第三章 组合数学

3.1 排列与组合

3.2 容斥原理与鸽笼原理

3.3 母函数

3.4* 指数母函数

3.5* 组合数学在信息安全中的应用

3.4 指数母函数

➢ 指数母函数可以用来解决允许重复并且重复有限制的排列问题。

例 6 设 $S=\{a,b,c\}$，现从 S 中任取 r 个，要求 a 的个数不超过 3，b 的个数不超过2，c 的个数不超过3， 求排列方案数。

解 用 x_1,x_2,x_3 表示 a,b,c，计算

$$\left(1+x_1+x_1^2+x_1^3\right)\left(1+x_2+x_2^2\right)\left(1+x_3+x_3^2+x_3^2\right)$$

$$=1+(x_1+x_2+x_3)+\left(x_1^2+x_1x_2+x_2^2+x_1x_3+x_2x_3+x_3^2\right)$$

$$+\cdots$$

$$+\left(x_1x_3^3+x_2x_3^3+x_1^2x_2^2+x_1x_2x_3^2+x_2^2x_3^2+x_1^3x_3+x_1^2x_2x_3\right.$$

3.4 指数母函数

例 6 设 $S=\{a,b,c\}$，现从 S 中任取 r 个，要求 a 的个数不超过3，b 的个数不超过2，c 的个数不超过3， 求排列方案数。

解（续）上述多项式中4次方项为:

$$x_1x_3^3,\quad x_2x_3^3,\quad x_1^2x_2^2,\quad x_1x_2x_3^2,\quad x_2^2x_3^2,$$
$$x_1^3x_3,\quad x_1^2x_2x_3,\quad x_1x_2^2x_3,\quad x_1^3x_2,\quad x_1^2x_3^2$$

对于 $x_1^2x_2^2$ 表明2个 a 和2个 c 的4组合，可以得到 $4!/2!\,2!=6$ 个4排列。于是，4个元素的排列数 p_4 为

$$p_4=4!\left(\frac{1}{1!3!}+\frac{1}{1!3!}+\frac{1}{2!2!}+\frac{1}{1!1!2!}+\frac{1}{2!2!}+\frac{1}{1!3!}+\frac{1}{1!1!2!}+\frac{1}{1!2!1!}+\right.$$

3.4 指数母函数

例 6 设 $S=\{a,b,c\}$，现从 S 中任取 r 个，要求 a 的个数不超过3，b 的个数不超过2，c 的个数不超过3， 求排列方案数。

解（续）因此可以得到序列 $p_0,p_1,p_2,\ldots p_n,\ldots$ 的指数型母函数

$$G_e(x)=p_0+p_1\frac{x}{1!}+p_2\frac{x^2}{2!}+\cdots+p_n\frac{x^n}{n!}+\cdots$$

$$=\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}\right)\left(1+\frac{x}{1!}+\frac{x^2}{2!}\right)\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}\right)$$

$$=1+3\frac{x}{1!}+9\frac{x^2}{2!}+28\frac{x^3}{3!}+70\frac{x^4}{4!}+170\frac{x^5}{5!}+350\frac{x^6}{6!}$$

$$+420\frac{x^7}{7!}+560\frac{x^8}{8!}$$

3.4 指数母函数

例 6 设 $S=\{a,b,c\}$，现从 S 中任取 r 个，要求 a 的个数不超过3，b 的个数不超过2，c 的个数不超过3， 求排列方案数。

解（续）注意到，事实上，

$$70\frac{x^4}{4!}=\left(\frac{1}{1!3!}+\frac{1}{1!3!}+\frac{1}{2!2!}+\frac{1}{1!1!2!}+\frac{1}{2!2!}+\frac{1}{1!3!}+\frac{1}{1!1!2!}+\frac{1}{1!2!1!}+\right.$$

6.4 指数母函数

定义3.12 对于序列$a_0,a_1,a_2,\ldots$， 函数

$$G_e(x)=a_0+\frac{a_1}{1!}x+\frac{a_2}{2!}x^2+\frac{a_3}{3!}x^3+\cdots+\frac{a_k}{k!}x^k+\cdots$$

称为序列$a_0,a_1,a_2,\ldots$对应的**指数型母函数**。

➢对于一个多重集，其中a_1重复n_1次，a_2重复n_2次，…，a_k重复n_k次，从中取r个排列的不同排列数所对应的指数型母函数为：

$$G_e(x)=\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^{n_1}}{n_1!}\right)$$

$$\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^{n_2}}{n_2!}\right)\cdots\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^{n_k}}{n_k!}\right).$$

6.4 指数母函数

例3 求由1，3，5，7，9五个数字组成的n位数的个数，要求其中3，7出现的次数为偶数，其他1，5，9出现次数不加限制。

设满足上述条件的n位数个数为c_n，则其对应的指数型母函数为：

$$G_e(x) = \left(1+\frac{x^2}{2!}+\frac{x^4}{4!}+\cdots\right)^2\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)^3$$

$$=\left(\frac{e^x+e^{-x}}{2}\right)^2\left(e^x\right)^3$$

6.4 指数母函数

$$G_e(x)=\frac{1}{4}(e^{2x}+2+e^{-2x})e^{3x}$$

$$=\frac{1}{4}(e^{5x}+2e^{3x}+e^{x})$$

$$=\frac{1}{4}\left(\sum_{n=0}^{\infty}\frac{5^n}{n!}x^n+2\sum_{n=0}^{\infty}\frac{3^n x^n}{n!}+\sum_{n=0}^{\infty}\frac{x^n}{n!}\right)$$

$$=\frac{1}{4}\sum_{n=0}^{\infty}(5^n+2\cdot 3^n+1)\frac{x^n}{n!}.$$

因此

$$a_n=\frac{1}{4}(5^n+2\cdot 3^n+1).$$

6.4 指数母函数

例4 7个有区别的球放进4个有标志的盒子里，要求1，2两个盒子必须有偶数个球，第3个盒子有奇数个球，求不同的方案个数。

解：这相当于从1234这4个数中取7个做允许重复的排列，即每个数字对应于每个球所放的盒子的序号。

这样的排列数所对应的指数型母函数为：

$$G_e(x)=\left(1+\frac{x^2}{2!}+\frac{x^4}{4!}+\cdots\right)^2\left(\frac{x}{1!}+\frac{x^3}{3!}+\cdots\right)\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots\right)$$

$$=\left(\frac{e^x+e^{-x}}{2}\right)^2\left(\frac{e^x-e^{-x}}{2}\right)e^x$$

6.4 指数母函数

$$G_e(x)=\frac{1}{8}(e^{4x}-1+e^{2x}-e^{-2x})$$

$$=\frac{1}{8}\left\{-1+\sum_{n=1}^{\infty}\left[4^n+2^n-(-2)^n\right]\frac{x^n}{n!}\right\}.$$

因此

$$a_n=\frac{1}{8}\left[4^n+2^n-(-2)^n\right],$$

$$a_7=\frac{1}{8}\left[4^7+2^7-(-2)^7\right]=2080.$$

6.4 指数母函数

例5 r个有标志的球放进n个不同的盒子里，要求无一空盒，问有多少种不同的分配方案?

解：这相当于从1到n这n个数字中取r个做允许重复的排列，即每个数字对应于每个球所放的盒子的序号。

要求无一空盒即相当于要求每个数字至少出现一次。

这样的排列数所对应的指数型母函数为：

$$G_e(x)=\left(\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)^n$$

6.4 指数母函数

$$G_e(x)=\left(e^x-1\right)^n$$

$$=\sum_{k=0}^{\infty}\binom{n}{k}(e^x)^{n-k}(-1)^k$$

$$=\sum_{k=0}^{\infty}\left[\binom{n}{k}\sum_{r=0}^{\infty}\frac{(n-k)^r}{r!}x^r\right](-1)^k$$

$$=\sum_{r=0}^{\infty}\left[\sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^r\right]\frac{x^r}{r!},$$

因此

$$a_r=\sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^r.$$

第三章 组合数学

3.1 排列与组合

3.2 容斥原理与鸽笼原理

3.3 母函数

3.4* 指数母函数

3.5* 组合数学在信息安全中的应用

3.5 组合数学在信息安全中的应用

➢ **Hash函数及其组合基础**

对于 $x \in \{0,1\}^*$，计算 $y = H(x) \in \{0,1\}^n$，满足

1. 单向性（抗原像攻击）：给定输出 y，计算输入 x，使得 $y = H(x)$ 是困难的。
2. 弱抗碰撞性（抗第二原像攻击）：给定输入 x，计算另一输入 x'，使得 $H(x') = H(x)$ 是困难的。
3. 强抗碰撞性（抗碰撞攻击）：寻找两个不同输入 x, x'，使得 $H(x') = H(x)$ 是困难的。

3.5 组合数学在信息安全中的应用

例 3.34 已知 Hash 函数 H 的所有可能的输出值为 $n=2^m$ 个，即该 Hash 函数的消息摘要为 m bit，y 是一个给定的输出值。如果对 H 随机地取 k 个输入，则至少有 1 个输入值 x，使得 $H(x)=y$ 的概率为 0.5，k 有多大？

解 因为 Hash 函数 H 有 $n=2^m$ 个可能的输出，所以输入值 x 产生的输出值 $H(x)$ 等于给定值 y 的概率为 $1/n$，反过来讲，$H(x)\neq y$ 的概率为 $1-1/n$。x 值输入取 k 个随机值而函数 H 的 k 个输出值中没有一个等于 y，其概率等于每个输出都不等于 y 的概率之积，即 $(1-1/n)^k$，因此 x 取 k 个随机值得到函数的 k 个输出值中至少有 1 个等于 y 的概率为 $1-(1-1/n)^k$。注意到当 a 充分小时，$(1+a)^k\approx 1+ak$，故

$$1-(1-1/n)^k=1-(1-k/n)=k/n$$

若使上述概率等于 0.5，那么 $k=n/2=2^{m-1}$。 □

3.5 组合数学在信息安全中的应用

➢ **Hash函数的生日攻击**

例 3.35 已知 Hash 函数 H 的所有可能的输出值为 $n=2^m$ 个，即该 Hash 函数的消息摘要为 m bit，如果对 H 随机地取 k 个输入值，则至少有 2 个输入值 x 和 y，使得 $H(x)=H(y)$ 的概率为 0.5，k 有多大？

解 记 $P(n,k)$ 表示 k 个随机输入中至少有 2 个的输出值相同的概率，$Q(n,k)$ 表示 k 个随机输入中任意 2 个的输出值都不相同的概率，则 $P(n,k)=1-Q(n,k)$。下面计算 $Q(n,k)$，当 $k>n$ 时，k 个随机输入中至少有 2 个的输出值相同，这时 $Q(n,k)=0$，从而 $P(n,k)=1$。当 $k\leqslant n$ 时，k 个随机输入中任意 2 个的输出值都不相同的所有取值方式的个数为

$$n\times(n-1)\times(n-2)\times\cdots\times(n-k+1)=\frac{n!}{(n-k)!}$$

3.5 组合数学在信息安全中的应用

例3.35 解（续）

即第一个数据项可以从 n 个中任取一个，第二个数据项可在剩余的 $n-1$ 个中任取一个，依次类推，最后一个数据项可以从 $n-k+1$ 个值中任取一个。注意到 k 个随机输入的全部取值方式共有 n^k，故

$$Q(n,k)=\frac{n!}{(n-k)!n^k} \qquad P(n,k)=1-\frac{n!}{(n-k)!n^k}$$

如果要求 $P(n,k)=0.5$，可得 $k=1.18\sqrt{n}\approx\sqrt{n}$。 □

例（生日悖论）：随机选择的23个成员的组里面，至少有两个人生日相同的概率至少为1/2。

事实上，$H(x)$ 表示某人 x 的生日（设范围是365天），则生日相同表示找到 x,x' 碰撞。生日悖论说明了当选取 $Q=1.18\sqrt{365}\approx 23$ 个人时，至少有两个人生日相同的概率至少为1/2。

3.5 组合数学在信息安全中的应用

- **Hash函数攻击复杂度分析**

1. 抗原像攻击/抗第二原像攻击：复杂度 $O(2^m)$。
2. 抗碰撞攻击：复杂度 $O\left(2^{m/2}\right)$。