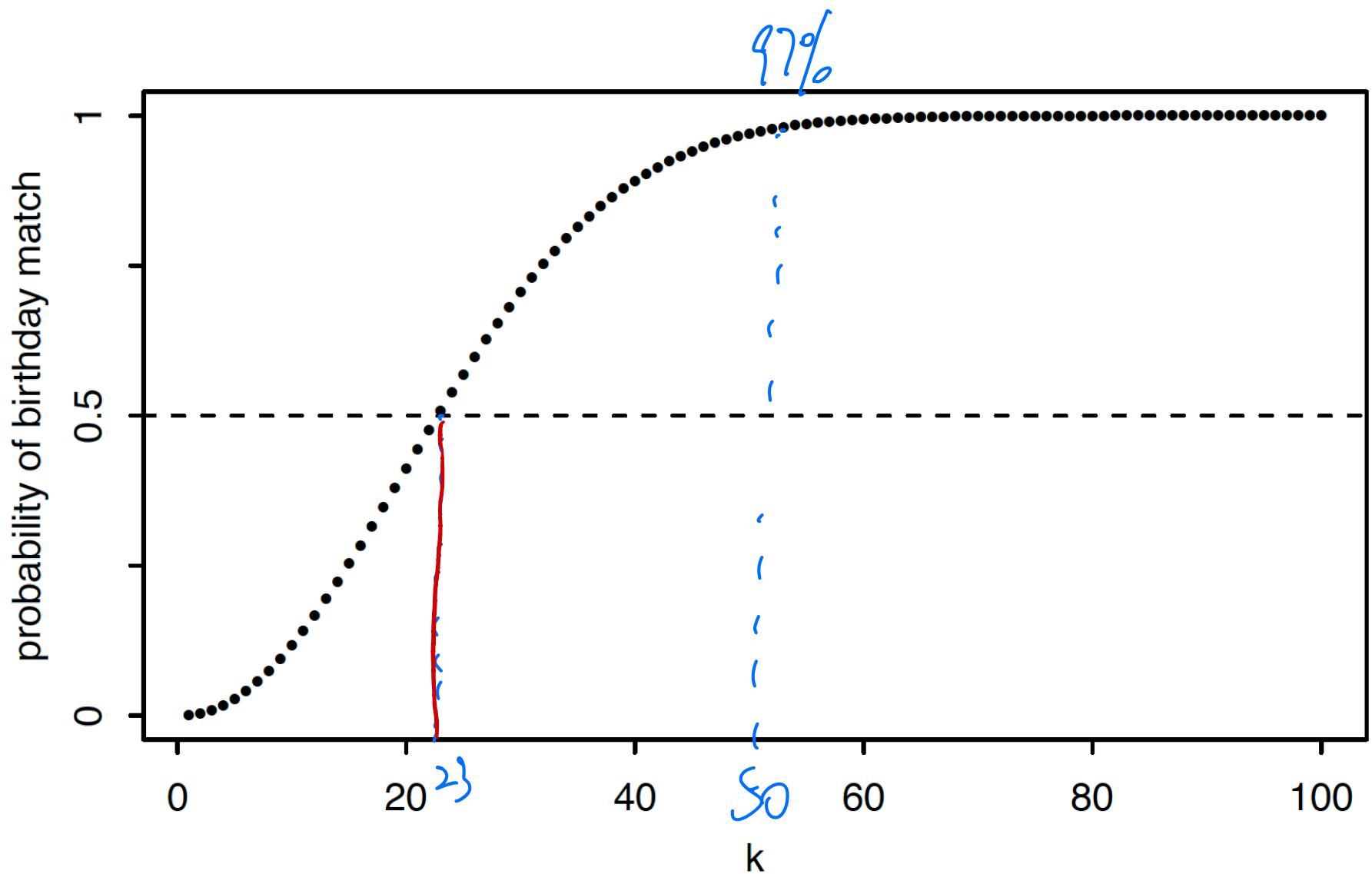
$$P(A^c) = \frac{\text{# of ways to assign birthdays to } k \text{ people}}{\text{without repetition}}$$

$$= \frac{k\text{-sample of 365 days without replacement}}{k\text{-sample of 365 days with replacement}}$$

$$= \frac{365 \cdot (365-1) \cdot \dots \cdot (365-k+1)}{365^k}$$

$$\underline{P(A)} = 1 - P(A^c)$$

Solution of Birthday Problem



Generalized Birthday Problem

① event A: "at least 2 people have a same value"

A^c : "no one share a same value".

- Each of k people has a random number ("birthday") drawn from n values ("days").
- If the probability that at least two people have the same number is 50%, then $k \approx 1.18\sqrt{n}$.

$$\sqrt{n \cdot 2 \ln 2} \quad \sqrt{2 \ln 2} \approx 1.177$$

$$P(A^c) = \frac{n(n-1) \cdots (n-k+1)}{n^k} = \left(1 - \frac{1}{n}\right) \times \cdots \times \left(1 - \frac{k-1}{n}\right)$$

Generalized Birthday Problem

$$[x] \ll 1, e^{-x} \approx 1-x$$

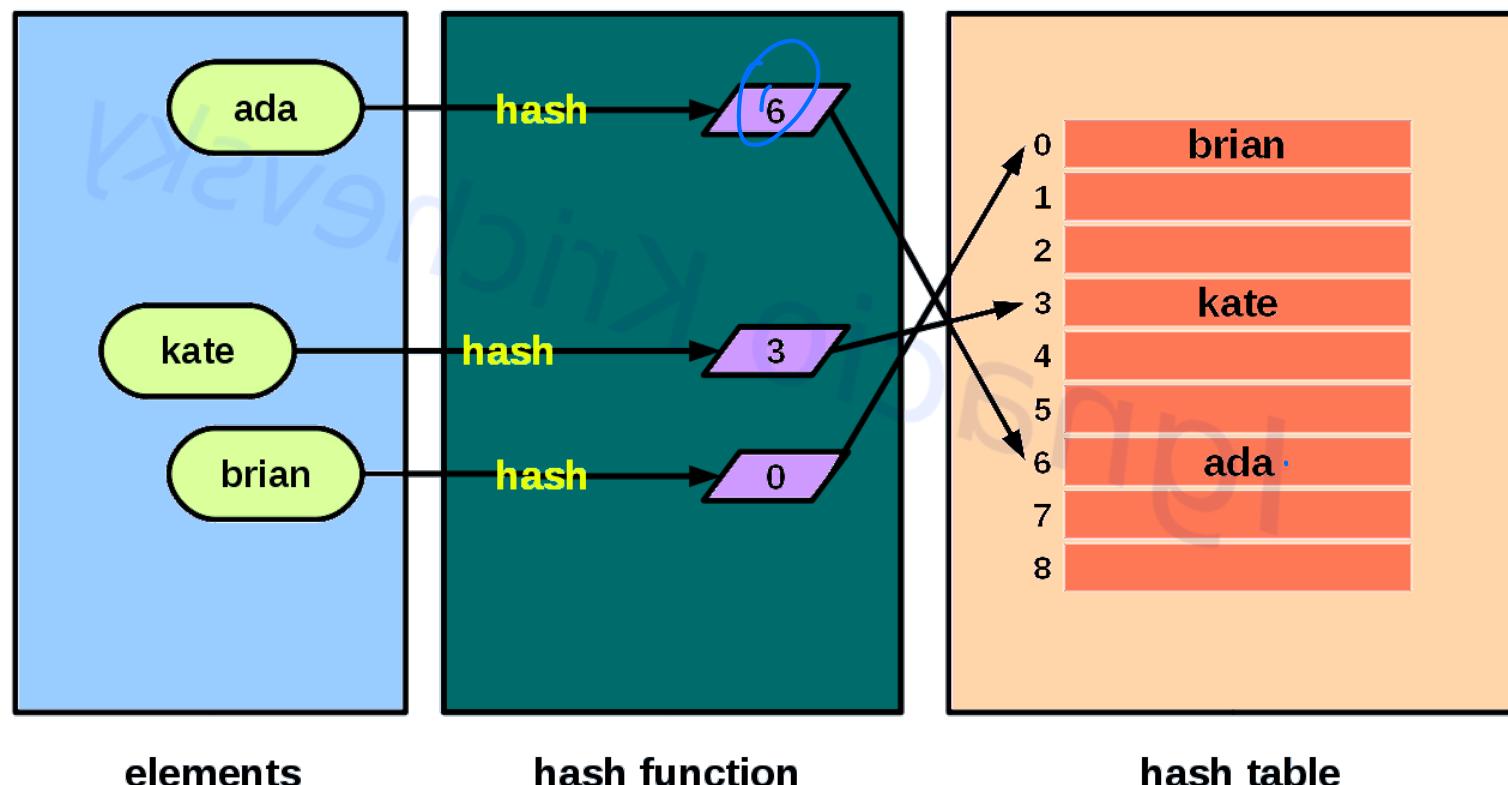
$$\begin{aligned}
 P(A^c) &= 1 \times \left(1 - \frac{1}{n}\right) \times \left(1 - \frac{2}{n}\right) \times \cdots \times \left(1 - \frac{k-1}{n}\right) \\
 &\approx e^{-\frac{1}{n}} \cdot e^{-\frac{2}{n}} \cdot \cdots \cdot e^{-\frac{k-1}{n}} \\
 &= \exp\left(-\frac{1}{n} - \frac{2}{n} - \cdots - \frac{k-1}{n}\right) \\
 &= \exp\left[-\frac{k(k-1)}{2n}\right] \approx \exp\left(-\frac{k^2}{2n}\right)
 \end{aligned}$$

$$P(A) = 0.5, \quad P(A^c) = 0.5 \Rightarrow e^{-\frac{k^2}{2n}} = 0.5$$

$$k = \sqrt{n \cdot 2 \ln 2} \approx 1.18\sqrt{n}$$

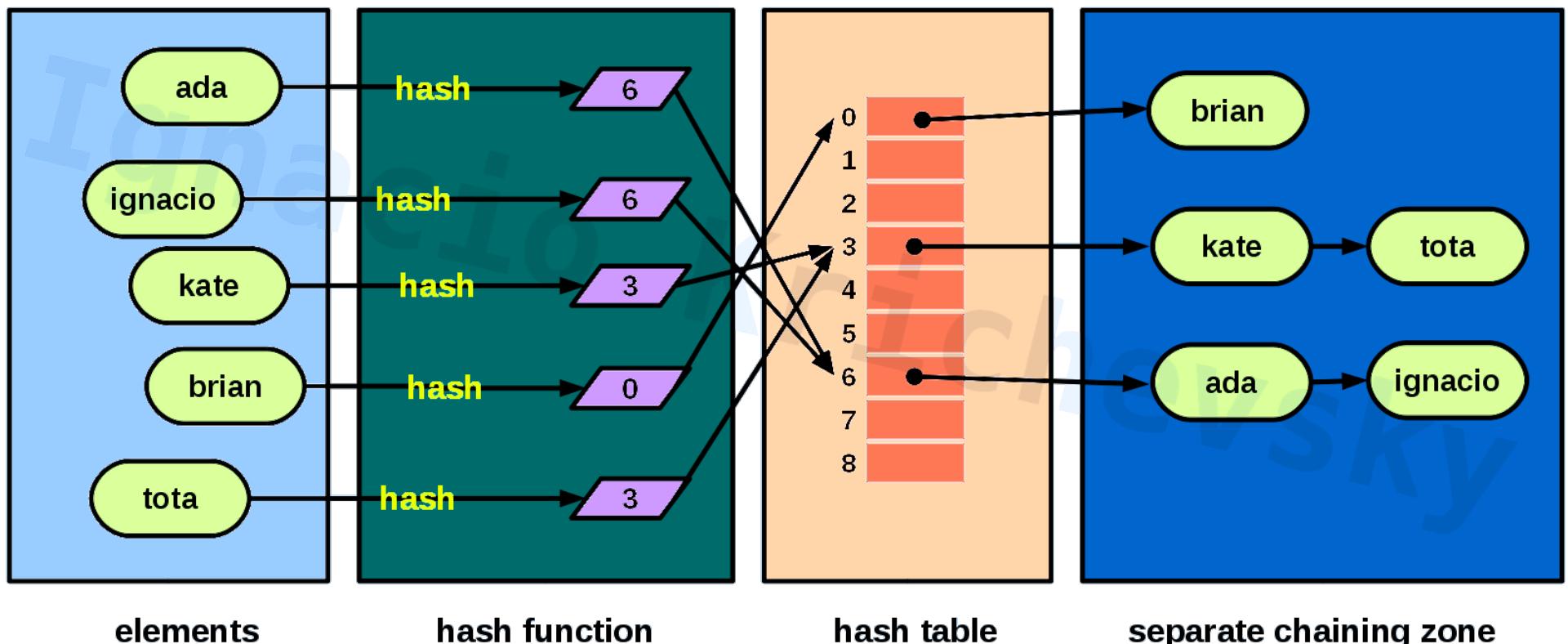
Application: Hash Table

- A commonly used data structure for fast information retrieval.
- Example: store people's name. For each people x , a hash function h is computed.
- $h(x)$: the location that will be used to store x 's name.



Hash Collision

- Collision: $x \neq y$, but $h(x) = h(y)$. (≥ 1 locations has ≥ 2 names stored there)
- Given k people (different names) and n locations, what is the probability of occurrence of hash collision?



Solution of Hash Collision

$$k \leq n, \quad P(\text{"hash collision"}) = 1 - \frac{n(n-1) \cdots (n-k+1)}{n^k}$$

$$\approx 1 - \boxed{e^{-\frac{k^2}{2n}}}$$

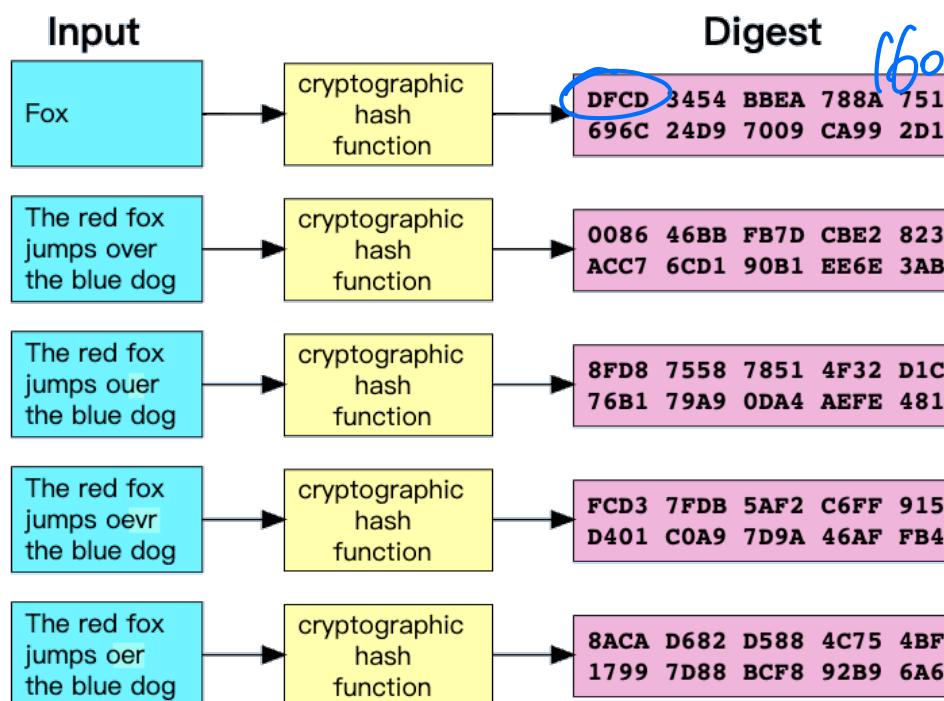
Application: Cryptographic Hash Function

- A map which “scrambles” long strings (message) into m -bit “hashes” (digest).
- Example 1: MD (Message-Digest Algorithm) 5 (bittorrent) with $m = 128$.
- Example 2: SHA (Secure Hash Algorithm)-1 (SSL, PGP) with $m = 160$.

$4 \times 4 \times 10 = 160$ byte

(60 bits)

SHA-1



Cryptographic Hash Function

- A good cryptographic hash function f has two properties:
 - ▶ Given the hash $f(M)$ of a message string M , it's computationally infeasible to recover M .
 - ▶ It's computationally infeasible to find a “collision”, meaning a pair of distinct messages $M_1 \neq M_2$ such that $f(M_1) = f(M_2)$.

The Birthday Attack

- Suppose we try to “break” a hash function by finding a collision (forged digital signature).
- One method: take a huge number of messages M , hash them all, and hope to find two with the same hash value.
- Now how many messages would you have to try before there was at least a 50% chance of finding two with the same hash?
- $n = 2^m$ and $k \approx \sqrt{n} = 2^{m/2}$. For SHA-1, $k \approx \underline{2^{80}}$.

$$M = 160$$

$$1.18\sqrt{n}$$

$$\underline{n = 2^m}$$

The Birthday Attack

- The birthday attack: trying to find collisions by testing many random messages.
- A cryptographic hash function is broken: when there is a way of finding collisions much faster than the Birthday Attack method.
- SHA-1 is now broken: Xiaoyun Wang find a SHA-1 collision with 2^{69} tests in 2005, then 2^{63} tests later (compared to 2^{80} tests by the birthday attack).
- Now SHA-2 ($m = 256$) and SHA-3 ($m = 512$) are on the way.

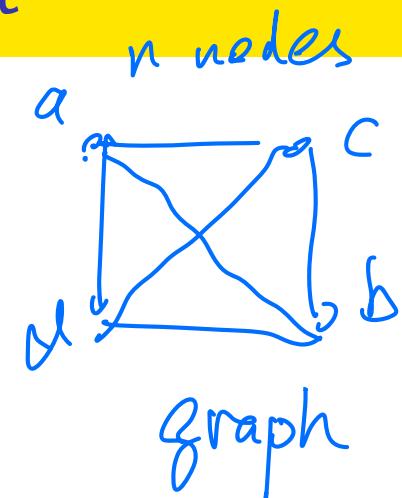
Summary of Counting

Choose k elements from a set with n elements (choose k objects out of n distinguishable objects), the number of possible ways:

	Order Matters	Order Not Matter
with replacement	n^k	
without replacement	$n(n - 1) \cdots (n - k + 1)$?

Unordered Sampling without Replacement

$$\frac{n(n-1)}{2}$$



$$\frac{n!}{(n-k)! k!}$$

- also called Combination
- k -combination: choose a k -element subset of a set with n elements.

order matters

$$\frac{n!}{(n-k)!}$$

of ways to order k elements

order not matters

$$\underline{k! = k(k-1) \cdots 1}$$

Binomial Coefficient

Definition

For any nonnegative integers k and n , the binomial coefficient $\binom{n}{k}$ (circled) read as "n choose k", is the number of subsets of size k for a set of size n .

Theorem

For $k \leq n$, we have

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Binomial Theorem

Theorem

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

Multinomial Theorem

$$\binom{n}{k} = \binom{n}{d-k}$$

Story proof

A team of n people

$$\frac{k}{\text{group A}} \quad \frac{n-k}{\text{B}}$$

— — — — —

A team with 10 people

$$5 \quad 3 \quad 2$$

$$\binom{10}{5} \cdot \binom{5}{3} \cdot \binom{2}{2}$$

$$= (5, 3, 2)$$

Multinomial Theorem

Theorem

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{n_1, n_2, \dots, n_r \geq 0} \frac{n!}{n_1! n_2! \cdots n_r!} x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r},$$

where $n_1 + n_2 + \cdots + n_r = n$.



$$\begin{aligned}
 & C_n^{n_1} \cdot C_{n-n_1}^{n_2} \cdot C_{n-n_1-n_2}^{n_3} \cdots \cdot C_{n-n_1-n_2-\cdots-n_{r-1}}^{n_r} \\
 &= \frac{n!}{(n-n_1)! n_1!} \cdot \frac{(n-n_1)!}{(n-n_1-n_2)! n_2!} \cdot \frac{(n-n_1-n_2)!}{(n-n_1-n_2-n_3)! \cdots n_3!} \cdots \\
 &= \frac{n!}{n_1! n_2! \cdots n_r!}
 \end{aligned}$$

Story Proof: The Team Captain

1. a group of n people

2. choose k of them to form a team.

3. one of the team is assigned as the Captain.

For any positive integers n and k with $k \leq n$,

左: 选一个组长 $\binom{n}{1}$
选 $k-1$ 个人 $\binom{n-1}{k-1}$

$$\underbrace{n \binom{n-1}{k-1}}_{\text{L: choose a captain first, } n} = \underbrace{k \binom{n}{k}}_{\text{R: choose the team first } \binom{n}{k}}$$

右: 选 k 个人 $\binom{n}{k}$
选组长 $\binom{1}{k}$

L: choose a captain first, n

R: choose the team first $\binom{n}{k}$

choose the residual $(k-1)$ $\binom{n-1}{k-1}$
from $(n-1)$ people.

choose a captain from k
the team

Story Proof: Vandermonde's Identity 范德蒙恒等式

group A: m people

group B: n people

whole group: $A \cup B$

$m+n$ people

A famous relationship between binomial coefficients, called *Vandermonde's identity*, says that

$$\text{A, B 2组, 选 } k \text{ 个人完成工作} \quad \binom{m+n}{k} = \sum_{j=0}^k \binom{m}{j} \binom{n}{k-j}.$$

left: choose k from
the whole group

→ A组出 j 个人
B组出 $k-j$ 个人

Summary of Counting

order with rep. $\begin{array}{c} r \\ n \end{array} \times \begin{array}{c} r \\ n \end{array} \times \cdots \times \begin{array}{c} r \\ n \end{array} = n^k$

order without rep. $n \times n-1 \times \cdots \times n-k+1 \times \frac{n!}{(n-k)!}$

Choose k elements from a set with n elements (choose k objects out of n distinguishable objects), the number of possible ways:

	Order Matters	Order Not Matter
with replacement	n^k	?
without replacement	$n(n-1)\cdots(n-k+1)$	$\binom{n}{k}$

unorder without rep.

$$\frac{n!}{(n-k)! k!}$$

Unordered Sampling with Replacement

$$n=3, \{a,b,c\}, k=2$$

$$\underbrace{\{a,b,c,\dots\}}_n \binom{k+n-1}{n-1} = \binom{k+n-1}{k}$$

$$\{a,a\}, \{a,b\}, \{a,c\}, \{b,b\}, \{b,c\}, \{c,c\}$$

$$\Rightarrow x_1 + x_2 + \dots + x_n = k \quad x_i \geq 0$$

- How many ways are there to choose k times from a set of n objects with replacement, if order doesn't matter (we only care about how many times each object was chosen, not the order in which they were chosen)?
- also called "Bose-Einstein Counting".

x_1 : # of a chosen.
 x_2 : ... b ...
 x_3 : ... c ...

$$\begin{aligned} \{a,a\}_r &: (x_1, x_2, x_3) = (2, 0, 0), \\ \{a,b\} &: (x_1, x_2, x_3) = (1, 1, 0) \\ &\dots \end{aligned}$$

$$x_1 + x_2 + x_3 = 2$$

Equivalent Problem

γ_i : # of i-th object selected. ($1 \leq i \leq n$)

$$\gamma_1 + \gamma_2 + \dots + \gamma_n = k, \quad \gamma_i \geq 0, \forall i.$$

$(\gamma_1, \gamma_2, \dots, \gamma_n)$ non-negative integer solution

Equivalent Problem

$\text{D}_k \cap \text{D}_l \cap \text{D}_m \cap \dots \cap \text{D}_r$

Theorem

There are $\binom{r-1}{n-1}$ distinct **positive** integer-valued vectors (x_1, x_2, \dots, x_n) satisfying the equation

$$\underline{x_1} + \underline{x_2} + \dots + \underline{x_n} = \underline{r}, \quad x_i > 0, \quad i = 1, 2, \dots, n.$$

$$\begin{array}{ll} r-1 & \text{spaces} \\ n-1 & \text{bars} \end{array} \quad \binom{r-1}{n-1}$$

Bose-Einstein Counting

Def: $y_i = \lfloor t x_i \rfloor$. ($x_i \geq 0$)

$$\sum_{i=1}^n y_i = k + n = r \quad \text{positive solutions}$$

Theorem

There are $\binom{n+k-1}{n-1}$ distinct **nonnegative** integer-valued vectors (x_1, x_2, \dots, x_n) satisfying the equation

$$x_1 + x_2 + \cdots + x_n = k, x_i \geq 0, i = 1, 2, \dots, n.$$

$$\binom{k+n-1}{n-1}$$

Example

$$\text{Def: } y_1 = x_1 - 2 \geq 1. \quad y_4 = x_4 - 9 \geq 1.$$

$$y_2 = x_2 - 4 \geq 1$$

$$y_3 = x_3 - 7 \geq 1$$

How many distinct **positive** integer-valued vectors (x_1, x_2, x_3, x_4) satisfying the equation

$$x_1 + x_2 + x_3 + x_4 = 88, \text{ where } x_1 \geq 3, x_2 \geq 5, x_3 \geq 8, x_4 \geq 10.$$

$$y_1 + y_2 + y_3 + y_4 = 88 - 2 - 4 - 7 - 9 = 66$$

$$\binom{66-1}{4-1} = \binom{65}{3}$$

Solution

Example: Multinomial Expansion

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{n_1, n_2, \dots, n_r \geq 0} \frac{n!}{n_1! n_2! \cdots n_r!} x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$$

$n_1 + n_2 + \cdots + n_r = n$

How many terms are there in the multinomial expansion of $(x_1 + x_2 + \cdots + x_r)^n$?

$$\sum_{\substack{n_1 + n_2 + \cdots + n_r = n \\ n_1 \geq 0, \dots, n_r \geq 0}} \frac{n!}{n_1! n_2! \cdots n_r!} x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$$

$$\binom{n+r-1}{r-1}$$

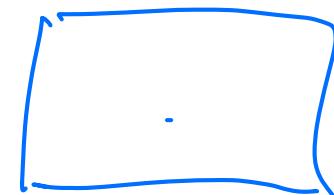
Example: Multinomial Expansion

Summary of Counting

Choose k elements from a set with n elements (choose k objects out of n distinguishable objects), the number of possible ways:

	Order Matters	Order Not Matter
with replacement	n^k	$\binom{n+k-1}{k}$
without replacement	$n(n - 1) \cdots (n - k + 1)$	$\binom{n}{k}$

Outline



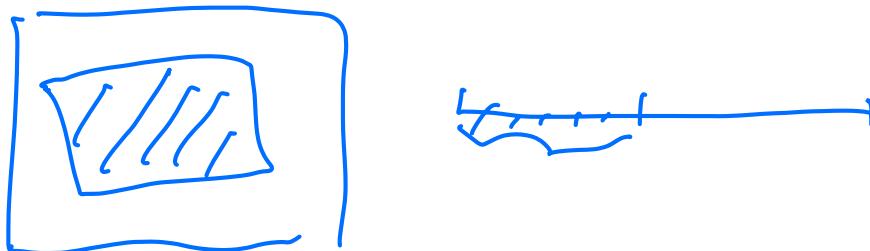
1 Probabilistic Model

2 Naive Definition of Probability & Counting

3 Other Non-Axiomatic Definitions of Probability

4 Axiomatic Definition of Probability

Geometric Probability: Infinite Sample Space



- Geometric probability is a tool to deal with the problem of infinite outcomes by measuring the number of outcomes geometrically, in terms of geometric measure such as length, area, or volume.
- Equally likely means the probability of falling into some geometric region is proportional to the measure of such region including length, area, or volume.
- Given a sample space S , the probability of event A occurring is $P(A) = \frac{M(A)}{M(S)}$, where $M(\cdot)$ is the measure of geometric region.

Example: 1-dimensional Geometric Probability

$$|x-0| > |x-1|, \quad 0 \leq x \leq 3.$$

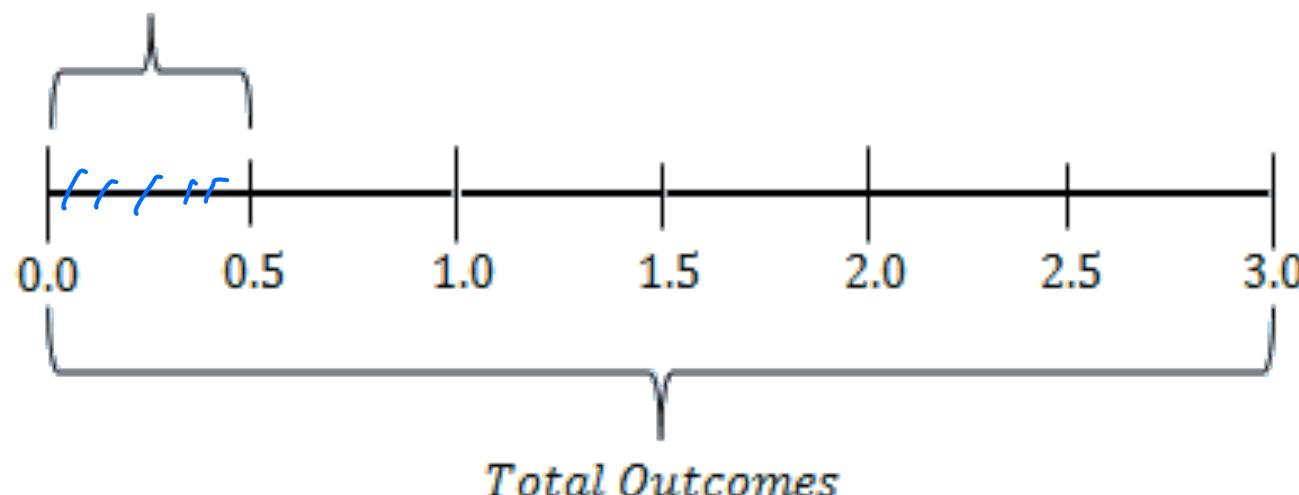
$$0 \leq x < 0.5$$

X is a random real number between 0 and 3. What is the probability that X is closer to 0 than it is to 1?

Solution

$$P(A) = \frac{M(A)}{M(S)} = \frac{\text{Desired Outcomes}}{\text{Total Outcomes}} = \frac{1}{3}.$$

Desired Outcomes



Example: 1-dimensional Geometric Probability

$$\mathcal{M}(\Omega) = 1 \quad \mathcal{M}(A) = 0 \quad P(A) = \frac{\mathcal{M}(A)}{\mathcal{M}(\Omega)} = 0.$$

X is a random real number between 1 and 2. What is the probability that X is equal to 1.5?

$A = \emptyset$, impossible $\Rightarrow P(A) = 0$.

$P(A) = 0$. $\boxed{\cancel{A \neq \emptyset}}$ $A \neq \emptyset$. $A = \{x=1.5\}$.

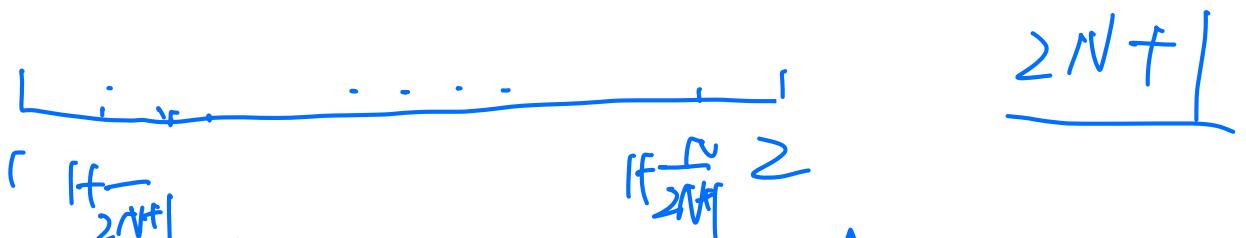
$A^c \neq \Omega$

$P(A^c) = 1$

$P(A^c) = 1$

$\Omega = \{X \in [1, 2]\}$

Solution



$$\textcircled{1} \quad \left(1 + \frac{1}{2N+1}\right), \left(1 + \frac{1}{2N+1}, \frac{2}{2N+1}\right), \dots, \left(\frac{2N}{2N+1} + 1, 2\right). \quad (\epsilon_1 = \frac{1}{2N+1})$$

$$\textcircled{2} \quad P(A_1) = P(A_2) = \dots = P(A_{2N+1}) = \frac{1}{2N+1}$$

$$1.5 \in \left(1 + \frac{N}{2N+1}, 1 + \frac{N+1}{2N+1}\right) = A_{N+1}$$

Q.E.D. $P(X=1.5) \leq P(A_{N+1}), \quad \forall N.$

$$\frac{1}{2N+1}$$

$$N \rightarrow +\infty \quad P(A_{N+1}) \geq 0$$

Example: 2-dimensional Geometric Probability

A point is chosen uniformly at random in the square. What is the probability that it will land within the circle?

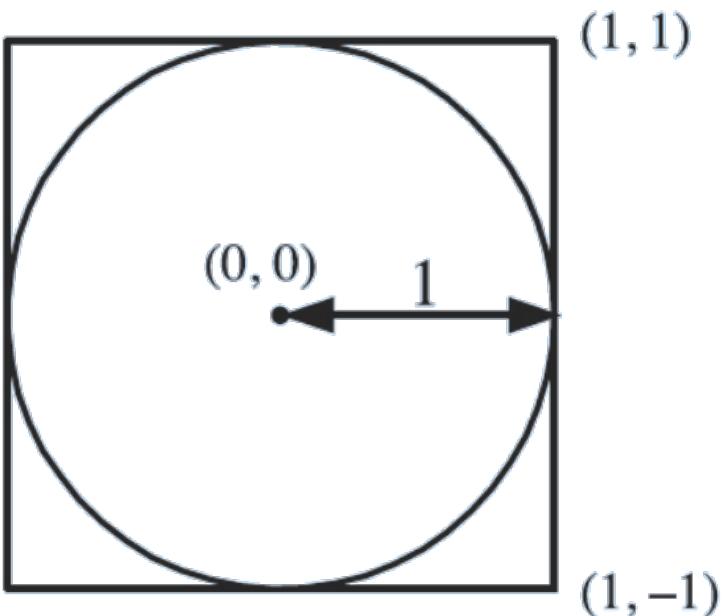
$$M(S) = 4.$$

$$(-1, 1)$$

$$A : \{(x,y) \mid x^2 + y^2 \leq 1\}$$

$$M(A) = \pi \cdot r^2 = \pi r.$$

$$P(A) = \frac{MCA}{MS} = \frac{1}{4} (-1, -1)$$



Solution

Probability: A Statistical Definition

- The frequentist view: probability represents a long-run frequency over a large number of repetitions of an experiment.
- If we say a coin has probability $1/2$ of Heads, that means the coin would land Heads 50% of the time if we tossed it over and over and over.
- However, the frequency may not exist in general.
- Now as the intuition behind the Monte Carlo Computing Method.

Probability: A Subjective Definition

- Probability represents a degree of belief about the event in question.
- So we can assign probabilities to hypotheses like “candidate A will win the election” or “the defendant is guilty” even if it isn’t possible to repeat the same election or the same crime over and over again.
- Related to Logic, Philosophy, and Psychology.

Outline

- 1 Probabilistic Model
- 2 Naive Definition of Probability & Counting
- 3 Other Non-Axiomatic Definitions of Probability
- 4 Axiomatic Definition of Probability

Axioms for Events

公理



Definition

Given a sample space S , the class of subsets of S that constitute the set of events satisfies the following axioms:

- ① S is an event.
- ② For every event A , the complement A^c is an event.
- ③ For every sequence of events A_1, A_2, \dots , the union $\bigcup_{j=1}^{\infty} A_j$ is an event.

$$A \cap B = \overline{A^c \cup B^c}$$

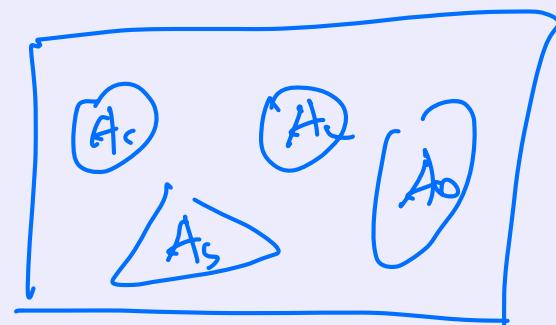
General Definition of Probability

Definition

A *probability space* consists of a sample space S and a probability function P which takes an event $A \subseteq S$ as input and returns $P(A)$, a real number between 0 and 1, as output. The function P must satisfy the following axioms:

- ① $P(\emptyset) = 0, P(S) = 1.$
- ② If A_1, A_2, \dots are disjoint events, then
互斥

$$P\left(\bigcup_{j=1}^{\infty} A_j\right) = \sum_{j=1}^{\infty} P(A_j).$$



(Saying that these events are disjoint means that they are mutually exclusive: $A_i \cap A_j = \emptyset$ for $i \neq j$.)

Properties of Probability

$$\textcircled{1} P(A \cup A^c) = P(S) = 1$$

[
P(A) + P(A^c)]

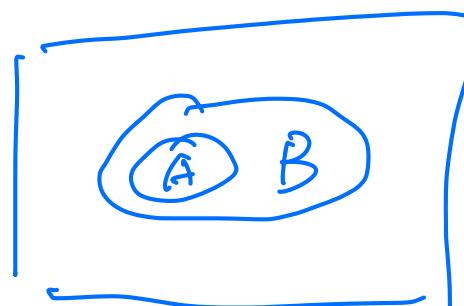
$$\textcircled{2} \quad B = A \cup (B \cap A^c)$$

$$P(B) = P(A) + \underline{P(B \cap A^c)}.$$

Q.E.D

Probability has the following properties, for any events A and B :

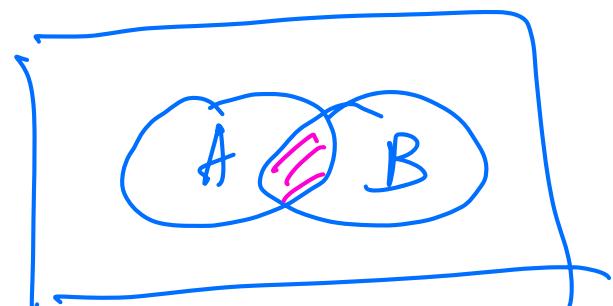
- ① $P(A^c) = 1 - P(A).$
 - ② If $A \subseteq B$, then $P(A) \leq P(B).$
 - ③ $P(A \cup B) = P(A) + P(B) - P(A \cap B).$



$$\textcircled{3} \quad A \cup B = A \cup \underline{(A^c \cap B)}$$

$$(A^c \cap B) \cup (A \cap B) = B$$

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



Example: Bonferroni's Inequality

$$A^c = \bar{A}$$

$$\Leftrightarrow 1 - P(A_1 \cap A_2 \cap \dots \cap A_n) \leq [1 - P(A_1)] + [1 - P(A_2)] + \dots + [1 - P(A_n)] - (n-1)$$

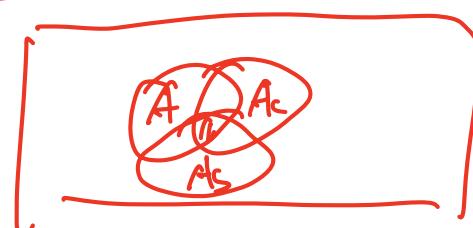
$$\Leftrightarrow P(\overline{A_1 \cap A_2 \cap \dots \cap A_n}) \leq [1 - P(A_1)] + [1 - P(A_2)] + \dots + [1 - P(A_n)]$$

Theorem

For any n events A_1, \dots, A_n , we have

$$P(A_1 \cap A_2 \cap \dots \cap A_n) \geq P(A_1) + P(A_2) + \dots + P(A_n) - (n-1).$$

$$\Leftrightarrow P(\overline{A_1 \cup A_2 \cup \dots \cup A_n}) \leq P(\bar{A}_1) + P(\bar{A}_2) + \dots + P(\bar{A}_n). \quad \text{✗}$$



Proof

Example: Boole's Inequality

$$1. \bar{A}_1 \cup A_2 = A_1 \cup (\bar{A}_1 \cap A_2)$$

$$2. \bar{A}_1 \cup \bar{A}_2 \cup A_3 = A_1 \cup (\bar{A}_1 \cap A_2) \cup (A_3 \cap \overline{\bar{A}_1 \cup A_2})$$

Theorem

For any events A_1, A_2, \dots , we have

$$P(\bigcup_{i=1}^{\infty} A_i) \leq \sum_{i=1}^{\infty} P(A_i).$$

$$3. A_1 \cup A_2 \cup \cdots \cup A_n = A_1 \cup (A_2 \cap \overline{A_1}) \cup (A_3 \cap \overline{A_1 \cup A_2})$$

$$\begin{aligned} & \cdots \cup (A_n \cap \overline{A_1 \cup A_2 \cup \cdots \cup A_{n-1}}) \\ &= A_1 \cup \bigcup_{i=2}^n (A_i \cap \overline{\bigcup_{j=1}^{i-1} A_j}) \end{aligned}$$

Proof

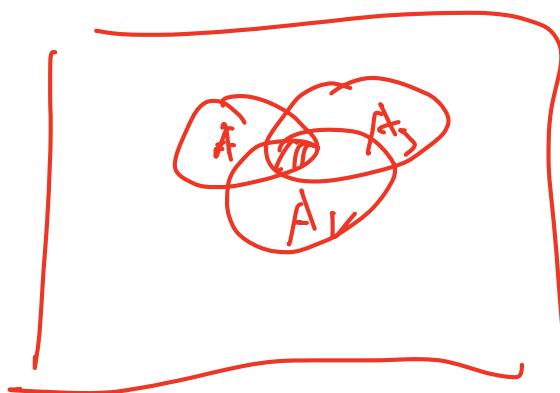
$$\begin{aligned} P\left(\bigcup_{i=1}^{\infty} A_i\right) &= P(A_r) + \sum_{i=2}^{\infty} P\left(A_i \cap \overline{A_r \cup A_2 \cup \dots \cup A_{i-1}}\right) \\ &\leq P(A_r) + \sum_{i=2}^{\infty} P(A_i). \end{aligned}$$

$\overbrace{\quad}^{\wedge i}$

$$\begin{aligned} A_i^- &= \left(A_i \cap \overline{\bigcup_{j=1}^{i-1} A_j} \right) \\ &\cup \left(A_i \cap \left(\bigcup_{j=1}^{i-1} A_j \right) \right) \end{aligned}$$

Inclusion-Exclusion Formula

容斥原理



For any events A_1, \dots, A_n :

$$\begin{aligned}
 p\left(\bigcup_{i=1}^n A_i\right) = & \underbrace{\sum_i P(A_i)}_{\text{Red line}} - \underbrace{\sum_{i < j} P(A_i \cap A_j)}_{\text{Blue line}} + \sum_{i < j < k} P(A_i \cap A_j \cap A_k) \\
 & + \cdots + (-1)^{n+1} P(A_1 \cap \cdots \cap A_n).
 \end{aligned}$$

Example: De Montmort's Matching Problem

$A_i = \text{"i-th card has the number } i\text{"}$

A_i : 第*i*张牌是*i*

B : win

$$B = \bigcup_{i=1}^n A_i$$

$$B = \bigcup_{i=1}^n A_i$$

Consider a well-shuffled deck of n cards, labeled 1 through n . You flip over the cards one by one, saying the numbers 1 through n as you do so. You win the game if, at some point, the number you say aloud is the same as the number on the card being flipped over (for example, if the 7th card in the deck has the label 7). What is the probability of winning?

$$P(B) = P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i) - \sum_{1 \leq i < j \leq n} P(A_i \cap A_j) + \dots$$

$$P(A_i) = \frac{1}{n} = \frac{(n-1)!}{n!}$$

Solution

Solution

Summary 1: Events & Numbers

What can happen?

events

A

not A

A and B

A or B

something happened

$$\xrightarrow{P}$$



numbers

$$P(A)$$

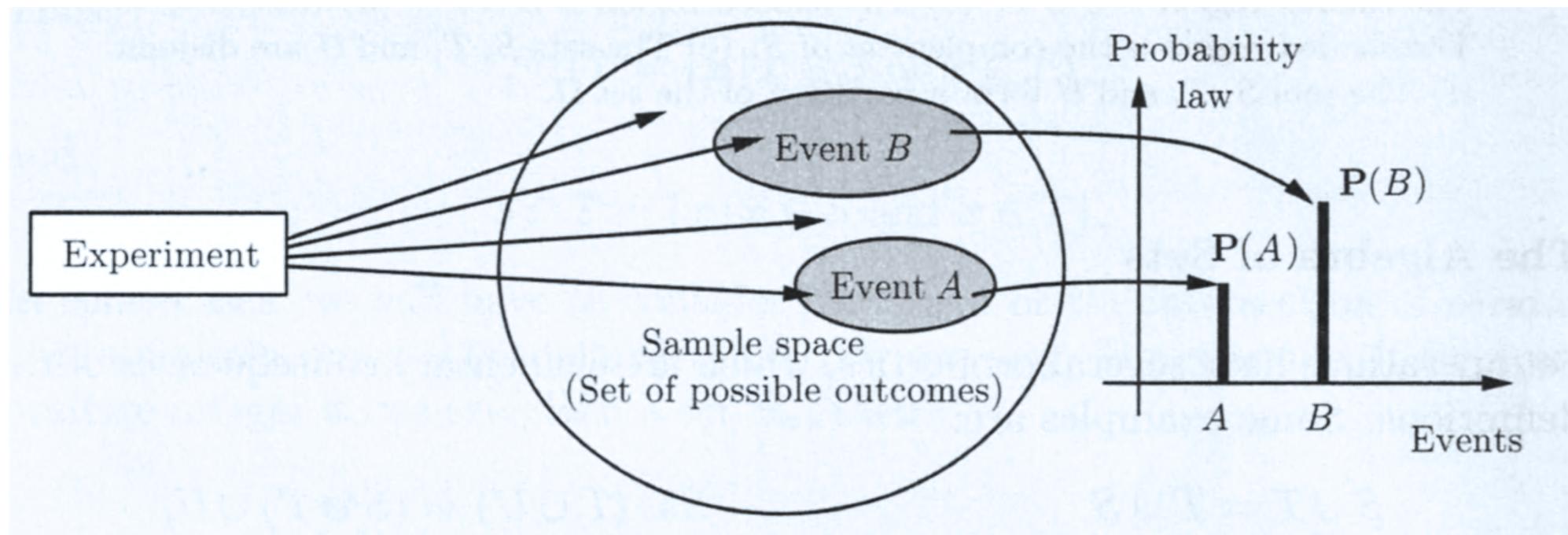
$$P(A^c) = 1 - P(A)$$

$$P(A \cap B)$$

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

$$P(S) = 1$$

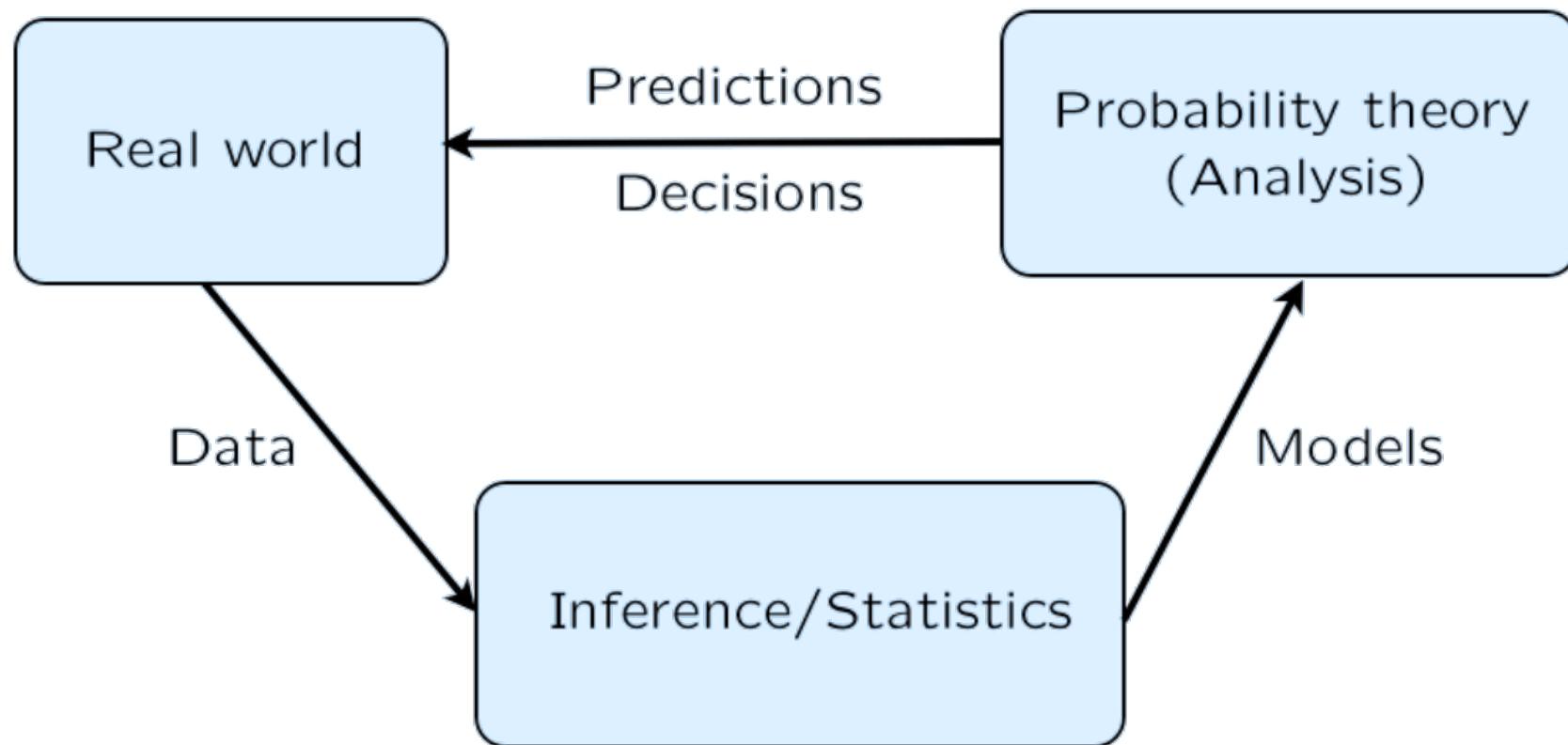
Summary 2: Probability Space



Summary 3: The Role of Probability & Statistics

A framework for analyzing phenomena with uncertain outcomes:

- Rules for consistent reasoning.
- Used for predictions and decisions.



References

- Chapter 1 of **BH**
- Chapter 1 of **BT**