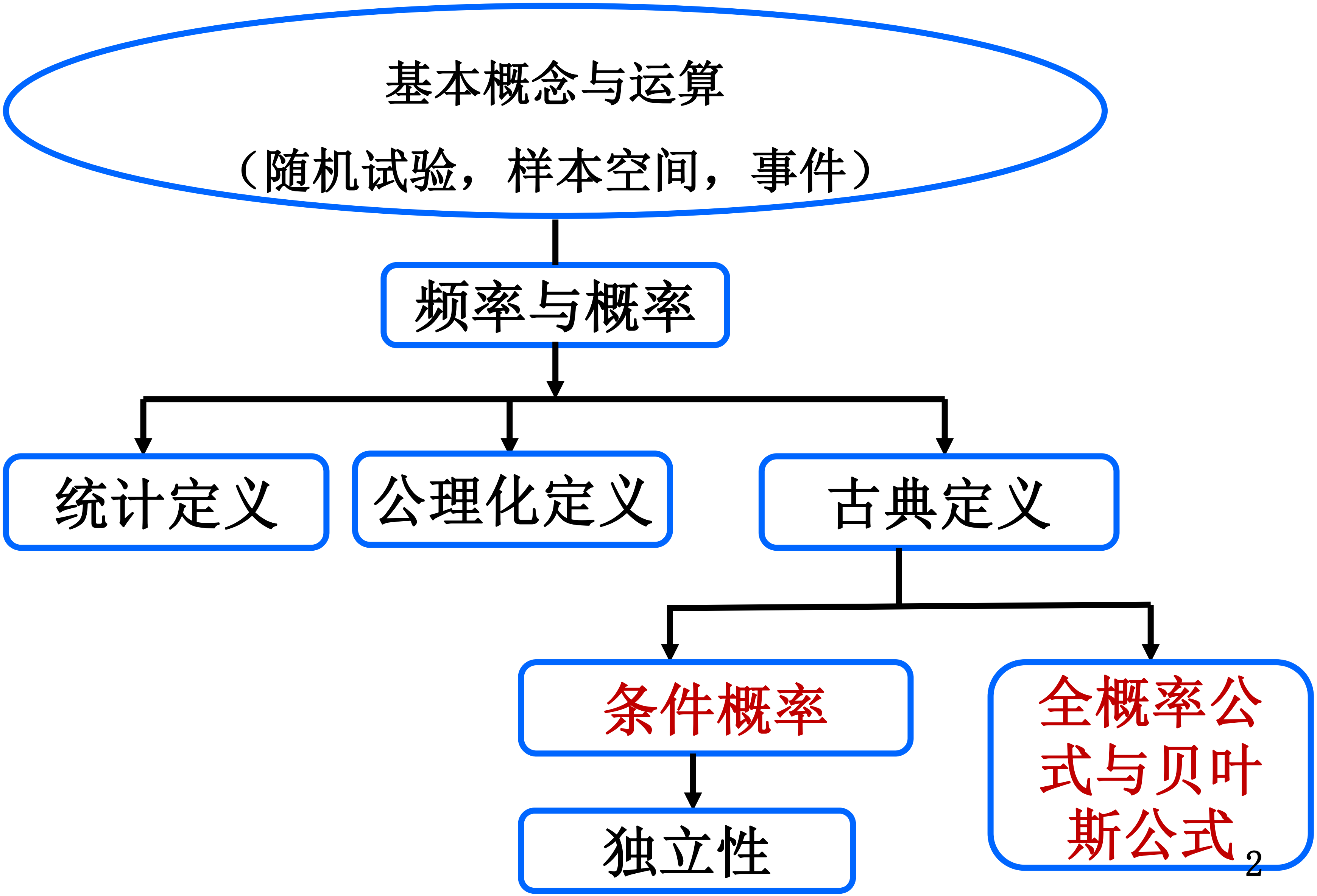
第一章
概率论的基本概念

王笑尘

北京邮电大学网络空间安全学院

wxiaochen@bupt.edu.cn

第五节 条件概率



基本概念与运算
（随机试验，样本空间，事件）
频率与概率
统计定义
公理化定义
古典定义
条件概率
全概率公式与贝叶斯公式
独立性

条件概率

引例　7个球，其中5个红球，2个白球。不放回取球，每次取一个球，共取两次。问：第1次取到红球的条件下，第2次取到红球的概率是多少？

记: A={第1次取到红球}，B={第2次取到红球},

$$P(B|A)=\frac{4}{6},\ P(AB)=\frac{5}{7}\times\frac{4}{6},\ P(A)=\frac{5}{7}$$

$$P(B|A)=P(AB)/P(A)$$

注：本例中，计算$P(A)$时，依据的前提条件是7个球中红球的比例。计算$P(B|A)$时，这个前提条件未变, 只是加上“事件A已发生”这个新的条件。

条件概率

提出三个问题：

1. 对于一般具有附加条件的概率问题，是否也一定具有引例中的表达形式？

2. 由条件概率的概念是否可以得出两个事件积（交）的概率？

3. 无条件概率 P(A)、条件概率P(B|A)与乘积概率 P(AB)的区别是什么？

条件概率

1. 定义： 设 A ,B是两个事件, 则称$P(B|A)=P(AB)/P(A)$为在事件 A 发生的条件下事件 B 发生的条件概率，其中 $P(A)>0$。

注：

▲ 条件概率符合概率定义中的三个条件:

★ 对每个事件 B, 有: $1\geq P(B|A)\geq 0$ 非负性

★ 对于必然事件S, 有: $P(S|A)=1$ 规范性

★ 设有 $B_1, B_2, \cdots\cdots$ 是两两互不相容的事件, 则有

$$P(\bigcup_{i=1}^{\infty}B_i|A)=\sum_{i=1}^{\infty}P(B_i|A)$$

可列可加性

条件概率

2．性质

条件概率常用的相关性质有：

(1) $P(\Phi|B)=0$

(2) $P(A|B)=1-P(\overline{A}|B)$

(3) $P(A_1\cup A_2|B)=P(A_1|B)+P(A_2|B)-P(A_1A_2|B)$

条件概率

3.　条件概率的计算

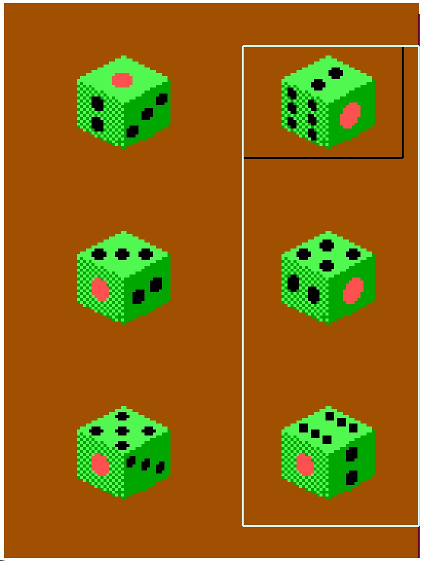
1) 用定义计算:

$$P(A|B)=\frac{P(AB)}{P(B)},$$

$P(B)>0$

2)从“加入条件后改变了的情况”去计算:

比如：　A={掷出2点}，　B={掷出偶数点}



则: $P(A|B)=\frac{1}{3}$

B发生后的缩减样本空间所含样本点总数

在缩减样本空间中A所含样本点个数

例1. 掷两颗骰子,观察出现的点数 ,设 x_1, x_2

分别表示第一颗,第二颗骰子的点数,且设:

$$A=\left\{(x_1,x_2)\middle|x_1+x_2=10\right\} \quad B=\left\{(x_1,x_2)\middle|x_1>x_2\right\}$$

求: $P(B|A),\ P(A|B)$

解: 依题意,样本空间

$$S=\{(1,1),(1,2)\cdots(1,6)\cdots(2,1),(2,2)\cdots$$

$$(2,6)\cdots\cdots(6,1),(6,2)\cdots(6,6)\}$$

------36 种

$$A=\{(5,5),(4,6),(6,4)\}$$

------3 种

$$B=\{(2,1),(3,2),(3,1),(4,3),(4,2),(4,1)$$

$$\cdots\cdots(6,5),(6,4)\cdots(6,1)\}$$

------ 15种

方法 1:

在样本空间 S 中计算 P(B), P(AB) 然后依公式 $P(A|B)$ 计算

$$\because AB = \{ (6,4) \}$$

$$\therefore P(AB) = \frac{1}{36}, \text{又} \because P(A) = \frac{3}{36}, P(B) = \frac{15}{36}$$

从而: $$P(B|A) = \frac{P(AB)}{P(A)} = \frac{1}{3}$$

$$P(A|B) = \frac{P(AB)}{P(B)} = \frac{1}{15}$$

掷两颗骰子,观察出现的点数，设 x_1, x_2分别表示第一颗,第二颗骰子的点数,且设:

$$A = \left\{ (x_1, x_2) \middle| x_1 + x_2 = 10 \right\} \quad B = \left\{ (x_1, x_2) \middle| x_1 > x_2 \right\}$$

方法2：

在缩减的样本空间 S_A 或 S_B中计算B或A出现的概率就可得所求的条件概率(这种方法适合简单的问题)

在缩减的样本空间 S_A 中看：A中有3个基本事件,其中只有(6,4)是B中包含的基本事件, 故有：$P(B|A)=\dfrac{1}{3}$

在缩减的样本空间 S_B 中看：B中有15个基本事件,其中只有(6,4)是A中包含的基本事件，故有:

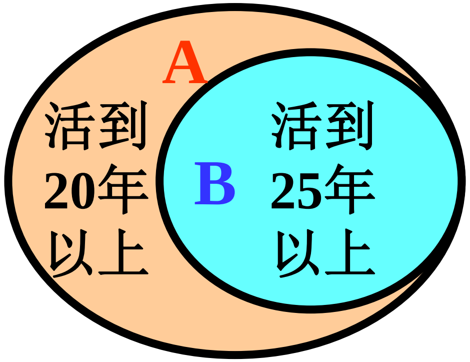
$$P(A|B)=\frac{1}{15}$$

$$A=\{(5,5),(4,6),(6,4)\}$$
$$B=\{(2,1),(3,2),(3,1),(4,3),(4,2),(4,1)$$
$$\cdots\cdots(6,5),(6,4)\cdots(6,1)\}$$

例3 设某种动物由出生算起活到20年以上的概率为0.8，活到25年以上的概率为0.4。 问现年20岁的这种动物，它能活到25岁以上的概率是多少？

解： 设A={能活20年以上}，B={能活25年以上}

所求为 $P(B|A)$ 。



依题意， $P(A) = 0.8,\ P(B) = 0.4$

$$P(B\mid A)=\frac{P(AB)}{P(A)}=\frac{P(B)}{P(A)}=\frac{0.4}{0.8}=0.5$$

乘法定理

由条件概率的定义： $P(A|B)=\dfrac{P(AB)}{P(B)}$

若已知$P(B)$, $P(A|B)$时, 可以反求$P(AB)$，即有：

定理1： 设 P(B)>0 或 P(A)>0，则：

$$P(AB)=P(B)P(A|B)=P(A)P(B|A)$$

注： 乘法定理可推广到多个事件的积事件的情形：

(1) $P(ABC)=P(A)\cdot P(B|A)\cdot P(C|AB)$

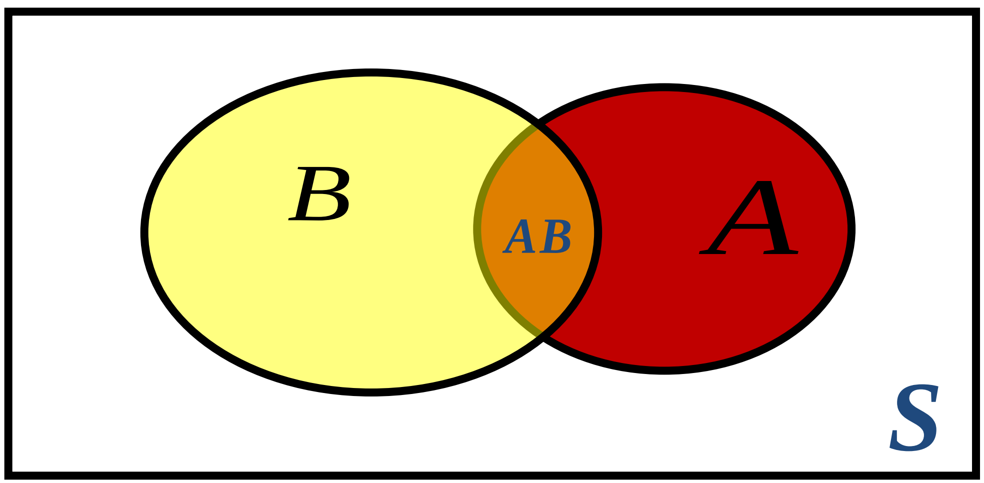
其中：$P(AB)>0$

(2) $P(A_1A_2\cdots A_n)=P(A_1)\cdot P(A_2|A_1)\cdot P(A_3|A_1A_2)\cdot$

$$\cdots\cdots P(A_n|A_1A_2\cdots\cdots A_{n-1})$$

归纳

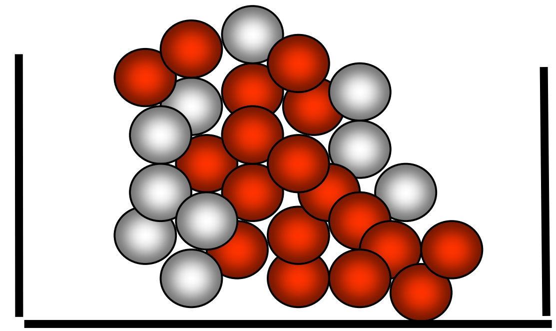
无条件概率 $P(A)$、 $P(AB)$ 及条件概率 $P(A|B)$ 的区别



$$P(A|B)=\frac{P(AB)}{P(B)},$$

例 4　波里亚（Polya）罐子模型

一个罐子中包含b 个白球和 r 个红球。随机地抽取一个球，观看颜色后放回罐中，并且再加进 c 个与所抽出的球具有相同颜色的球。这种过程进行四次，试求：第一、二次取到白球且第三、四次取到红球的概率.



b个白球, r 个红球

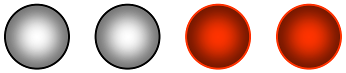
解: 设W_i={ 第 i 次取出是白球 },

i =1, 2, 3, 4

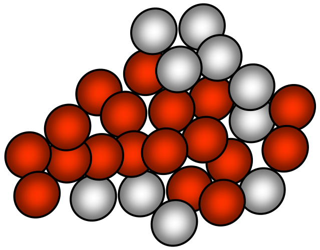
R_j={ 第 j 次取出是红球 },

j =1, 2, 3, 4

于是：$W_1W_2\ R_3\ R_4$ 表示事件 “连续取四个球，第一、第二个是白球，第三、四个是红球。”



用乘法公式容易求出（原罐b个白球、r个红球）：



$$P(W_1W_2R_3R_4)$$

$$= P(W_1)\,P(W_2|W_1)\,P(R_3|W_1W_2)\,P(R_4|W_1W_2R_3)$$

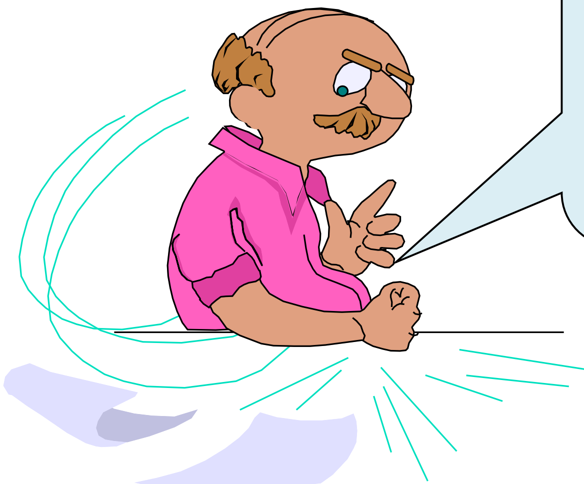
$$= \frac{b}{b+r} \cdot \frac{b+c}{b+r+c} \cdot \frac{r}{b+r+2c} \cdot \frac{r+c}{b+r+3c}$$

例5. 一场精彩的足球赛将要举行，5个球迷好不容易才搞到一张入场券。大家都想去，只好用抽签的方法来解决。

入场券

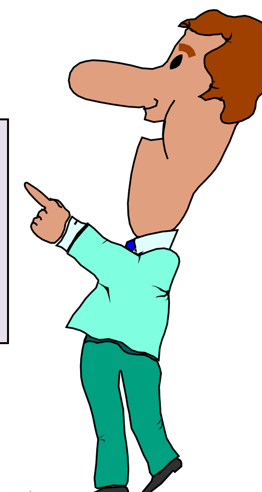
5 张同样的卡片，只有一张上写有“入场券”，其余的什么也没写。 将它们放在一起洗匀，让5个人依次抽取。

问：后抽的人确实比先抽的人吃亏吗?



“大家不必争先恐后，你们一个一个按次序来，谁抽到 ‘入场券’ 的机会都一样大。”

“先抽的人当然要比后抽的人抽到的机会大。”



到底谁说的对呢？请用已学的条件概率、乘法定理来计算一下,每个人抽到“入场券”的概率到底有多大?

设：A_i 表示“第 i 个人抽到入场券” i＝1,2,3,4,5.

则：$\overline{A}_i$ 表示“第 i 个人未抽到入场券”

显然：$P(A_1)=1/5$，$P(\overline{A}_1)=4/5$

也就是说，第1个人抽到入场券的概率是1/5.

由于：$$A_2=\overline{A}_1 A_2$$

因为若第2个人抽到了入场券，则第1个人肯定没抽到。

所以由乘法公式：$P(A_2)=P(\overline{A}_1)P(A_2\mid\overline{A}_1)$

计算得：$$P(A_2)=\frac{4}{5}\cdot\frac{1}{4}=\frac{1}{5}$$

即：第2个人抽到入场券的概率也是1/5。

同理，第3个人要抽到“入场券”，必须第1、第2个人都没有抽到. 因此:

$$P(A_3)=P(\overline{A}_1\overline{A}_2A_3)=P(\overline{A}_1)P(\overline{A}_2\,|\,\overline{A}_1)P(A_3\,|\,\overline{A}_1\overline{A}_2)$$

$=(4/5)(3/4)(1/3)=1/5$

由乘法公式

继续做下去就会发现, 每个人抽到“入场券”的概率都是1/5。

抽签不必争先恐后。

例 6.

箱子中装有10瓶形状相同的名酒,其中部优名酒7瓶,国优名酒3瓶,今有三个人从箱子中随机地取出一些酒来,每人只拿2瓶。

问：恰好第一个人拿到两瓶部优名酒,同时第二个人拿到部优、国优名酒各一瓶,第三个人拿到两瓶国优名酒的可能性有多大?

解： 设 $A=\{\text{第一个人拿到两瓶部优名酒}\}$

$B=\{\text{第二个人拿到部优国优名酒各一瓶}\}$

$C=\{\text{第三个人拿到两瓶国优名酒}\}$

北京邮电大学 Beijing University of Posts and Telecommunications

显然，所求事件的概率为：

$$P(ABC) = P(A)\cdot P(B|A)\cdot P(C|AB)$$

而：$P(A) = \dfrac{C_7^2}{C_{10}^2} = 0.467$

$$P(B|A) = \frac{C_5^1 \cdot C_3^1}{C_8^2} = 0.536$$

$$P(C|AB) = \frac{C_2^2}{C_6^2} = 0.067$$

10瓶名酒，其中部优7瓶，国优3瓶，第一人拿到两瓶部优名酒，同时第二人拿到部优、国优名酒各一瓶，第三个拿到两瓶国优名酒

从而：$P(ABC) = 0.467 \times 0.536 \times 0.067 = 0.017$

全概率公式和贝叶斯公式

全概率公式和贝叶斯公式主要用于计算比较复杂事件的概率，它们实质上是加法公式和乘法公式的综合运用.

综合运用

加法公式

$$\mathrm{P(A+B)}=P(A)+P(B)$$

A、B互斥

乘法公式

$$P(AB)=P(A)P(B|A)$$

$$P(A)>0$$

1. 样本空间的划分

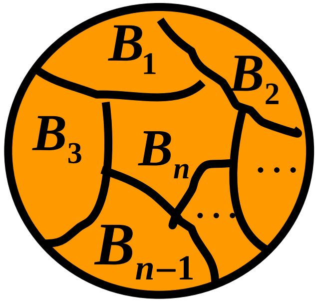
定义：设S为试验E的样本空间，$B_1, B_2, \cdots B_n$ 为 E 的一组事件, 若:

（1）$B_iB_j = \emptyset, i \neq j, i, j = 1, 2, \cdots, n,$

（2）$B_1 \cup B_2 \cup \cdots \cup B_n = S,$

则称$B_1, B_2, \cdots B_n$ 是样本空间S的一个划分或称$B_1, B_2,$ $\cdots B_n$是一个互斥事件完备组。

注：S 的一个划分：一是要互斥，二是要充满整个空间。



北京郵電大学 Beijing University of Posts and Telecommunications

比如：对“掷一颗骰子观察其点数”这一试验，其：

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

E的一组事件 $B_1=\{1,2,3\}, B_2=\{4,5\}, B_3=\{6\}$

是S的一个划分;

E的另一组事件 $C_1=\{1,2,3\}, C_2=\{3,4\}, C_3=\{5,6\}$

就不是S的一个划分。

2. 全概率公式

定理2 设试验E的样本空间为 S，A 为 E的事件, $B_1, B_2, \cdots, B_n$ 为S 的一个划分, 且 $P(B_i) > 0$ $i = 1,2,\cdots n$ 则：

$$P(A) = P(A|B_1)\cdot P(B_1) + P(A|B_2)\cdot P(B_2) + \cdots$$
$$+ P(A|B_n)\cdot P(B_n) = \sum_{i=1}^{n} P(A|B_i)\cdot P(B_i)$$

称为全概率公式。

[证明]: $\because A = AS = A(B_1 \cup B_2 \cup \cdots B_n)$

$$= AB_1 \cup AB_2 \cup \cdots AB_n$$

又 $\because P(B_i) > 0, i = 1,2,\cdots n,$ 且 $(AB_i)(AB_j) = \Phi, i \neq j$

$$\therefore \quad P(A) = P(AB_1) + P(AB_2) + \cdots + P(AB_n)$$

$$= P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots + P(A|B_n)P(B_n)$$

注: ▲ 全概率公式关键抓住寻找S的一个划分或寻找一个互斥事件完备组(这里事件 $B_i(i = 1,2,\cdots n)$ 是导致事件A发生的一组原因，而事件A的出现只能与 B_i 中之一同时出现)。

▲ 全概率公式一般用于“用条件概率求非条件概率”的问题。即P(A)不易求，但却很容易找到S的一个划分时用全概率公式比较方便。

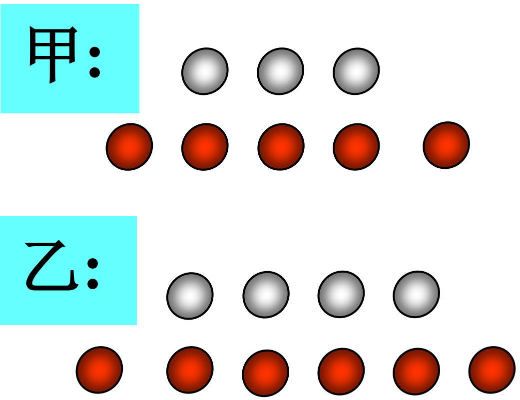
▲从另一个角度去理解全概率公式

某一事件A的发生有各种可能的原因($i=1,2,\ldots,n$)，如果A是由原因B_i所引起，则A发生的概率是：

$$P(AB_i)=P(B_i)P(A|B_i)$$

每一原因都可能导致A发生，故A发生的概率是各原因引起A发生概率的总和，即为全概率公式。

例8. 设甲袋中有3个白球5个红球,乙袋中有4个白球,6个红球,现从甲袋中任取一个球放入乙袋中,再从乙袋中任取一球。求：从乙袋中取得白球的概率。



解： 设A：从乙袋中取得白球

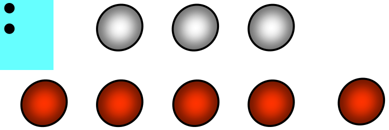
因为: 取球只有两种情况，要么白球要么红球

所以设： B_1: 从甲袋中任取一球是白球

B_2: 从甲袋中任取一球是红球

显然： B_1, B_2 构成一个互斥事件完备组

甲:

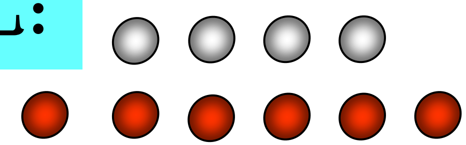


$$S = B_1 \cup B_2, \quad B_1 B_2 = \Phi$$

$$\therefore P(A) = P(A|B_1)\cdot P(B_1) + P(A|B_2)\cdot P(B_2)$$

$$= \frac{5}{11}\cdot\frac{3}{8} + \frac{4}{11}\cdot\frac{5}{8} = \frac{35}{88} = 0.398$$

乙:



例9.某工厂有四条流水线生产同一种产品, 四条流水线的产量分别占该产品总产量的15%，20%，25%，40%，且四条流水线生产产品的次品率分别是 0.01, 0.02, 0.03, 0.025。

求： 从出厂的这种产品中任取一件恰是次品的概率。

解：因为抽出的产品只能出自这四条流水线，故设：

A：取出的一件是次品

B_i：取出的一件产品恰出自第 i 条流水线，$i=1,2,3,4$

显然：$S=\bigcup_{i=1}^{4} B_i$，且 $B_iB_j=\Phi$，$i\neq j$，$i,j=1,2,3,4$

从而：
$$P(A)=\sum_{i=1}^{4} P(B_i)P(A|B_i)$$
$$=0.15\times0.01+0.2\times0.02+0.25\times0.03+0.4\times0.025$$
$$=0.023$$

四条流水线产量(率)：　15%，20%，25%，40%

四条流水线次品(率)：　0.01，0.02，0.03，0.025

例 10.甲、乙、丙三人同时对飞机进行射击, 三人击中的概率分别为0.4、0.5、0.7。飞机被一人击中而击落的概率为0.2，被两人击中而击落的概率为0.6， 若三人都击中，飞机必定被击落, 求:飞机被击落的概率.

例 10. 甲、乙、丙三人同时对飞机进行射击, 三人击中的概率分别为0.4、0.5、0.7。飞机被一人击中而击落的概率为0.2，被两人击中而击落的概率为0.6， 若三人都击中，飞机必定被击落, 求:飞机被击落的概率.

解: 设B= {飞机被击落}，A_i= {飞机被i人击中}， i=0,1,2,3

$$\text{则}B = A_0B + A_1B + A_2B + A_3B$$

由全概率公式:

$$P(B)= P(A_0)P(B|A_0)+ P(A_1)P(B|A_1) + P(A_2)P(B|A_2) + P(A_3)P(B|A_3)$$

为求$P(A_i)$，设 H_i={飞机被第i人击中}，i=1,2,3

可求得:

$$P(A_1)=P(H_1\overline{H}_2\overline{H}_3+\overline{H}_1H_2\overline{H}_3+\overline{H}_1\overline{H}_2H_3)$$

$$P(A_2)=P(H_1H_2\overline{H}_3+H_1\overline{H}_2H_3+\overline{H}_1H_2H_3)$$

$$P(A_3)=P(H_1H_2H_3)$$

将数据代入计算得:

$P(A_0)=0.09$; $P(A_1)=0.36$; $P(A_2)=0.41$; $P(A_3)=0.14$。

于是:

$P(B)=P(A_1)P(B|A_1)+P(A_2)P(B|A_2)+P(A_3)P(B|A_3)$

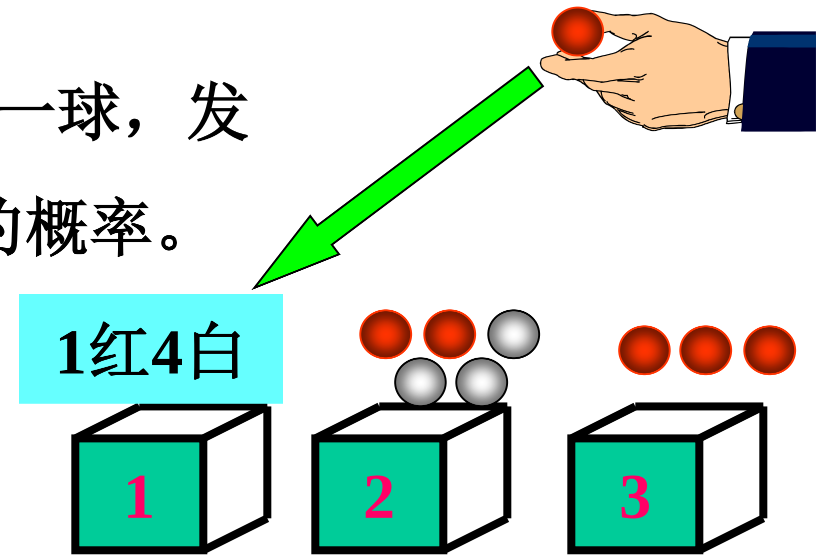
$=0.36\times0.2+0.41\times0.6+0.14\times1=0.458$

依题意，
$P(B|A_1)=0.2$,
$P(B|A_2)=0.6$,
$P(B|A_3)=1$

即飞机被击落的概率为 0.458。

实际中还有下面一类问题：“已知结果求原因”。

引例：某人从任一箱中任意摸出一球，发现是红球，求该球是取自1号箱的概率。



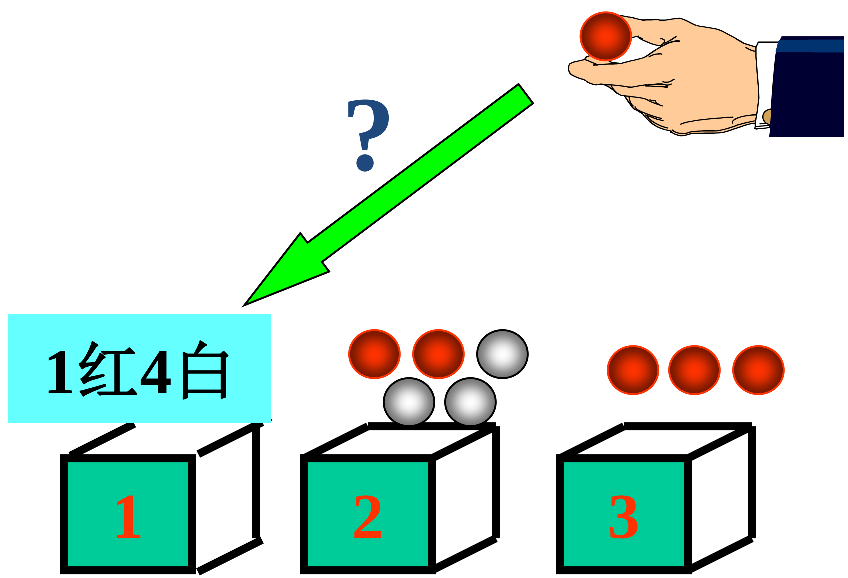
或者问：

该球取自哪号箱的可能性最大?

这一类问题在实际中更为常见，它所求的是条件概率，是已知某结果发生条件下，求各原因发生可能性大小。

引例 ：有三个箱子，分别编号为1,2,3，1号箱装有1个红球4个白球，2号箱装有2个红球3个白球，3号箱装有3个红球。某人从三箱中任取一箱，从中任意摸出一球，发现是红球。

求：该球是取自1号箱的概率

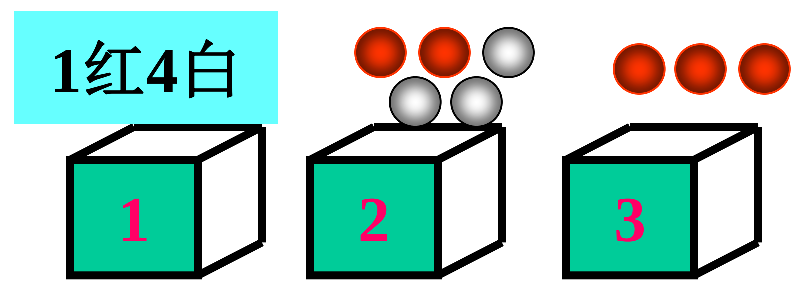


记 B_i={球取自i号箱}, i=1,2,3; A ={取得红球}

求: $P(B_1|A)$

$$P(B_1 \mid A)=\frac{P(AB_1)}{P(A)} = \frac{P(B_1)P(A \mid B_1)}{\sum_{k=1}^{3} P(B_k)P(A \mid B_k)}$$

运用全概率公式
计算$P(A)$



将这里得到的公式一般化，就得到: 贝叶斯公式

3．贝叶斯公式

定理3． 设试验 E 的样本空间为 S，A为 E 的事件，

$B_1, B_2 \cdots B_n$为 S 的一个划分，且 $P(A)>0$，$P(B_i)>0$

则：
$$P(B_i|A)=\frac{P(A|B_i)P(B_i)}{\sum_{j=1}^{n}P(A|B_j)P(B_j)}, i=1,2\cdots n$$

称为贝叶斯 (Bayes) 公式

贝叶斯公式与全概率公式一样都是加法公式和乘法公式的综合运用。

注: ▲ 贝叶斯公式 $P(B_i|A)=\dfrac{P(A|B_i)P(B_i)}{\sum_{j=1}^{n}P(A|B_j)P(B_j)},i=1,2\cdots n$

在贝叶斯公式中，$P(B_i)$ 和 $P(B_i|A)$分别称为原因的先验概率和后验概率.

$P(B_i)$ 是在没有进一步信息（不知道事件A是否发生）的情况下，人们对诸事件发生可能性大小的认识。

当有了新的信息（知道A发生）,人们对诸事件发生可能性大小 $P(B_i|A)$有了新的估计。

▲ 贝叶斯公式适用于“用条件概率求条件概率”

例如，某地发生了一个案件，怀疑对象有甲、乙、丙三人。

在不了解案情细节(事件A)之前，侦破人员根据过去的前科，对他们作案的可能性有一个估计，设为:

偏小

丙	乙	甲
$P(B_1)$	$P(B_2)$	$P(B_3)$

但在知道案情细节后，这个估计就有了变化。

知道A发生后

$P(B_1 \mid A)$	$P(B_2 \mid A)$	$P(B_3 \mid A)$

最大

比如，原来认为作案可能性较小的某甲，现在变成了重点嫌疑犯。（贝叶斯公式从数量上刻划了这种变化）

例11. 在例 9 中已知任取一件产品是次品。

问：此次品出自哪条的流水线的可能性大?

例9. 某工厂有四条流水线生产同一种产品, 四条流水线的产量分别占该产品总产量的15%，20%，25%，40%，且四条流水线生产产品的次品率分别是 0.01, 0.02, 0.03, 0.025。

解：

$$P(B_1|A)=\frac{P(B_1)\cdot P(A|B_1)}{\sum_{j=1}^{4}P(B_j)P(A|B_j)}=\frac{P(B_1)P(A|B_1)}{P(A)}=\frac{0.15\times 0.01}{0.023}=0.065$$

$$P(B_2|A)=\frac{0.2\times 0.02}{0.023}=0.174$$

$$P(B_3|A)=\frac{0.25\times 0.03}{0.023}=0.326$$

$$P(B_4|A)=\frac{0.4\times 0.025}{0.023}=0.435$$

出自第四条流水线可能性大

例 12.某一地区患有癌症的人占0.005，患者对一种试验反应是阳性的概率为0.95，正常人对这种试验反应是阳性的概率为0.04，现抽查了一个人，试验反应是阳性。

问：此人是癌症患者的概率有多大?

解: 设 $C = \{$ 抽查的人患有癌症 $\}$,
$A = \{$ 试验结果是阳性 $\}$,

则 $\overline{C}$ 表示“抽查的人不患癌症”。

$P(C) = 0.005$，$P(\bar{C}) = 0.995$，$P(A|C) = 0.95$，$P(A|\bar{C}) = 0.04$

此例即为求 $P(C \mid A)$

由贝叶斯公式，可得:

$$P(C\mid A)=\frac{P(C)P(A\mid C)}{P(C)P(A\mid C)+P(\overline{C})P(A\mid \overline{C})}$$

代入数据计算得试验结果为阳性的条件下，患癌症的概率:

$$P(C\mid A)=0.1066$$

现在来分析一下结果的意义:

1. 这种试验对于诊断一个人是否患有癌症有无意义?

2. 检出阳性是否一定患有癌症?

分析问题1.

这种试验对于诊断一个人是否患有癌症有无意义?

如果不做试验， 抽查一人, 他是患者的概率:

$$P(C) = 0.005$$

若试验后得阳性反应，则根据试验得来的信息，此人是患者的概率为:

$$P(C \mid A) = 0.1066$$

从0.005 增加到 0.1066，将近增加约 21 倍。

这说明：这种试验对于诊断一个人是否患有癌症是有意义的。

分析问题2.

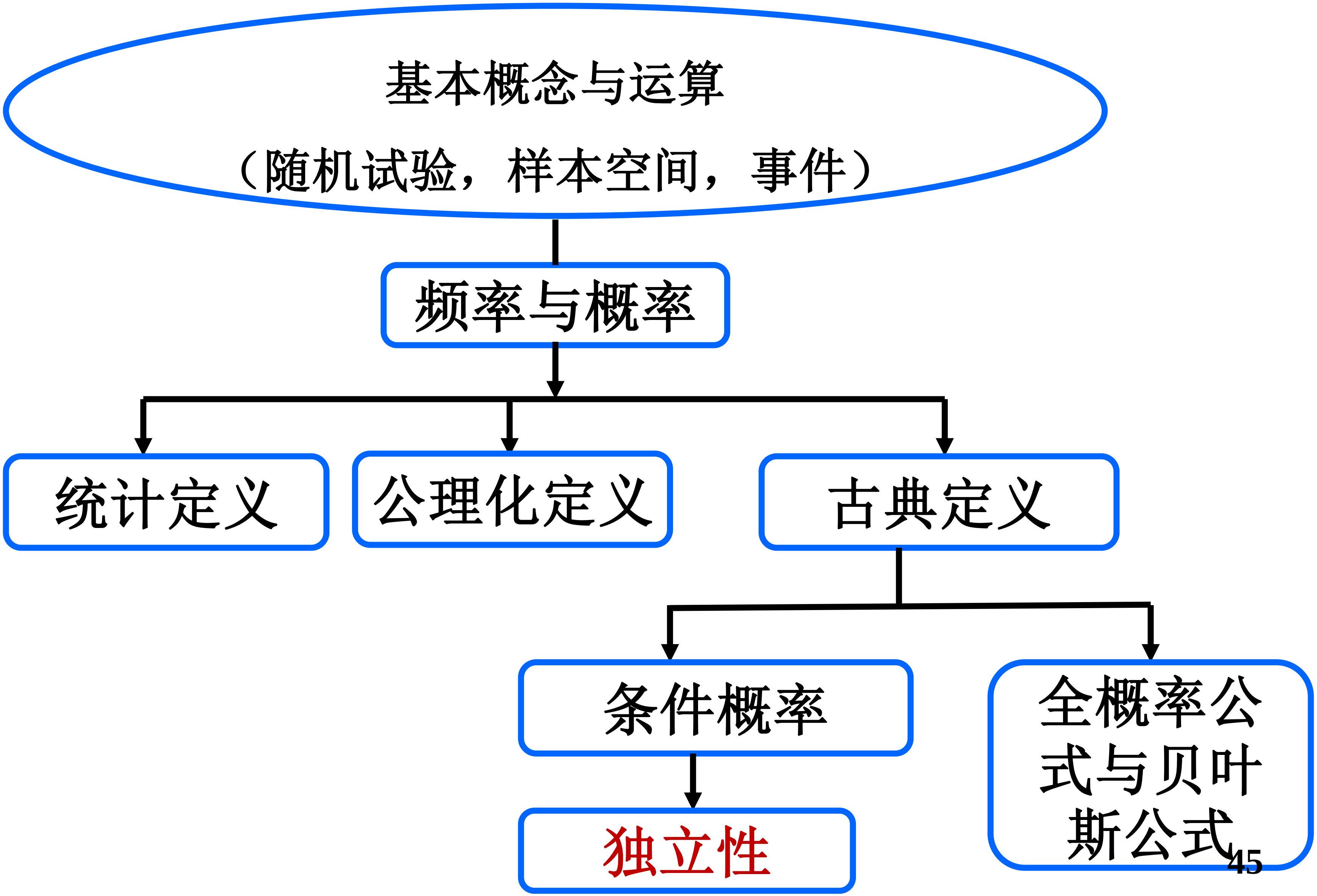
检出阳性是否一定患有癌症?

试验结果为阳性, 此人确患癌症的概率为:

$$P(C \mid A) = 0.1066$$

可见：即使一个人检验出阳性，尚可不必过早下结论此人确患有癌症，因为这种可能性只有 10.66% (平均来说，1000个人中大约只有107人确患癌症) 。

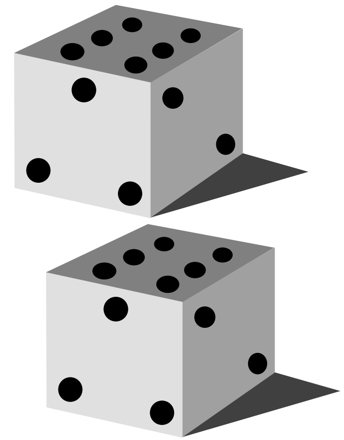
第六节 事件的独立性


基本概念与运算
（随机试验，样本空间，事件）
频率与概率
统计定义
公理化定义
古典定义
条件概率
全概率公式与贝叶斯公式
独立性

引例1. 将一颗均匀骰子连掷两次，设

A={第二次掷出6点}，

B={第一次掷出6点}，



显然： $P(A\,|\,B)=P(A)$

这就是说，已知事件B发生，并不影响事件A 发生的概率，

这时称事件A、B独立。

由乘法公式知，当事件A、B独立时，有：

$$P(AB)=P(A)\,P(B)$$

$$P(AB)=P(B)P(A|B)$$

事件的独立性

定义1. 设 A, B是两个事件，如果具有等式：

$$P(AB) = P(A)P(B)$$

则称 A， B 为相互独立的事件，简称A， B独立。

定理：设 A, B是两事件, 且$P(A) > 0$, 若 A, B相互独立，则 $P(B|A) = P(B)$。

事件的独立性

性质1: 若 A与 B 相互独立 ➡ A 与 $\overline{B}$, $\overline{A}$ 与 B, $\overline{A}$ 与 $\overline{B}$ 也相互独立。

[证]:（只证 A与 $\overline{B}$ 相互独立，其余自证）

$$\because\ P(A\overline{B}) = P(A - AB) \quad \text{而}\ A \supset AB$$

$$= P(A) - P(AB)$$

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

$$= P(A)(1 - P(B)) = P(A)\cdot P(\overline{B})$$

由可减性
与独立性

性质2: 若$P(A) > 0, P(B) > 0$，则A，B相互独立与A，B互不相容不同时成立。

事件的独立性

定义2 (两两独立)：设 A, B, C 三个事件, 如果具有如下等式:

$$\begin{cases} P(AB)=P(A)P(B) \\ P(BC)=P(B)P(C) \\ P(AC)=P(A)P(C) \end{cases}$$

则称 A，B，C 两两独立。

事件的独立性

注： 若A , B , C 两两独立，$P(ABC) = P(A)P(B)P(C)$不一定成立。

因为$P(ABC) = P(C|AB)P(AB)$, 而$P(C|AB)$不一定等于$P(C)$。

例： 随机扔两枚硬币，事件A={第一枚硬币出现正面}，事件B={第二枚硬币出现正面}，事件C={两枚硬币同样一面}。

$P(A)=1/2$，$P(B)=1/2$，$P(C)=1/2$。

$P(AC)=1/4=P(A)P(C)$，$P(BC)=1/4=P(B)P(C)$。

AB的发生会影响C的发生，故$P(C|AB) \neq P(C)$。

事件的独立性

问题： 满足什么条件，$P(ABC) = P(A)P(B)P(C)$ 才能成立？

三个事件的“相互独立”的概念

定义 3. 设 A, B, C 是三个事件，如果具有等式：

$$\begin{cases} P(AB) = P(A)P(B) \\ P(BC) = P(B)P(C) \\ P(AC) = P(A)P(C) \\ P(ABC) = P(A)P(B)P(C) \end{cases}$$

则称事件 A, B, C 为相互独立的事件。

事件的独立性

推广：设 $A_1, A_2, \cdots A_n$ 是 n 个事件, 如果对于任意 $k \quad (1 \le k \le n)$

和任意 $1 \le i_1 < i_2 < \cdots < i_k \le n$，具有等式

$$P(A_{i_1} A_{i_2} \cdots A_{i_k}) = P(A_{i_1}) P(A_{i_2}) \cdots P(A_{i_k})$$

则称 $A_1, A_2, \cdots A_n$ 为相互独立的事件。

事件的独立性

▲ 相互独立与两两独立的关系：

两两独立——n 个事件任何两个彼此独立

相互独立——n个事件任意 k个 $(k \le n)$都是独立的

故相互独立 $\Rightarrow$ 两两独立, 反之则不真

事件的独立性

▲ n 个独立事件**和** 的概率公式:

设事件 $A_1, A_2, \cdots, A_n$ 相互独立, 则

$$P(A_1+\ldots+A_n) = 1 - P(\overline{A_1 + A_2 + \cdots + A_n})$$

$$= 1 - P(\overline{A}_1\overline{A}_2\cdots\overline{A}_n)$$

$$= 1 - P(\overline{A}_1)P(\overline{A}_2)\cdots P(\overline{A}_n)$$

由德摩根律

$\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_n$ 也相互独立

▲ 类似地, $A_1, A_2, \cdots, A_n$ 至少有一个不发生的概率（1-都发生的概率）:

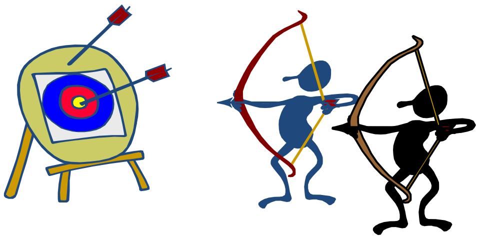
$$P(\overline{A}_1 + \overline{A}_2 + \cdots + \overline{A}_n) = 1 - P(A_1)P(A_2)\cdots P(A_n)$$

事件的独立性

注：在实际应用中，往往根据问题的实际意义去判断两事件是否独立。

例如：甲、乙两人向同一目标射击，记 A={甲命中}，B={乙命中}，A与B是否独立？

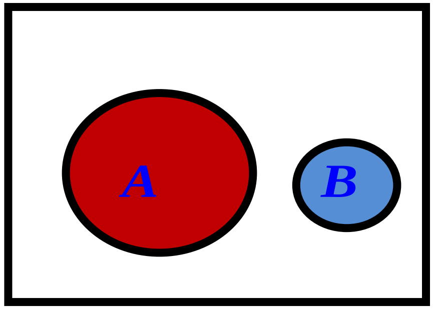
可根据实际意义，由于“甲命中”并不影响“乙命中”的概率，故认为A、B 独立 。（即一事件发生与否并不影响另一事件发生的概率）



例1：

（1）如图的两个事件是独立的吗？

（2）能否在样本空间S 中找两个事件,它们既相互独立又互斥?



解：(1) 因为：$P(AB)=0$

而 $P(A)\neq 0$， $P(B)\neq 0$

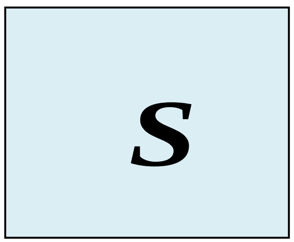
即：$P(AB)\neq P(A)P(B)$

故 A、B不独立

即：若A、B 互斥，且 $P(A)>0$, $P(B)>0$, 则 A 与 B 不独立。

反之，若 A与 B 独立，且 $P(A)>0$，$P(B)>0$, 则 A 、B 不互斥。

（2）所要寻找的这两个事件就是S 和 ϕ



因为: $\phi S = \phi$

所以: $P(S\phi) = P(\phi)P(S) = 0$

则: ϕ 与 S 独立且互斥

注意: ϕ 与任何事件都独立。

独立与互斥的区别和联系的思考题:

(1) 设A、B为互斥事件，且 $P(A) > 0$, $P(B) > 0$, 下面四个结论中，正确的是:

1. $P(B|A) > 0$
2. $P(A|B) = \mathrm{P(A)}$
3. $P(A|B) = 0$
4. $P(AB) = P(A)\,P(B)$

(2) 设A、B为独立事件，且$P(A) > 0$, $P(B) > 0$, 下面四个结论中，正确的是:

1. $P(B|A) > 0$
2. $P(A|B) = P(A)$
3. $P(A|B) = 0$
4. $P(AB) = P(A)\,P(B)$

独立与互斥的区别和联系的思考题:

(1) 设A、B为互斥事件，且 $P(A)>0$, $P(B)>0$,
下面四个结论中，正确的是:

1. $P(B|A) > 0$
2. $P(A|B) = \mathrm{P(A)}$
3. $P(A|B) = 0$
4. $P(AB) = P(A)\,P(B)$

(2) 设A、B为独立事件，且$P(A) > 0$, $P(B) > 0$,
下面四个结论中，正确的是:

1. $P(B|A) > 0$
2. $P(A|B) = P(A)$
3. $P(A|B) = 0$
4. $P(AB) = P(A)\,P(B)$

答案：(1) 3 ；(2) 1，2, 4

例：甲、乙、丙三台机床独立工作,由一个操作者照管, 某段时间内它们不需要操作者照管的概率分别为 0.9，0.8，0.85。

求：(1) 没有 一台机床 不需要 照管的概率（都需要照管）

(2) 至少 一台机床 需要 照管的概率

(3) 至多 一台机床 不需要 照管的概率

解：设 A, B, C：分别表示甲，乙，丙三台机床不需要照管

因为：三台机床要不要照看是相互独立的

$$(1)\ \ P(\bar{A}\bar{B}\bar{C}) = P(\bar{A})P(\bar{B})P(\bar{C})$$

$$= (1-0.9)(1-0.8)(1-0.85) = 0.003$$

$$(2)\ P(\bar{A}\cup\bar{B}\cup\bar{C}) = P(\overline{ABC}) = 1 - P(ABC)$$

$$= 1 - P(A)P(B)P(C)$$

$$= 1 - 0.9\times0.8\times0.85$$

$$= 0.388$$

甲,乙,丙三台机床不需要照管的概率分别为:
0.9, 0.8, 0.85

(3) **D:** 至多只有一台机床不需要照看

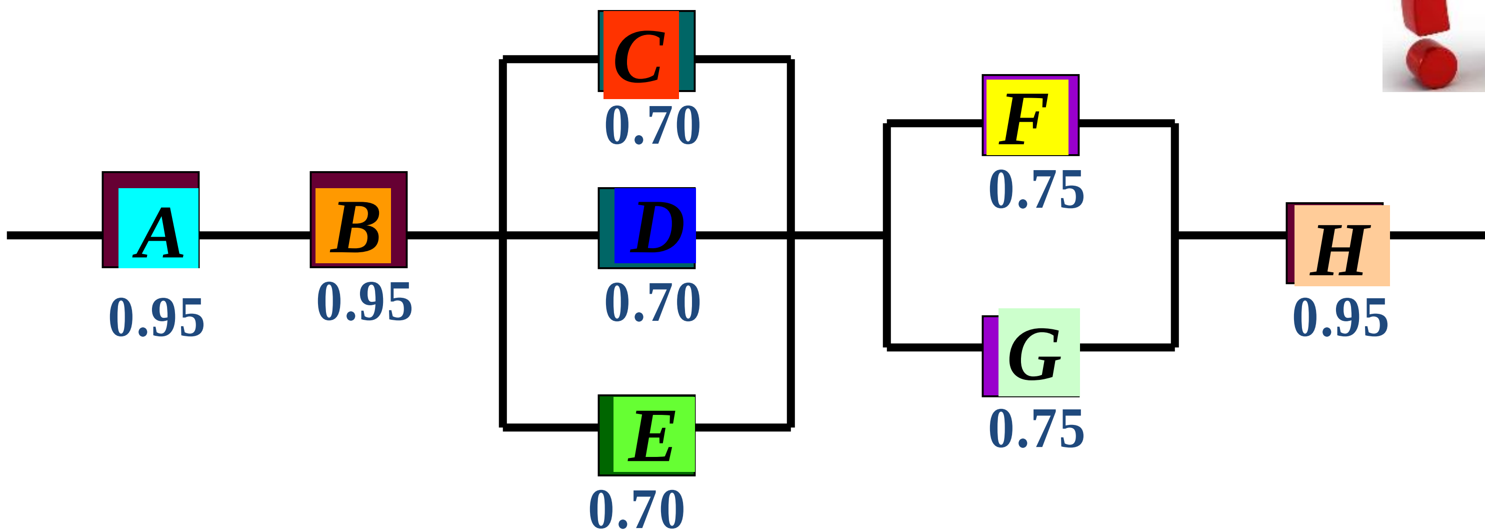
$$P(D) = P(\bar{A}\bar{B}\bar{C}) + P(A\bar{B}\bar{C}) + P(\bar{A}B\bar{C}) + P(\bar{A}\bar{B}C)$$

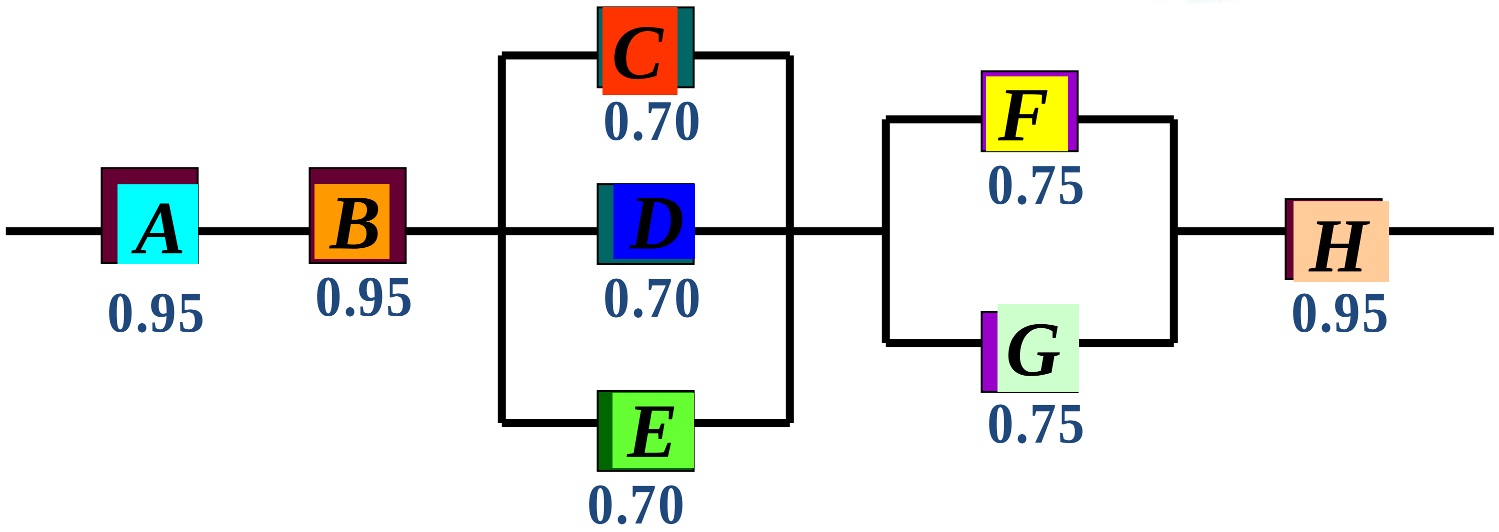
$$= 0.003 + 0.9\times0.2\times0.15 + 0.1\times0.8\times0.15$$

$$+ 0.1\times0.2\times0.85 = 0.059$$

例4. 下图是一个串并联电路示意图．*A*、*B*、*C*、*D*、*E*、*F*、*G*、*H* 都是电路中的元件。 它们下方的数是它们各自正常工作的概率。

求： 电路正常工作的概率。





解：将电路正常工作记为 W，由于各元件独立工作，故有：

$$P(W)=P(A)\,P(B)\,P(C+D+E)\,P(F+G)\,P(H)$$

其中：

$$P(C+D+E)=1-P(\bar{C})P(\bar{D})P(\bar{E})=0.973$$

$$P(F+G)=1-P(\bar{F})P(\bar{G})=0.9375$$

代入得： $P(W)\approx 0.783$

独立试验序列模型

例如 将一骰子掷 10 次, 那么掷 10 次掷骰子的试验便是 10 次独立试验. 如果我们关注于每次试验中点数 6 是否出现, 这便是 10 重伯努利试验. 点数 6 恰好出现 2 次的概率为

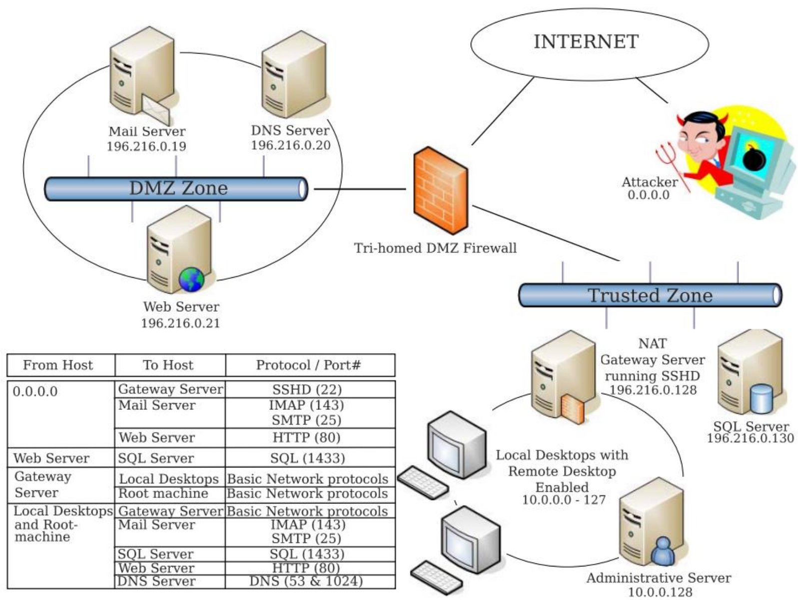
$$p_{10}(2)=C_{10}^{2}\left(\frac{1}{6}\right)^{2}\left(\frac{5}{6}\right)^{8}$$

点数 6 至少出现 2 次的概率为

$$p=\sum_{k=2}^{10}C_{10}^{k}\left(\frac{1}{6}\right)^{k}\left(\frac{5}{6}\right)^{10-k}$$

网络横向移动攻击事件

相互连接关系



From Host	To Host	Protocol / Port#
0.0.0.0	Gateway Server	SSHD (22)
	Mail Server	IMAP (143) SMTP (25)
	Web Server	HTTP (80)
Web Server	SQL Server	SQL (1433)
Gateway Server	Local Desktops	Basic Network protocols
	Root machine	Basic Network protocols
Local Desktops and Root-machine	Gateway Server	Basic Network protocols
	Mail Server	IMAP (143) SMTP (25)
	SQL Server	SQL (1433)
	Web Server	HTTP (80)
	DNS Server	DNS (53 & 1024)

Fig. 1. Test-bed network model.

不安全诱因

TABLE 1
Initial List of Vulnerabilities in Test Network

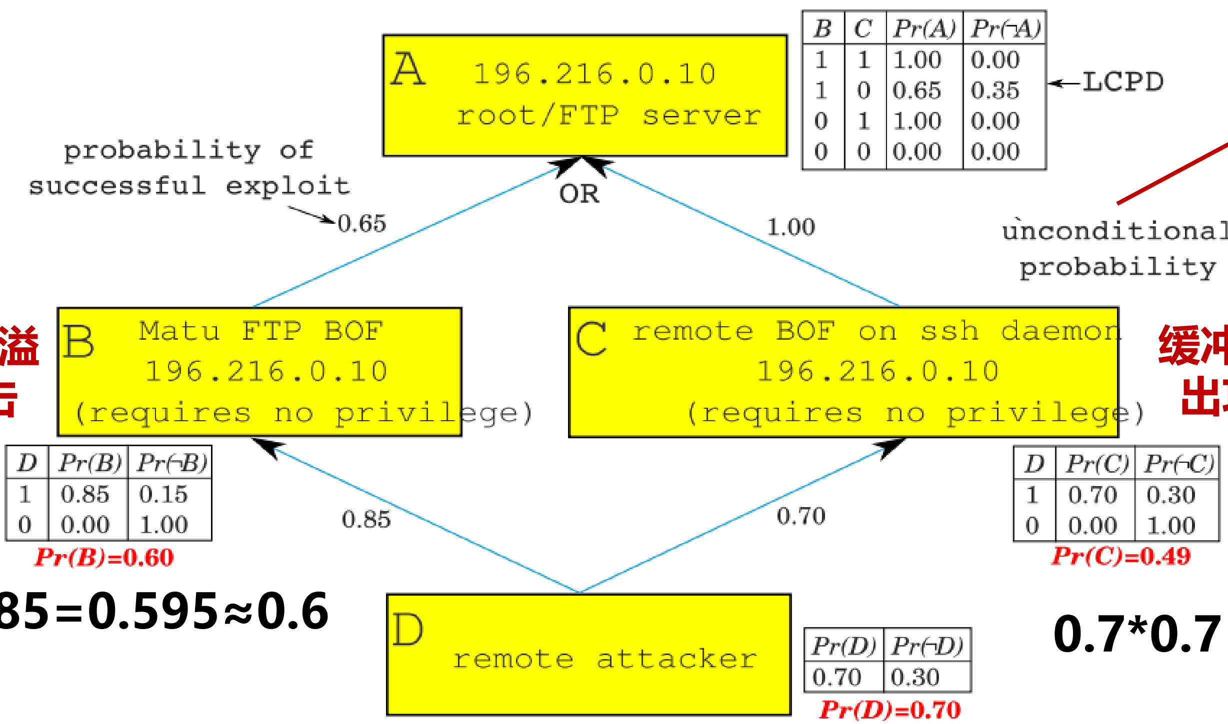
Host	Vulnerability	CVE#	Type of Attack
Local desktops (10.0.0.0-127)	Remote login LICQ Buffer Overflow (BOF) MS Video ActiveX Stack BOF	CA 1996-83 CVE 2001-0439 CVE 2009-0015	remote-2-user remote-2-user remote-2-root
Admin machine (10.0.0.128)	MS SMV service Stack BOF	CVE 2008-4050	local-2-root
Gateway server (196.216.0.128)	OpenSSL uses predictable random Heap corruption in OpenSSH Improper cookies handler in OpenSSH	CVE 2008-0166 CVE 2003-0693 CVE 2007-4752	information leakage local-2-root authentication bypass
SQL Server (196.216.0.130)	SQL Injection	CVE 2008-5416	remote-2-root
Mail Server (196.216.0.19)	Remote code execution in SMTP Error message information leakage Squid port scan vulnerability	CVE 2004-0840 CVE 2008-3060 CVE 2001-1030	remote-2-root account information theft information leakage
DNS Server (196.216.0.20)	DNS Cache Poisoning	CVE 2008-1447	integrity
Web Server (196.216.0.21)	IIS vulnerability in WebDAV service	CVE 2009-1535	remote-2-local authentication bypass

N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74.

网络横向移动攻击事件

Pr(A)=
0.6*0.49+
0.6*0.51*0.65+
0.4*0.49
=0.6889

缓冲区溢出攻击



B	C	Pr(A)	Pr(¬A)
1	1	1.00	0.00
1	0	0.65	0.35
0	1	1.00	0.00
0	0	0.00	0.00

D	Pr(B)	Pr(¬B)
1	0.85	0.15
0	0.00	1.00

D	Pr(C)	Pr(¬C)
1	0.70	0.30
0	0.00	1.00

Pr(D)	Pr(¬D)
0.70	0.30

缓冲区溢出攻击

0.7*0.85=0.595≈0.6

0.7*0.7=0.49

Fig. 3. Simple BAG illustrating probability computations.

N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74.

北京郵電大學
Beijing University of Posts and Telecommunications

网络横向移动攻击事件

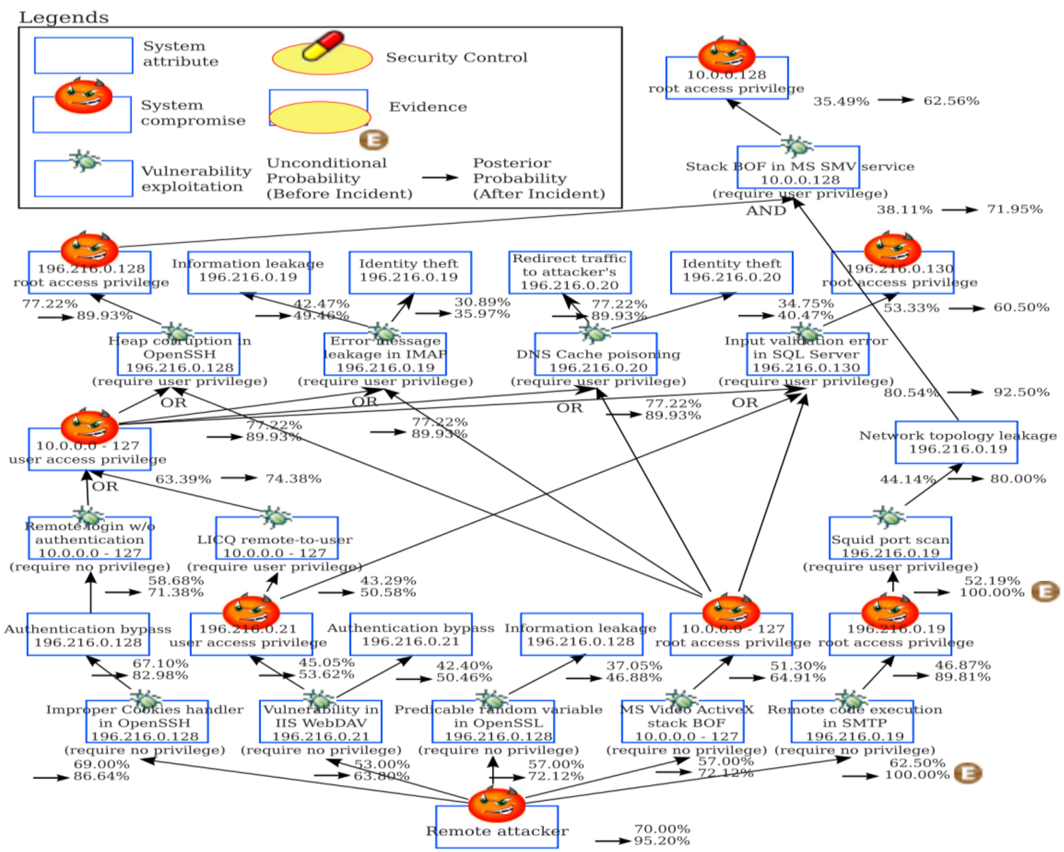


Fig. 2. BAG of test network with unconditional probabilities and posterior probabilities given two attack incidences (marked by Ⓔ).

N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74.

第一章作业（教材第五版）：

P25：1、2、3、4

P26：8、9、10、11、13、14、19

P27：20、21、29

P28：33

P29：35

注：作业不得抄袭；写上姓名、班级、学号和页码（如1/5），9月27日前提交至教学云平台。