信息安全数学基础 －－

概率论

王丽萍
wangliping@iie.ac.cn

中科院信息工程所

2021年11月

参考书：《信息安全中的数学方法与技术》 冯登国 等编 清华大学出版社

序　言

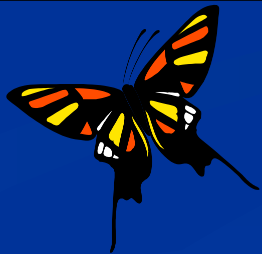
概率论是研究什么的？

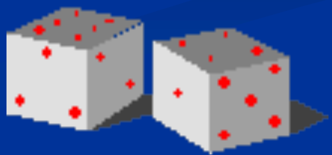
随机现象：不确定性与统计规律性

概率论——研究和揭示随机现象的统计规律性的科学

在我们所生活的世界上,充满了不确定性

从扔硬币、掷骰子和玩扑克等简单的机会游戏，到复杂的社会现象；从婴儿的诞生，到世间万物的繁衍生息；从流星坠落，到大自然的千变万化……，我们无时无刻不面临着不确定性（随机性）.





从亚里士多德时代开始，哲学家们就已经认识到随机性在生活中的作用，他们把随机性看作为破坏生活规律、超越了人们理解能力范围的东西。他们没有认识到有可能去研究随机性，或者是去测量不定性。

而将不定性（随机性）数量化，来尝试研究随机现象，是直到20世纪初叶才开始的. 还不能说这个努力已经十分成功了，但就是那些已得到的成果，已经给人类活动的一切领域带来了一场革命.




本学科的应用

概率统计理论与方法的应用几乎遍及所有科学技术领域、工农业生产和国民经济的各个部门中. 例如

1. 气象、水文、地震预报、人口控制及预测都与《概率论》紧密相关；

2. 产品的抽样验收，新研制的药品能否在临床中应用，均要用到《假设检验》；

3. 寻求最佳生产方案要进行《实验设计》和《数据处理》；

4. 电子系统的设计, 火箭卫星的研制及其发射都离不开《可靠性估计》；

5. 处理通信问题, 需要研究《信息论》；

6. 探讨太阳黑子的变化规律时,《时间序列分析》方法非常有用;

7. 研究化学反应的时变率，要以《马尔可夫过程》 来描述;

8. 量子计算：基态 $|0>, |1>$

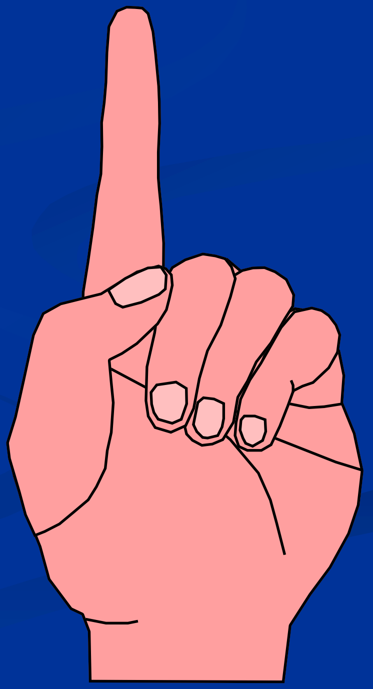
$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha^2+\beta^2=1$$

9. **密码领域：密钥流序列的伪随机性；基于格的密码、基于LWE的密码体制等。**

第一章 随机事件及其概率

- 随机事件及其运算
- 概率的各种定义
- 概率的公理化定义与性质
- 条件概率



1.1 随机事件

1.1.1 随机现象与随机事件

●确定性现象—— 在一定的条件下, 发生结果只有一个的现象，即必然发生。

A. 在标准大气压条件下，温度达到100度的纯水必然沸腾;

B. 太阳每天从东方升起;

C. 异性电荷必然互相吸引。

●随机现象—— 在一定的条件下, 或发生这样的结果,或发生那样的结果,即发生的结果有多种可能性。

A. 抛一枚质地均匀的骰子所出现的点数；

B. **某电话台每小时内接到的呼唤电话数;**

C. **明天的最高温度；**

D. **新生婴儿的体重;**

E. **抛一枚质地均匀的硬币.**

大量试验，其结果具有统计规律性。

- 对某事物特征进行观察，统称**试验**,用T表示
- 随机试验

  若某个试验满足

  - 可在相同的条件下重复进行
  - 试验结果不止一个， 但知道每次试验所有可能的结果。
  - 试验前不能预知出现哪种结果

称此试验为**简单随机试验**，简称**随机试验**

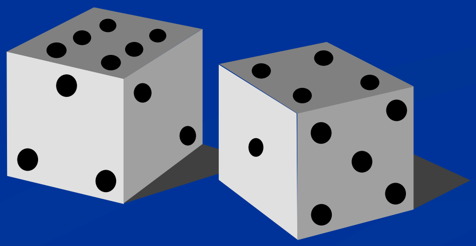
随机试验的例子

T_1: 抛一枚硬币，分别用“H” 和 “T” 表示出现正面和反面;

T_2: 将一枚硬币连抛三次，考虑正反面出现的情况；

T_3:将一枚硬币连抛三次，考虑正面出现的次数;

T_4:掷一颗骰子，考虑可能出现的点数；



随机事件

样本空间

1. **样本空间**：试验的所有可能结果所组成的集合称为样本空间，记为 Ω

2. **样本点**：试验的每一个结果或样本空间的元素称为一个样本点,记为 ω.

3. 由一个样本点组成的单点集称为一个**基本事件**，记为$\{\omega\}$

4. 有限样本空间：样本点总数为有限多个。如：

5. 无限样本空间：样本点总数为无限多个。如：

随机事件

1.定义 试验中, 每一个可能的结果叫“随机事件”，简称“事件（event）”.记作A、B、C等

任何事件均可表示为样本空间 Ω的某个子集.

称事件A发生当且仅当试验的结果是子集A中的元素

2.两个特殊事件: 必然事件S 、不可能事件 ϕ.

例如:对于试验T2，以下A、B、C即为三个随机事件

A＝“至少出一个正面”

＝{HHH, HHT, HTH, THH，HTT，THT，TTH}；

B=“三次出现同一面”={HHH,TTT}

C=“恰好出现一次正面”={HTT，THT，TTH}

可见，可以用文字表示事件，事件也可以表示为样本空间的子集，后者反映了事件的实质，且更便于今后计算概率。

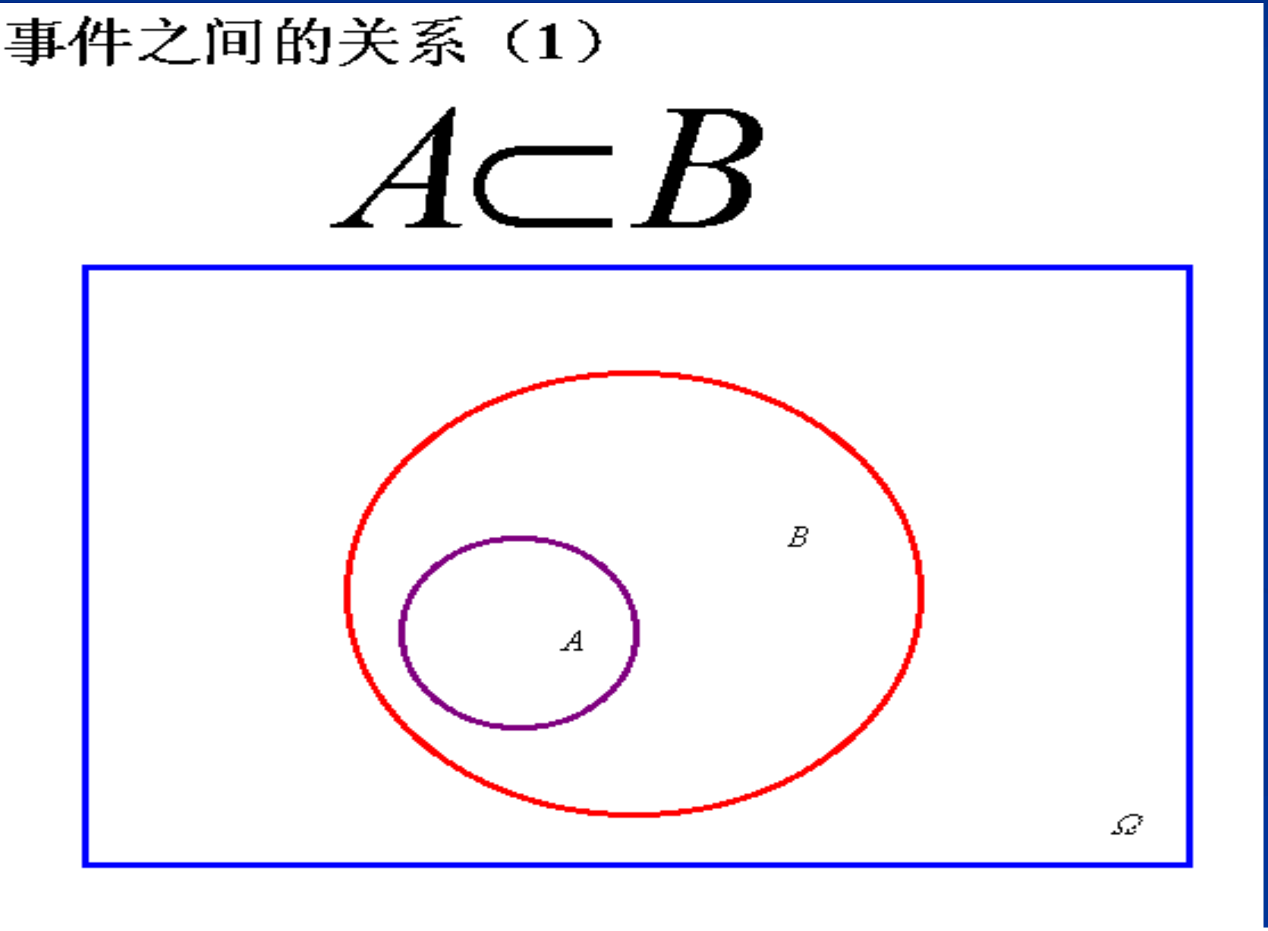
还应注意，同一样本空间中，不同的事件之间有一定的关系，易见，事件之间的关系是由它们所包含的样本点所决定的，这种关系可以用集合之间的关系来描述。

1.1.2 事件之间的关系及运算

注意关系运算与事件发生实际意义的联系。

1.包含关系 “ A发生必导致B发生”记为A⊂B

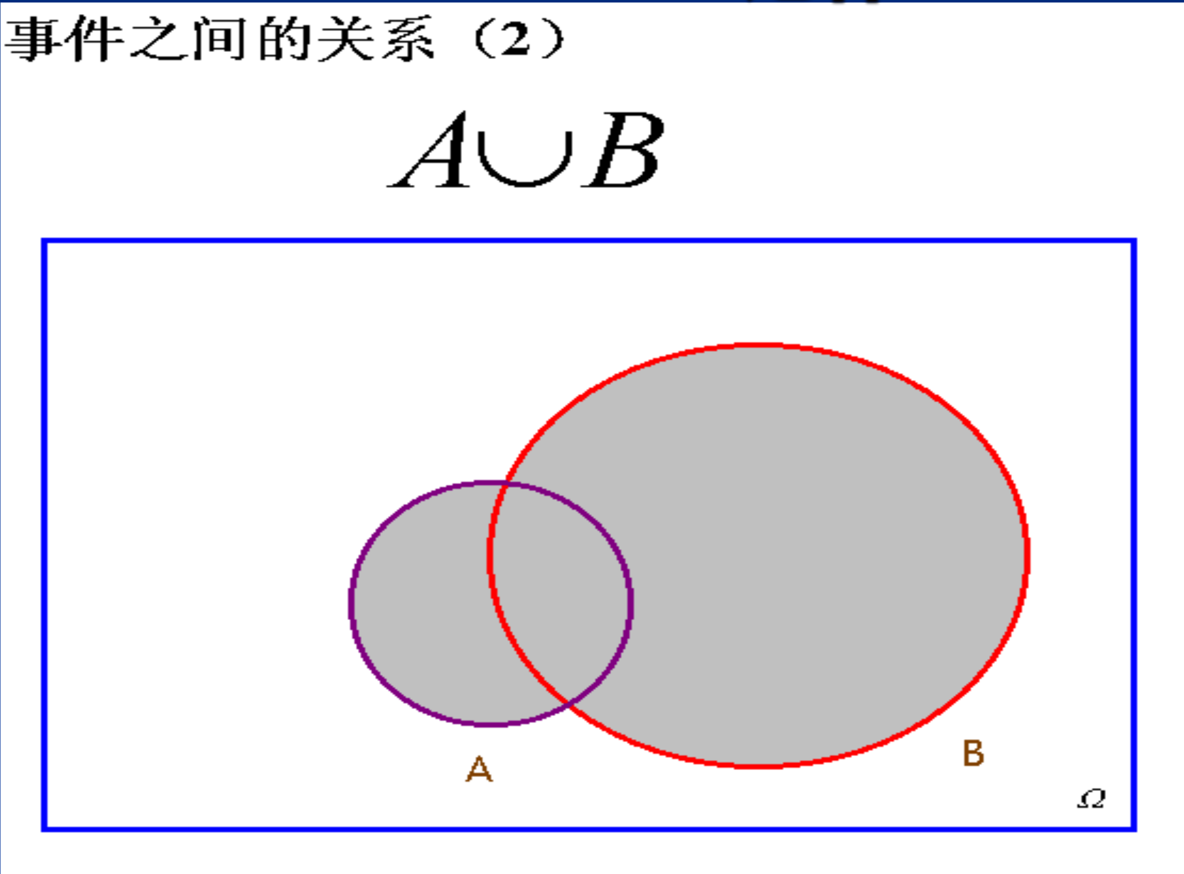
$$A = B \Leftrightarrow A\subset B \text{且} B\subset A.$$



如：射击三次，事件A：命中二次；事件B至少命中二次，则A⊂B

等价说法：B不发生，必导致A不发生。

2. 和事件：(p4)“事件A与B至少有一个发生”，记作A∪B



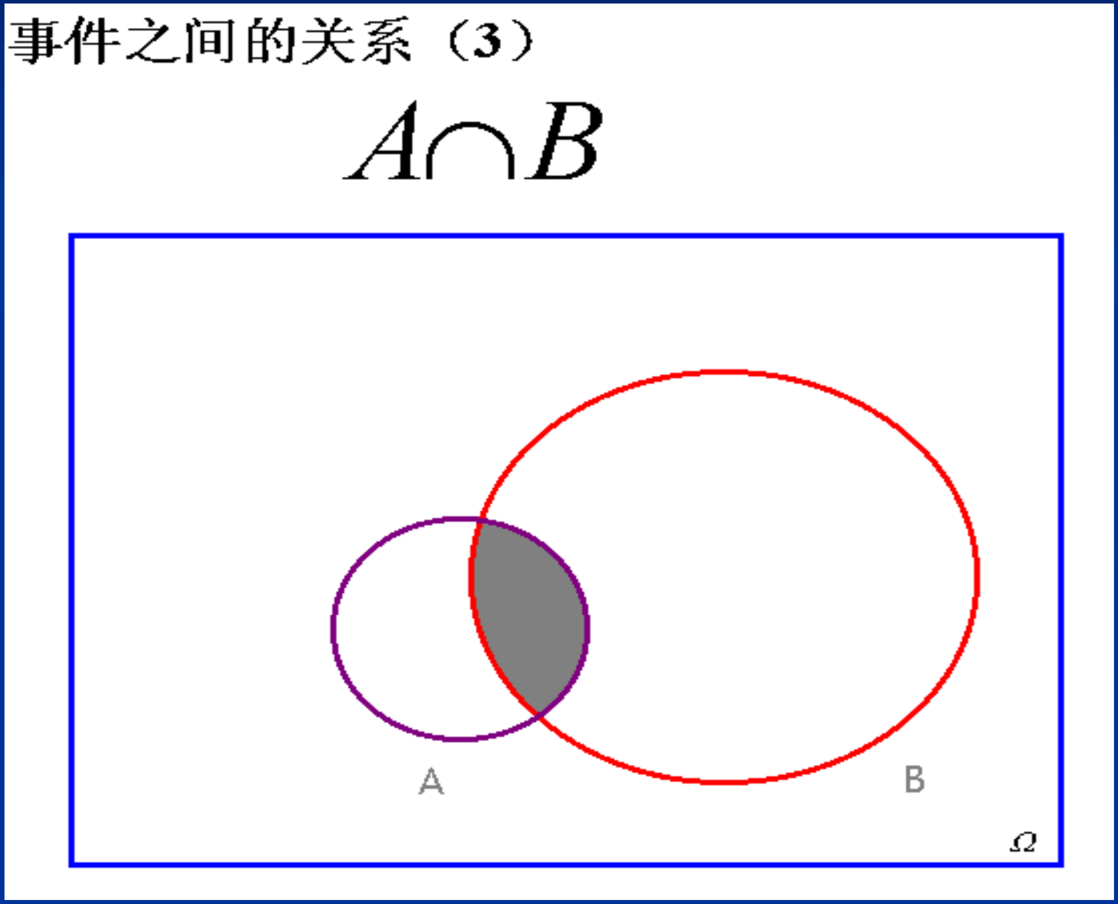
例：甲乙同时向目标射击。

A：甲击中；B：乙击中

C ＝ **A∪B** 如何解释？

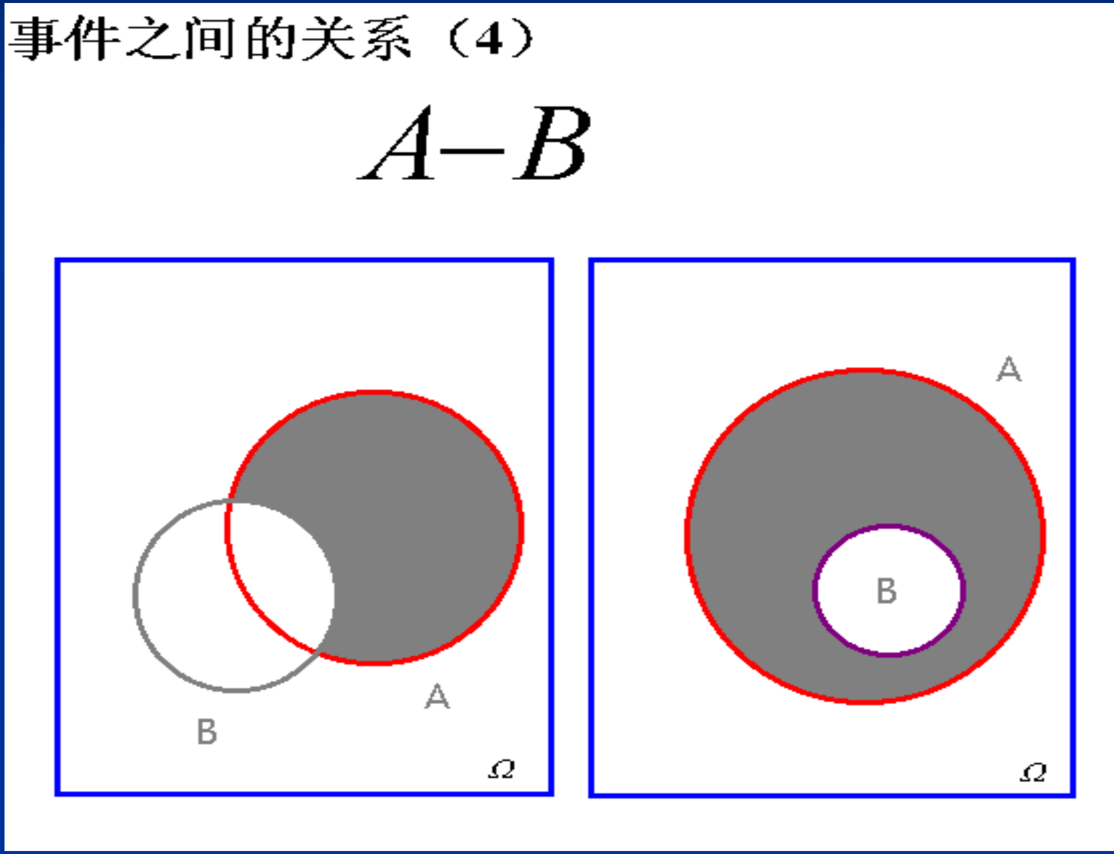
2′. **n个事件$A_1, A_2, \ldots, A_n$至少有一个发生，记作** $\bigcup_{i=1}^{n} A_i$

3. 积事件：A与B同时发生，记作 $A \cap B = AB$



$3'$. n个事件$A_1, A_2, \ldots, A_n$同时发生，记作 $A_1A_2\ldots A_n$

4. 差事件 ：A - B称为A与B的差事件,表示事件A发生而B不发生



例：抽取5名同学。

A:至少一名女生

B:至少两名女生

C:全男生

$\overline{A} = ?$

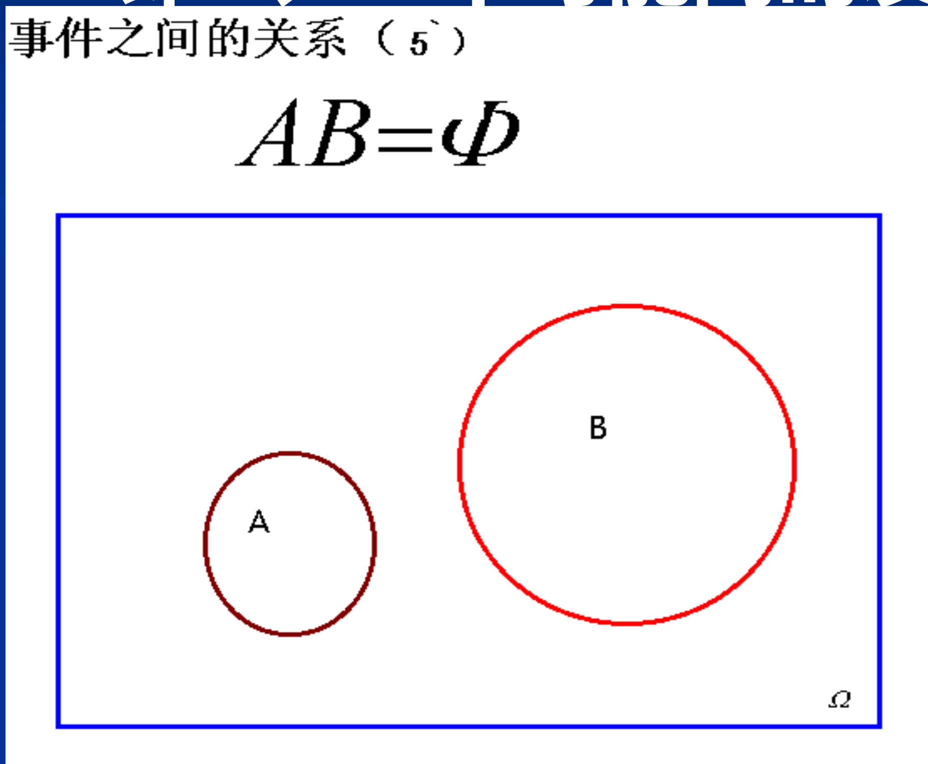
$\overline{B} =$ 至多一名女生

$A - B =$ 只有一名女生

思考：何时 A-B = φ？何时 A-B = A ？

$AB = A$ or $A \subset B$　　$AB = \phi$

5. **互斥的事件**(p5) ：$AB=\phi$ **又称互不相容。即A、B不可能同时发生。**

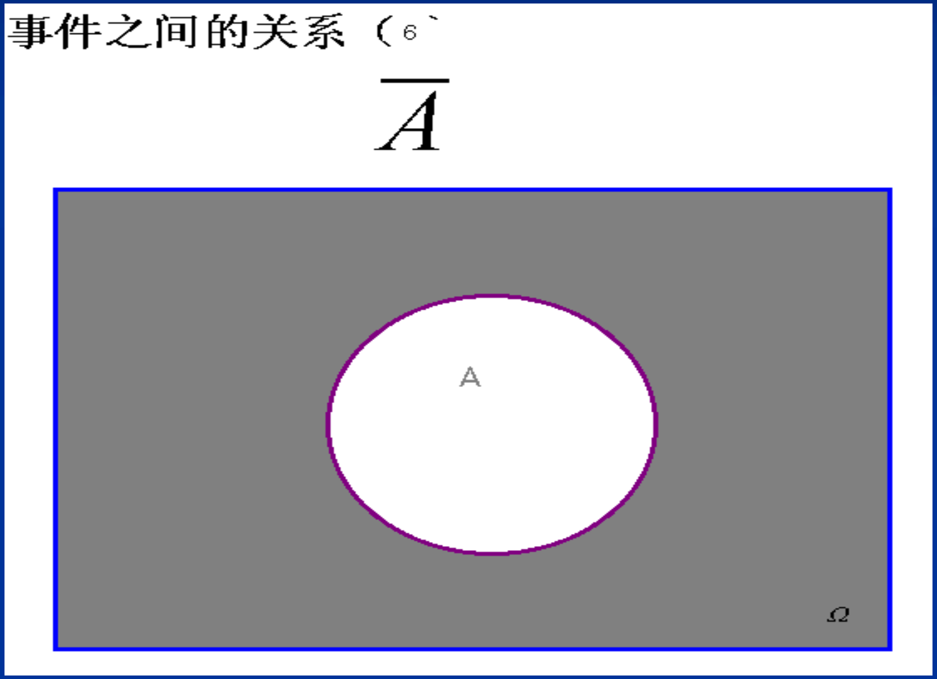


例：

注意：**三个事件A、B、C，即使**$ABC=\phi$ **也不一定A、B、C互不相容。n个事件互不相容，指的是两两互不相容。**掷骰子 $A=\{1,3,5,6\}$ $B=\{1,2,4,6\}$ $C=\{5,4\}$

6. 互补的事件 $\Leftrightarrow A \cup B = \Omega$, 且$AB = \phi$

记作$B = \overline{A}$, 称为A的对立事件; 易见 $A - B = A\overline{B}$



注意：互不相容与对立事件是不同的。前者A不发生B也可以不发生，但对立事件中，A、B必有一个发生。对立事件一定是互不相容的，反之不一定。

符号	集合论	概率论
Ω	空间	样本空间；必然事件
ϕ	空集	不可能事件
ω\in Ω	Ω中的元素	样本点
$\{\omega\}$	单点集	基本事件
$A\subset\Omega$	Ω的子集A	事件A
$A\subset B$	集合A包含在集合B中	事件A含于事件B
$A=B$	集合A与集合B相等（等价）	事件A与事件B相等（等价）
$A\cup B$	集合A与集合B之和	事件A与事件B至少有一个
		发生（事件A与B之和）
$A\cap B$	集合A与集合B之交	事件A与事件B同时发生
		（事件A与B之积或交）
$\bar{A}$	集合A的补集（余集）	事件A的逆事件
$A-B$	集合A与集合B的差	事件A发生而事件B不发生
		（事件A与B之差）
$A\cap B=\phi$	事件A与B没有公共元素	事件A与事件B互不相容

事件的运算

1、**交换律**：$A\cup B = B\cup A$，$AB = BA$

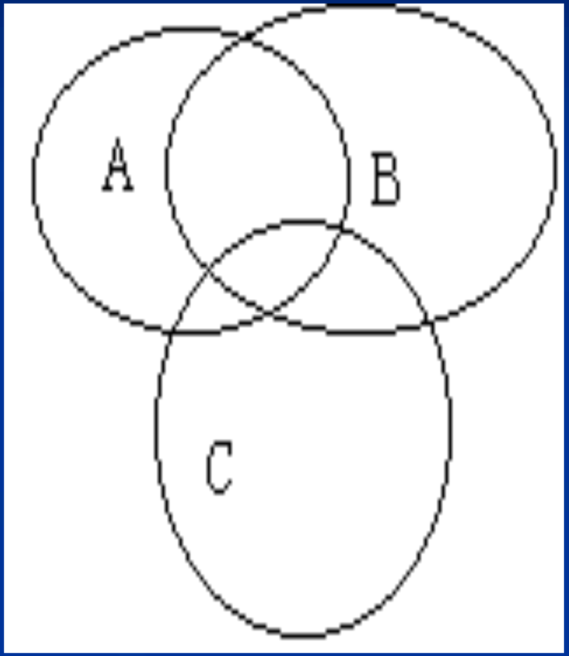
2、**结合律**：$(A\cup B)\cup C = A\cup(B\cup C)$，

$(AB)C = A(BC)$

3、**分配律**：$(A\cup B)C = (AC)\cup(BC)$，

$(AB)\cup C = (A\cup C)(B\cup C)$

4、**德摩根(De Morgan)律**：



$$\overline{A\bigcup B} = \overline{A}\bigcap\overline{B}$$

$$\overline{A\bigcap B} = \overline{A}\bigcup\overline{B}$$

作业：甲、乙、丙三人各向目标射击一发子弹，以A、B、C分别表示甲、乙、丙命中目标，试用A、B、C的运算关系表示下列事件：

A_1:“至少有一人命中目标”:

A_2:“恰有一人命中目标”:

A_3:“恰有两人命中目标”:

A_4:“最多有一人命中目标”:

A_5:“三人均命中目标”:

A_6:“三人均未命中目标”:


稍事休息！