



SHANDONG UNIVERSITY
山东大学

第一章 随机事件及其概率

孙玲

网络空间安全学院

2022 年 9 月 5 日



lingsun@sdu.edu.cn



概率论与数理统计 0/19



课件符号说明

概念/定义

- ▶ 概念/定义的内容.

性质/定理等

- ▶ 需要重点关注的性质/定理等内容.

统一书写格式

- ▶ 统一书写格式.

例题

- ▶ 例题.

补充内容

- ▶ 与课程相关的补充内容.



第一章 随机事件及其概率

确定性现象

- ▶ 一定条件下**必然发生**或**绝不可能发生**的现象.
 - ▶ 例 1: 在 1 个标准大气压下把水加热到 100°C 时必然会沸腾.
 - ▶ 例 2: 在不受外力作用的条件下, 作等速直线运动的物体改变其等速直线运动状态是不可能的 (牛顿第一定律).

随机现象

- ▶ 在相同的条件下可能发生也可能不发生, 或者说, 可能出现这个结果, 也可能出现那个结果, 呈现出偶然性, 此类现象称为**随机现象**.
 - ▶ 例 1: 在落地之前, 抛一枚硬币究竟是正面朝上还是反面朝上是无法提前判定的.
 - ▶ 例 2: 同一门炮向同一目标发射多发同种炮弹, 弹落点也不一样, 一部分原因是炮弹制造时种种偶然因素对炮弹质量有影响.

◀ 前往弹坑原理

◀ 前往统计规律性



第一章 随机事件及其概率

弹坑原理

- ▶ 有战斗经验的老兵，在炮火连天的战场为了隐蔽自己，往往会跳进刚刚炸开的弹坑里，因为下一发炮弹，不容易落在同一点上，所以新弹坑是安全的。
 - ▶ 即使是用同样的发射器同样的动能在同一点将炮弹推出，还得考虑两次射击风速风向是不是完全一样（完全一样可能性太小了），只有完全一样的时候才是同一地点。
 - ▶ 两颗炮弹落到同一地点的几率非常小。 ◀ 返回随机现象





第一章 随机事件及其概率

统计规律性

在个别观察试验中呈现不确定的结果, 而在相同条件下, 大量重复试验, 试验结果呈现出的规律性称为**统计规律性**.

- ▶ 例 1: 大量重复抛掷同一枚硬币时正面朝上的次数约占抛掷总数的一半.
- ▶ 例 2: 衣服和用具总是在同样部位以相似的方式破损.
- ▶ 例 3: 下雨时地面各处总是差不多同时淋湿.

概率论与数理统计

- ▶ 概率论与数理统计是探究**随机现象统计规律性**的一门数学学科, 在自然科学、工程技术和社会科学有许多领域中有着重要的应用.

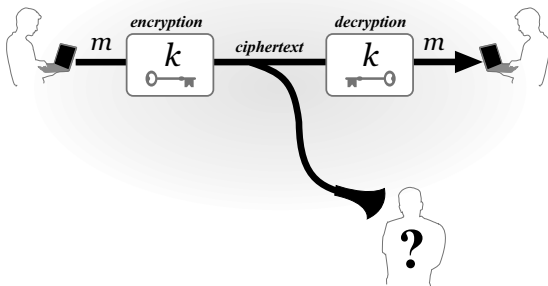
[◀ 前往密码分析](#)[◀ 前往机器学习](#)[◀ 前往 §1.1](#)



概率论在古典密码分析中的应用

密码学简介

- ▶ 从某种意义上来说, 战争是促进科技发展最有效的催化剂.
- ▶ 纵观整个历史进程, 每一次战争之后都会带来科技的快速飞跃, 密码的产生和发展都与战争有着千丝万缕的关系.
- ▶ 自从有了战争, 人类就产生了对安全通信的需求, 密码也在这种背景下应运而生.





概率论在古典密码分析中的应用

密码学简介

- ▶ 密码的使用最早可追溯到公元前 400 多年, 密码学的发展大致经历了四个阶段.
- ▶ **密码学发展的前夜时期 (古代 ~ 1948 年)**
 - ▶ 这一阶段密码的分析与设计没有严谨的数学理论支持.
 - ▶ 密码研究人员凭借自己的直觉和经验进行研究.
 - ▶ 这一阶段出现了一些比较经典的古典密码, 如: 凯撒 (Caesar) 密码和维吉尼亚 (Vigenère) 密码等.

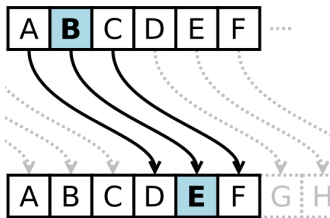




概率论在古典密码分析中的应用

凯撒密码 (Caesar Cipher)

- 密码学中，**凯撒密码**是一种最简单且最广为人知的加密技术。
- 它是一种替换加密的技术，明文中的所有字母都在字母表上向后/向前按照一个固定数目进行偏移后被替换成密文。
- 这个加密方法是以罗马共和时期凯撒的名字命名的，当年凯撒曾用此方法与其将军们进行联系。



- 例：APPLE → DSSOH.



概率论在古典密码分析中的应用

凯撒密码的破解

- ▶ 需要考虑两种情况：
 1. 攻击者知道/猜测密码中使用了某个简单的替换加密方式，但是不确定是凯撒密码。
 2. 攻击者知道/猜测使用了凯撒密码，但是不知道其偏移量。
- ▶ 对于第二种情况，解决方法更加简单。由于使用凯撒密码进行加密的语言一般都是字母文字系统，因此密码中可能是使用的偏移量也是有限的，因而可以使用**穷尽搜索**的方法。
- ▶ 对于第一种情况，可以首先采用**频率分析法**来确定所使用的加密方式是否为凯撒密码。

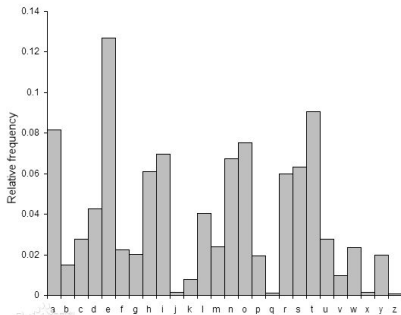




概率论在古典密码分析中的应用

频率分析法

- ▶ 当密文长度足够大的情况下, 可以先分析密文中每个字母出现的频率, 然后将这一频率与正常情况下的该语言字母表中所有字母的出现频率做比较.
- ▶ 例如在英语中, 正常明文中字母 E 和 T 出现的频率特别高, 而字母 Q 和 Z 出现的频率特别低.





概率论在古典密码分析中的应用

频率分析法

- ▶ 有时还可以将频率分析从字母推广到单词.
 - ▶ 例如英语中, 出现频率最高的单词是: the, of, and, a, to, in... 我们可以通过将最常见的单词的所有可能的 25 组密文, 编组成字典, 进行分析. 比如 QEB 可能是 the, MPQY 可能是单词 know.
- ▶ 频率分析也有其局限性, 它对于较短或故意省略元音字母或者其他缩写方式写成的明文加密出来的密文进行解密并不适用.





k -近邻算法 (k -Nearest Neighbor, KNN)

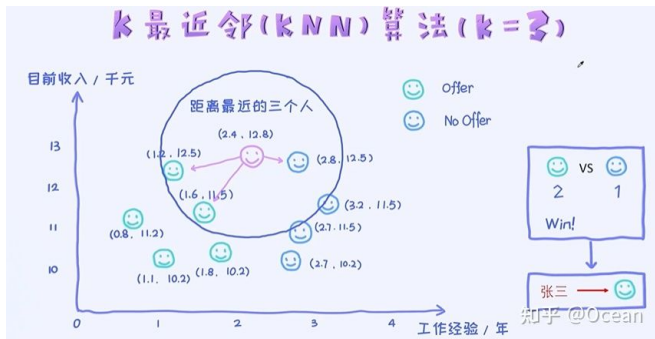
- ▶ 存在一个样本数据集合, 也称之为**训练样本集** (Training Set), 并且样本集中每个数据都存在**标签** (Label), 即我们知道样本集中每一个数据与所属分类的对应关系.
- ▶ 输入没有标签的**新数据** (Test Set) 后, 将新数据的每个特征与样本集中数据对应的特征进行比较, 然后算法提取样本最相似数据 (最近邻) 的分类标签.
- ▶ 一般来说, 我们只选择样本数据集中前 k 个最相似的数据, 这就是 k -近邻算法中 k 的出处, 通常 k 是不大于 20 的整数.
- ▶ 最后, 选择 k 个最相似数据中**出现次数最多的分类**作为新数据的分类.



概率论与机器学习

k-近邻算法示例

- ▶ 给定一些已经知道标签的样本（是否有 offer）。
- ▶ 判断张三是否有 offer。





§1.1 随机事件及其运算

本节主要内容

1. 随机试验与样本空间 [◀ 前往知识点](#)
2. 随机事件 [◀ 前往知识点](#)
3. 事件间的关系与运算 [◀ 前往知识点](#)

[◀ 前往 §1.2](#)





1. 随机试验与样本空间

试验

- ▶ 为了确定随机现象的规律性, 需要进行多次的试验、实验、调查或观察, 我们把这些工作统称为**试验**.

随机试验的三个特征

1. 试验可在相同的条件下重复进行.
 2. 试验的结果不止一个.
 3. 每次试验之前, 不能判定哪一个结果将会出现.
- ▶ 随机试验简称试验, 用 E 表示.

随机试验的例子

- ▶ 掷一枚骰子, 观察出现的点数.
- ▶ 观察日光灯的使用寿命.



1. 随机试验与样本空间

样本点 & 样本空间

- ▶ 试验 E 中的每一个可能的结果称为**基本事件/样本点**.
- ▶ 所有基本事件组成的集合称为试验 E 的**样本空间**, 记为 Ω .

样本空间 - 例 1

- ▶ 在投掷一枚硬币试验中, 共有两种可能的结果: “出现正面”和“出现反面”.
- ▶ 这个试验的样本空间为 $\Omega = \{\text{“出现正面”}, \text{“出现反面”}\}$.

样本空间 - 例 2

- ▶ 投掷一枚骰子, 观察其出现的点数, 所有可能出现的结果有 6 个, 分别是: 出现 1 点、出现 2 点、...、出现 6 点.
- ▶ 样本空间为
$$\Omega = \{\text{“出现 1 点”}, \text{“出现 2 点”}, \dots, \text{“出现 6 点”}\}.$$



1. 随机试验与样本空间

样本点 & 样本空间

- ▶ 试验 E 基本事件/样本点. E 样本空间, Ω .

样本空间 - 例 3

- ▶ 在一批日光灯中任意抽取一只, 测试其寿命, 用 t (单位: 小时) 表示日光灯的使用寿命, 则 t 可取所有非负实数: $t \geq 0$.
- ▶ 样本空间为 $\Omega = \{t \mid t \geq 0\}$.

观测

- ▶ 例 1 和例 2 为离散型样本空间, 例 3 为连续型样本空间.
- ▶ 样本空间应根据随机试验的内容来确定.



2. 随机事件

随机事件

- ▶ 随机试验 E 的样本空间 Ω 中的子集称为试验 E 的**随机事件**，简称**事件**，常用大写英文字母 A, B, C, \dots 表示。
- ▶ **基本事件**是最简单的随机事件。
- ▶ 一般的随机事件由若干个基本事件组成，称为**复合事件**。

随机事件 - 例子

- ▶ 投掷骰子，基本事件有：{出现 1 点}、{出现 2 点}、....
- ▶ 复合事件 {出现偶数点} 由基本事件 {出现 2 点}、{出现 4 点} 和 {出现 6 点} 组成。

统一书写格式

- ▶ 事件使用 $\{***\}$ 或 “***” 表示均可。



2. 随机事件

必然事件

- ▶ 由样本空间中的所有元素组成的集合, 称为**必然事件**, 用 Ω 来表示.

不可能事件

- ▶ 不含任何元素的空集合, 称之为**不可能事件**, 用 \emptyset 来表示.

必然事件 & 不可能事件的例子

- ▶ “掷骰子, 点数不超过 6”是必然事件.
- ▶ “掷骰子, 点数大于 6”是不可能事件.

备注

- ▶ 严格来说, 这两种事件不是随机事件, 但为了后续讨论方便, 仍把必然事件与不可能事件作为随机事件的一种特殊情况来统一处理.



3. 事件间的关系与运算

事件间的 6 种关系

1. 包含.
2. 事件的并.
3. 事件的交.
4. 事件的差.
5. 互不相容事件.
6. 对立事件.

讨论事件间关系的意义

- ▶ 讨论事件间关系有助于更好的理解事件的本质.



3. 事件间的关系与运算

关系 1: 包含

- ▶ 若事件 A 发生必然导致事件 B 发生, 则称事件 B 包含事件 A , 或称事件 A 包含于事件 B 中, 记 $B \supset A$ 或 $A \subset B$.

包含关系 - 性质

- ▶ 必然事件 Ω 包含任何事件 A , 事件 A 包含不可能事件 \emptyset , 即 $\Omega \supset A \supset \emptyset$.
- ▶ 若事件 A 包含事件 B , 且事件 B 也包含事件 A , 即 $A \supset B$ 且 $A \subset B$, 则称事件 A 与事件 B **相等**, 记 $A = B$.





3. 事件间的关系与运算

关系 2: 事件的并

- ▶ 若事件 A 与事件 B 至少有一个发生, 这样构成的事件称为事件 A 与事件 B 的**并事件**, 记 $A \cup B$.

事件的并 - 性质

- ▶ 事件 $A \cup B$ 通常包含三个部分: A 发生而 B 不发生, A 不发生而 B 发生, A 与 B 同时发生.
- ▶ n 个事件 A_1, A_2, \dots, A_n 的并事件为 $A_1 \cup A_2 \cup \dots \cup A_n$.

事件的并 - 例子

- ▶ 10 件产品中有 3 件次品, 从中任取 2 件, 记 $A = \{\text{取到 1 件次品}\}$, $B = \{\text{取到 2 件次品}\}$, 则 $A \cup B = \{\text{至少取到 1 件次品}\}$.



3. 事件间的关系与运算

关系 3: 事件的交

- ▶ 由事件 A 与事件 B 同时发生而构成的事件称为事件 A 与事件 B 的**交事件**, 记 $A \cap B$.

事件的交 - 性质

- ▶ n 个事件 A_1, A_2, \dots, A_n 的交事件为 $A_1 \cap A_2 \cap \dots \cap A_n$.

事件的交 - 例子

- ▶ 10 件产品中有 3 件次品, 从中任取 2 件, 记
 $A = \{\text{取到 1 件次品}\}$, $B = \{\text{取到 2 件次品}\}$,
 $C = \{\text{至多取到 2 件次品}\}$
- ▶ $A \cap B = \emptyset$.
- ▶ $A \cap C = A$.



3. 事件间的关系与运算

关系 4: 事件的差

- ▶ 事件 A 发生而事件 B 不发生, 这样构成的事件称为事件 A 与事件 B 的**差事件**, 记 $A - B$.

事件的差 - 例子

- ▶ 10 件产品中有 3 件次品, 从中任取 2 件, 记
 $A = \{\text{取到 1 件次品}\}$, $B = \{\text{取到 2 件次品}\}$,
 $C = \{\text{至多取到 2 件次品}\}$
- ▶ $C - B = \{\text{至多取到 1 件次品}\}$.





3. 事件间的关系与运算

关系 5: 互不相容事件

- 在一次试验中, 若事件 A 与事件 B 不能同时发生, 即 $A \cap B = \emptyset$, 则称事件 A 与事件 B 为**互不相容事件/互斥事件**.

互不相容事件 - 性质

- n 个事件 A_1, A_2, \dots, A_n , 若他们之间两两互不相容, 则称这 n 个事件是**互不相容的**. 此时, 可记

$$A_1 \cup A_2 \cup \dots \cup A_n = A_1 + A_2 + \dots + A_n = \sum_{i=1}^n A_i.$$

互不相容事件 - 例子

- 投掷骰子, 记 $A = \{\text{出现 3 点}\}$, 记 $B = \{\text{出现 4 点}\}$, 则事件 A 与事件 B 为互斥事件.



3. 事件间的关系与运算

关系 6: 对立事件

- ▶ 在一次试验中, 若事件 A 与事件 B 二者必有一个发生且仅有一个发生, 则称事件 A 与事件 B 为对立事件/互逆事件.
- ▶ 通常把 A 的对立事件记为 \bar{A} , 即 $B = \bar{A}$.
- ▶ \bar{A} 称为 A 的逆事件.

对立事件 - 性质

- ▶ $A \cap \bar{A} = \emptyset$.
- ▶ $A \cup \bar{A} = \Omega$ (与互不相容事件区别).
- ▶ 若事件 A 与事件 B 对立, 则事件 A 与事件 B 互不相容, 反之不成立.

对立事件 - 例子

- ▶ 投掷硬币, 记 $A = \{\text{出现图案}\}$, $B = \{\text{出现数字}\}$, 则事件 A 与事件 B 为对立事件.



3. 事件间的关系与运算

概率论中事件间的关系 & 集合论中集合间的关系

- 形式上具有相似性.

符号	概率论	集合论
Ω	必然事件	全集
\emptyset	不可能事件	空集
A	事件	子集
\bar{A}	A 的对立事件	补集
$A \cup B$	事件的并	并集
$A \cap B$	事件的交	交集
$A - B$	事件的差	差集
$A \cap B = \emptyset$ 互不相容事件 A 与 B 没有公共元素		



3. 事件间的关系与运算

常用的运算律

- 集合论中常用的运算律同样适用于概率论中事件的运算.
1. 交换律: $A \cup B = B \cup A$, $A \cap B = B \cap A$.
 2. 结合律: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$.
 3. 分配律: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
 4. 德摩根 (De Morgan) 定律: $\overline{A \cap B} = \overline{A} \cup \overline{B}$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
对于 n 个事件 A_1, A_2, \dots, A_n , 有

$$\begin{aligned}\overline{A_1 \cup A_2 \cup \dots \cup A_n} &= \overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}, \\ \overline{A_1 \cap A_2 \cap \dots \cap A_n} &= \overline{A_1} \cup \overline{A_2} \cup \dots \cup \overline{A_n}.\end{aligned}$$

常用的运算律 - 例子

- 教材 Page 6 例 1.1.5.



§1.2 随机事件的概率

随机现象数量指标

- ▶ 研究事件出现可能性大小对解决理论和实际问题非常重要。

概率满足的两个要求

- ▶ 事件的**概率**是刻画事件出现的可能性大小的一种数量指标, 这个数量指标应满足以下两个要求:
 1. 它应是事件本身固有的, 不随人的意志而改变的一种客观属性度量.
 2. 它必须符合一般常情, 即事件发生可能性大的, 它的值就大; 事件发生可能性小的, 它的值就小.

本节主要内容

1. 频率与概率
2. 古典概型
3. 几何概型
4. 概率的公理化定义





1. 频率与概率

定义 1.2.1

- ▶ 设在相同的条件下, 进行了 n 次试验, 在这 n 次试验中事件 A 出现了 m 次, 则称

$$f_n(A) = \frac{m}{n} = \frac{\text{事件 } A \text{ 出现的次数}}{\text{试验的总次数}}$$

为随机事件 A 在 n 次试验中出现的**频率**, m 称为**频数**.

频率 - 性质

- ▶ 根据频率的定义, 有 $0 \leq f_n(A) \leq 1$, $f_n(\Omega) = 1$, $f_n(\emptyset) = 0$.
- ▶ 若 A_1, A_2, \dots, A_n 为两两互不相容事件, 则

$$f_n(A_1 \cup A_2 \cup \dots \cup A_n) = f_n(A_1) + f_n(A_2) + \dots + f_n(A_n).$$



1. 频率与概率

定义 1.2.1

- ▶ 设在相同的条件下, 进行了 n 次试验, 在这 n 次试验中事件 A 出现了 m 次, 则称

$$f_n(A) = \frac{m}{n} = \frac{\text{事件 } A \text{ 出现的次数}}{\text{试验的总次数}}$$

为随机事件 A 在 n 次试验中出现的**频率**, m 称为**频数**.

频率 - 观测

- ▶ 事件的频率刻画了事件发生的频繁程度.
- ▶ 频率越大, 事件 A 发生的越频繁, 因而在一次试验中发生的可能性越大.
- ▶ 可否用频率来表示 A 在一次试验中发生的可能性的**大小**?



1. 频率与概率

频率与概率的直观区别

- ▶ 随机事件的频率与我们进行的试验有关，而随机事件的概率则是完全客观的存在。
- ▶ 随机事件的频率 $f_n(A)$ 可以看作是概率的随机表现。

频率的稳定性

- ▶ 大量经验表明，当试验的次数足够大时，频率总是稳定于某一个常数附近，发生较大偏离的可能性很小，这一性质称为**频率的稳定性**。

频率的稳定性 - 例子

- ▶ 教材 Page 7 例 1.2.1 - 1.2.2.



1. 频率与概率

观测

- ▶ 随机事件在大量试验中存在着一种客观规律性，频率稳定性是这种规律性的表现.
- ▶ 频率稳定性由大量统计得来，因而也叫统计规律性.
- ▶ 可以用频率的稳定值作为事件发生可能性大小的度量指标.

定义 1.2.2 (概率的统计定义)

- ▶ 在大量重复试验中，若事件 A 发生的频率稳定地在某一常数 p 的附近摆动，则称该常数 p 为事件 A 发生的概率，记为 $P(A)$ ，且有 $P(A) = p$.

注意区分频率与概率

- ▶ 频率是变动的，概率为常数.
- ▶ 当试验次数足够多时，频率相对稳定，可把频率作为概率的近似值，即 $f_n(A) \approx P(A)$.
- ▶ 日常生活中遇到的产品合格率，彩票中奖率等一般指频率.



2. 古典概型

观测

- ▶ 如果使用概率的统计学定义, 要确定一个事件的概率, 需要进行大量重复试验.

古典概型的两个特点

- ▶ **有限性:** 试验样本空间中的样本点只有有限个, 即基本事件的总数有限.
- ▶ **等可能性:** 每一次试验中, 每个基本事件发生的可能性相等.

定义 1.2.3 (概率的古典定义)

- ▶ 设试验结果共有 n 个基本事件 $\omega_1, \omega_2, \dots, \omega_n$, 并且这些事件发生的可能性相等. 事件 A 由其中的 m 个基本事件组成, 则事件 A 的概率为

$$P(A) = \frac{\text{事件 } A \text{ 包含的基本事件数}(m)}{\text{基本事件总数}(n)}.$$



2. 古典概型

古典概型 - 例子 (教材 Page 9: 例 1.2.3)

- 某城市电话号码升位后为八位数, 且第一位为 6 或 8. 求:
- (1) 从该城市中随机抽取一个电话号码为不重复的八位数的概率;
 - (2) 从该城市中随机抽取一个电话号码后三位数都是 8 的概率.





2. 古典概型

古典概型 - 例子 (教材 Page 9: 例 1.2.3)

- ▶ 某城市电话号码升位后为八位数, 且第一位为 6 或 8. 求:
 - (1) 从该城市中随机抽取一个电话号码为不重复的八位数的概率;
 - (2) 从该城市中随机抽取一个电话号码后三位数都是 8 的概率.

▶ 古典概型解题思路:

Step 1 分析样本空间中样本点的个数.

▶ $n = 2 \times 10^7$.

Step 2 分析所考虑的随机事件中包含的样本点个数.

(1) $m = 2 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3$.

(2) $m = 2 \times 10^4$.





2. 古典概型

古典概型 - 例子 (教材 Page 9: 例 1.2.4)

- ▶ 设有一批产品共计 100 件, 其中有 80 件是正品, 20 件为次品, 现按两种方法抽取产品:
 - (a) 有放回抽样: 每次任意抽取一件, 经观察后放回, 再从中任取下一件.
 - (b) 不放回抽样: 每次任意抽取一件, 经观察后不放回, 从剩下的产品中任取一件.
- ▶ 分别按两种抽样方法, 求从这 100 件产品中任意抽取 3 件, 其中有 2 件次品的概率.



2. 古典概型

古典概型 - 例子 (教材 Page 9: 例 1.2.4)

- ▶ 设有一批产品共计 100 件, 其中有 80 件是正品, 20 件为次品, 现按两种方法抽取产品:
 - (a) 有放回抽样: 每次任意抽取一件, 经观察后放回, 再从中任取下一件.
 - (b) 不放回抽样: 每次任意抽取一件, 经观察后不放回, 从剩下的产品中任取一件.
- ▶ 分别按两种抽样方法, 求从这 100 件产品中任意抽取 3 件, 其中有 2 件次品的概率.
 - (a) $n = 100^3$, $m = C_3^2 \times 20^2 \times 80$.
 - (b) $n = 100 \times 99 \times 98$, $m = C_3^2 \times 20 \times 19 \times 80$.



2. 古典概型

两种重要的抽样方式

1. **有放回抽样**: 每次任意抽取一件, 经观察后放回, 再从中任取下一件 (基本事件数量: n^m).
2. **不放回抽样**: 每次任意抽取一件, 经观察后不放回, 从剩下的产品中任取一件 (基本事件数量: $n!/(n-m)!$).

两种抽样方式之间的区别与联系

- ▶ 采用两种抽样方法求同一事件的概率很有可能是不同的.
- ▶ 当产品的总数较大, 而抽取的数量相对来说较小时, 在两种抽样方式下计算的概率值相差不大.
- ▶ 在实际问题中, 当产品的总数较大时, 可把不放回的抽样视为有放回抽样.



2. 古典概型

古典概型 - 例子

- ▶ 在 N 件产品中已知有 M 件次品, 现从中随机抽取 n 件 (取后不放回). 问这 n 件中恰有 k 件次品的概率?





2. 古典概型

古典概型 - 例子

- ▶ 在 N 件产品中已知有 M 件次品, 现从中随机抽取 n 件 (取后不放回). 问这 n 件中恰有 k 件次品的概率?
- ▶ 样本空间中基本事件的数量 $n = C_N^n$.
- ▶ 事件包含的基本事件数 $m = C_M^k \cdot C_{N-M}^{n-k}$.





2. 古典概型

古典概型 - 例子 (教材 Page 10: 例 1.2.5)

- 把 n 个不同的球以同样的概率随机放入 N ($N \geq n$) 个盒子中, 假设每个盒子能容纳的球数没有限制, 试求下列各事件的概率:
- (1) 某指定的 n 个盒子中各有一个球;
 - (2) 任意 n 个盒子中各有一个球;
 - (3) 有一个盒子中恰有 m ($m \leq n$) 个球.



2. 古典概型

古典概型 - 例子 (教材 Page 10: 例 1.2.5)

- ▶ 把 n 个不同的球以同样的概率随机放入 N ($N \geq n$) 个盒子中, 假设每个盒子能容纳的球数没有限制, 试求下列各事件的概率:
 - (1) 某指定的 n 个盒子中各有一个球;
 - (2) 任意 n 个盒子中各有一个球;
 - (3) 有一个盒子中恰有 m ($m \leq n$) 个球.
- ▶ 样本空间中基本事件数 N^n .
 - (1) 事件所包含的基本事件数 $n!$.
 - (2) 事件所包含的基本事件数 $C_N^n \cdot n!$.
 - (3) 事件所包含的基本事件数 $C_n^m \cdot N \cdot (N-1)^{n-m}$.



2. 古典概型

例 1.2.5 的衍生 - 生日问题

- ▶ 求参加某次集会的 n 个人中至少有两人生日相同的概率 p_n .



2. 古典概型

例 1.2.5 的衍生 - 生日问题

- ▶ 求参加某次集会的 n 个人中至少有两人生日相同的概率 p_n .
- ▶ 把 n 个人看成 n 个小球, 把一年的 365 天看作盒子, $N = 365$.

$$\begin{aligned} p_n &= 1 - P(\{\text{所有人生日均不相同}\}) \\ &= 1 - \frac{C_N^n \cdot n!}{N^n}. \end{aligned}$$

- ▶ 当 $n = 23$ 时, 同生日的概率已超过 $\frac{1}{2}$;
- ▶ 当 $n = 40$ 时, 概率几乎达九成.
- ▶ 当 $n = 60$ 时, 几乎可以肯定必有两人生日相同.

n	5	10	20	23	30	40	60
p_n	0.027	0.117	0.411	0.507	0.706	0.891	0.994



3. 几何概率

古典概型的局限性

- ▶ 试验的可能结果只能是有限个, 并且要求等可能性.
- ▶ 推广第一步: 样本空间中的样本点有无穷多个, 但仍具备等可能性.

定义 1.2.4 (几何概率)

- ▶ 如果试验 E 的可能结果可以几何地表示为某区域 Ω 中的一个点 (区域 Ω 可以是一维的、二维的、三维的、...), 并且点落在 Ω 中某区域 A 的概率与 A 的测度 (长度, 面积, 体积等) 成正比, 而与 A 的位置及形状无关, 则随机点落在区域 A 的概率为

$$P(A) = \frac{A \text{ 的测度}}{\Omega \text{ 的测度}} = \frac{m(A)}{m(\Omega)},$$

称上式定义的概率为**几何概率**.



3. 几何概率

定义 1.2.4 (几何概率)

- ▶ 如果试验 E 的可能结果可以几何地表示为某区域 Ω 中的一个点 (区域 Ω 可以是一维的、二维的、三维的、...), 并且点落在 Ω 中某区域 A 的概率与 A 的测度 (长度, 面积, 体积等) 成正比, 而与 A 的位置及形状无关, 则随机点落在区域 A 的概率为

$$P(A) = \frac{A \text{ 的测度}}{\Omega \text{ 的测度}} = \frac{m(A)}{m(\Omega)},$$

称上式定义的概率为**几何概率**.

统一书写格式

- ▶ 统一用 $m(A)$ 表示事件 A 的测度.



3. 几何概率

几何概率 - 例子 (教材 Page 12: 例 1.2.7)

▶ 在线段 $[0,3]$ 上任投一点, 求此点坐标小于 1 的概率.

▶ 几何概率解题思路:

Step 1 确定样本空间 Ω .

▶ $\Omega = [0, 3]$.

Step 2 确定事件 A 的范围.

▶ $A = [0, 1]$.





3. 几何概率

几何概率 - 例子 (教材 Page 12: 例 1.2.8)

- ▶ 向区间 $[0,1]$ 上任意投两点, 求此两点间距离小于 $\frac{1}{2}$ 的概率.



3. 几何概率

几何概率 - 例子 (教材 Page 12: 例 1.2.8)

► 向区间 $[0,1]$ 上任意投两点, 求此两点间距离小于 $\frac{1}{2}$ 的概率.

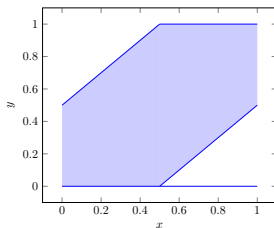
1. 确定样本空间 Ω .

► x, y 表示两点坐标, $0 \leq x \leq 1, 0 \leq y \leq 1$.

► $\Omega = [0, 1] \times [0, 1]$.

2. 确定事件 A 的范围.

► $|x - y| < \frac{1}{2}$.





3. 几何概率

几何概率 - 例子 (教材 Page 12: 例 1.2.9 蒲丰投针问题)

- ▶ 平面上画着一些平行线, 它们之间的距离都等于 d , 向此平面上任投一长度为 l ($l < d$) 的针, 求此针与任一平行线相交的概率.



3. 几何概率

几何概率 - 例子 (教材 Page 12: 例 1.2.9 蒲丰投针问题)

- ▶ 平面上画着一些平行线, 它们之间的距离都等于 d , 向此平面上任投一长度为 ℓ ($\ell < d$) 的针, 求此针与任一平行线相交的概率.

1. 确定样本空间 Ω .

- ▶ x 表示针的中点到最近的一条平行线的距离, $0 \leq x \leq \frac{d}{2}$.
- ▶ ϕ 表示针与平行线所成的夹角, $0 \leq \phi \leq \pi$.
- ▶ $\Omega = \{(x, \phi) | 0 \leq x \leq \frac{d}{2}, 0 \leq \phi \leq \pi\}$.

2. 确定事件 A 的范围.

- ▶ $x \leq \frac{\ell}{2} \cdot \sin \phi$.
- ▶ $p = \frac{2\ell}{\pi d}$.

