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

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

组合数学概述

- 组合数学是一门古老的学科。
- 计算机出现以后，由于离散对象的处理是计算机科学的核心，研究离散对象的组合数学得到迅猛发展。

组合数学概述-幻方问题

- 1977年美国旅行者1号、2号宇宙飞船就带上了幻方以作为人类智慧的信号。

2200BC

4	9	2
3	5	7
8	1	6

神农幻方

15世纪

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

4阶幻方


百子回歸圖
82 25 29 89 100 13 52 70 10 35
84 75 41 17 18 87 40 48 57 38
81 93 53 24 86 26 85 39 03 15
33 76 09 54 16 14 61 59 92 91
45 64 01 78 19 99 22 60 43 74
67 63 96 47 12 20 27 42 73 58
05 66 55 11 97 49 98 62 30 32
08 34 90 83 46 68 56 04 95 21
06 07 80 37 88 79 28 77 31 72
94 02 51 65 23 50 36 44 71 69

3.1 排列与组合—加法法则与乘法法则

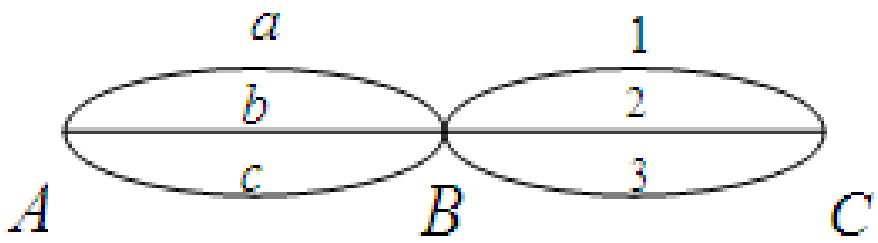
- **加法法则：** 设A和B是两类不同的事件，若事件A有m种产生方式，事件B有n种产生方式，则“事件A或事件B”有$m+n$种产生方式.

- **乘法法则：** 设A和B是两类不同的事件，若事件A有m种产生方式，事件B有n种产生方式，则“事件A与事件B”有mn种产生方式.

3.1 排列与组合—加法法则与乘法法则

例 1 一个学生想选修一门数学课程或一门生物课程，但两者不同时选，如果学校开有4门数学课程和3门生物课程，则该学生可以有7种不同的选课方式.

例 2 设A到B有3条不同的路径，B到C也有3条不同的路径，则从A经过B到C有$3\times3=9$ 条不同的路径.



例 3 比10000小且数字中含有1的正整数个数?

3.1 排列与组合

本小节将解决如下问题：

1. 不允许重复的排列、不允许重复的组合
2. 允许重复的排列、允许重复的组合
3. （不）可辨别的物体放入（不）可辨别的盒子

母函数与指数母函数将解决：

1. 有重复且重复有限制的组合
2. 有重复且重复有限制的排列

3.1 排列与组合—不允许重复的排列

定义3.1 从n个不同的元素中取出r个，将这r个元素按次序排列所得到的结果称为这n个元素的 **r-排列**。

- 所有r排列的个数记为 $P(n,r)$ 或 P_n^r
- n-排列通常称为全排列。

(1) 由乘法规则：

$$P(n,r)=n(n-1)\cdots(n-r+1)=\frac{n!}{(n-r)!}$$

(2) $P(n,r)=0\ (r>n)$, $P(n,1)=1$, $P(n,n)=n!$

3.1 排列与组合—不允许重复的组合

定义3.2 从n个不同的元素中，不考虑次序取出r个所得到的结果，称为这n个元素的一个**r-组合**。

- 所有r-组合的个数记为 $C(n,r), C_n^r$ 或 $\binom{n}{r}$。

（1）由乘法规则：$P(n,r) = C(n,r)P(r,r)$

$$C(n,r) = \frac{P(n,r)}{P(r,r)} = \frac{n!}{r!\,(n-r)!}$$

（2）$C_n^0 = 1, \quad C_n^n = 1$

3.1 排列与组合—不允许重复的组合

例4 从1～300之间任取3个不同的数，使得这3个数的和正好被3除尽，问共有多少种不同的取法？

解：构造余数集合

$$A = \{x \mid 1 \le x \le 300, x \equiv 0 \bmod 3\}$$

$$B = \{x \mid 1 \le x \le 300, x \equiv 1 \bmod 3\}$$

$$C = \{x \mid 1 \le x \le 300, x \equiv 2 \bmod 3\}$$

- 3个不同的数同属A：C_{100}^{3}
- 3个不同的数同属B：C_{100}^{3}
- 3个不同的数同属C：C_{100}^{3}
- 3个不同的数分别属于A, B, C：$C_{100}^{1}C_{100}^{1}C_{100}^{1}$

根据加法法则：共有 $3 \times C_{100}^{3} + \left(C_{100}^{1}\right)^{3} =$ **1485100**种方案。

3.1 排列与组合–允许重复排列与组合

定理3.3

具有 n 个对象的集合允许重复的 r 排列数是

$$n^r$$

例 5 用英文大写字母可以构成多少个长度为 r 的字符串?

解 因为有26 个大写字母，且每个字母可以被重复使用，所以由乘积法则可以看出存在 26^r 个长度为 r 的字符串。

3.1 排列与组合-允许重复排列与组合

定理3.4

具有 n 个对象的集合允许重复的 r 组合数是

$$C(n+r-1,r)=C(n+r-1,n-1)$$

例 6 从包含苹果、橙子和梨的碗里选 4 个水果。如果不计顺序，只关心水果的类型，那么当碗中每类水果至少有 4 个时有多少种选法?

解 具有 3 个对象的集合允许重复的 4 组合数

$$C(7-1,2)=C(6,2)=15$$

3.1 排列与组合-允许重复排列与组合

苹果	橙子	梨
* * *	*	
*	* *	*
* *	*	* *
*		* * *
*	*	* *
⋮		

因此，当允许重复时，n 元素集合的每个 r 组合可以用 $n-1$ 条竖线和 r 颗星的列表来表示。

3.1 排列与组合–允许重复排列与组合

例 7 方程

$$x_1 + x_2 + x_3 = 11$$

有多少个非负整数解？

解 解的个数等于 3 元素集合允许重复的 11 组合数。

由**定理3.4**，存在解的个数为

$$C(3 + 11 - 1, 2) = C(13,2) = 78$$

3.1 排列与组合-允许重复排列与组合

允许和不允许重复的组合与排列

类型	是否允许重复	公式
r 排列	否	$\frac{n!}{(n-r)!}$
r 组合	否	$\frac{n!}{r!\,(n-r)!}$
r 排列	是	n^r
r 组合	是	$\frac{(n+r-1)!}{r!\,(n-1)!}$

3.1 排列与组合-允许重复排列与组合

定理3.5

设类型 1 的相同的物体有 n_1 个，类型 2 的相同的物体有 n_2 个，…，类型 k 的相同的物体有 n_k 个，那么 $n = n_1 + \cdots + n_k$ 个物体的不同排列数是 $\dfrac{n!}{n_1!n_2!\cdots n_k!}$

例 8 重新排序单词SUCCESS 中的字母能构成多少个不同的串？

解 由定理 3.5，7 个物体的不同排列数是

$$\frac{7!}{3!\,2!\,1!\,1!} = 420$$

3.1 排列与组合–物体放入盒子

- 把物体放入盒子
  - 可辨别的物体与可辨别的盒子
  - 不可辨别的物体与可辨别的盒子

  容易计算
  - 可辨别的物体与不可辨别的盒子
  - 不可辨别的物体与不可辨别的盒子

  不容易计算

3.1 排列与组合–物体放入盒子

- 把物体放入盒子
  - 可辨别的物体与可辨别的盒子

定理3.6

把 n 个不同的物体分配到 k 个不同的盒子使得 n_i 个物体放入盒子 i （ $i = 1,2,\ldots,k$）的方式数等于

$$\frac{n!}{n_1!\,n_2!\cdots n_k!}$$

3.1 排列与组合–物体放入盒子

- 把物体放入盒子
  - 不可辨别的物体与可辨别的盒子

定理3.7

把 n 个不可辨别的物体分配到 k 个可辨别的盒子的方式数等于

$$C(k+n-1, k-1)$$

注：

- 上述问题等价于有重复且重复**无限制**的组合。
- 有重复但重复**有限制**的组合问题见3.3母函数。

3.1 排列与组合-物体放入盒子

- 把物体放入盒子
  - 可辨别的物体与不可辨别的盒子

定理3.8

把 n 个可辨别的物体分配到 k 个不可辨别的盒子的方式数等于

$$\sum_{j=1}^{k} S(n,j) = \sum_{j=1}^{k} \frac{1}{j!} \sum_{i=0}^{j-1} (-1)^i \binom{j}{i} (j-i)^n$$

其中，$S(n,j)$ 表示 n 个可辨别的物体放入 j 个不可辨别的盒子（不允许空）的方式数，$S(n,j)$ 称为第二类斯特林数（Stirling数）。

3.1 排列与组合–物体放入盒子

例 9 将4 个不同的雇员安排在3 间不可辨别的办公室，有多少种方式？其中每间办公室可以安排任意个数的雇员。

解 上述每一种安排方式都可以用把A 、B 、C 、D 分成不相交的子集的方式来表示。

1. 4 个雇员排 1 间，$S(4,1)=1$：$\{\{A,B,C,D\}\}$
2. 4 个雇员排 2 间，$S(4,2)=7$:

$$\{\{A,B,C\},\{D\}\},\{\{A,B,D\},\{C\}\},$$
$$\{\{A,C,D\},\{B\}\},\{\{B,C,D\},\{A\}\},$$
$$\{\{A,B\},\{C,D\}\},\{\{A,C\},\{B,D\}\},\{\{A,D\},\{B,C\}\}$$

3. 4 个雇员排 3 间，$S(4,3)=6$:

$$\{\{A,B\},\{C\},\{D\}\},\{\{A,C\},\{B\},\{D\}\},\{\{A,D\},\{B\},\{C\}\},$$
$$\{\{B,C\},\{A\},\{D\}\},\{\{B,D\},\{A\},\{C\}\},\{\{C,D\},\{A\},\{B\}\}$$

3.1 排列与组合–物体放入盒子

- **不可辨别**的物体与**不可辨别**的盒子

例 10 将同一本书的 6 个副本放到 4 个相同的盒子里，其中每个盒子都能容纳 6 个副本，有多少种不同的方式？

解 按照具有最多副本数的盒子的递减次序依次列出每个盒子里的副本数，得到 9 中方式：

6,
5, 1
4, 2
4, 1, 1
3, 3
3, 2, 1
3, 1, 1, 1
2, 2, 2
2, 2, 1, 1

3.1 排列与组合–物体放入盒子

定义3.9

如果 $a_1 + a_2 + \cdots + a_j = n$， 其中 $a_1, a_2, \ldots, a_j$ 都是正整数，且 $a_1 \geq a_2 \geq \cdots \geq a_j$，那么就说 $a_1, a_2, \ldots, a_j$ 是将正整数 n 划分成 j 个正整数的一个**划分**。

将 n 个不可辨别的物体放入 k 个不可辨别的盒子里的方式数就是将正整数 n 划分成最多 k 个正整数的方式数， 记为 $p_k(n)$，关于这个数，我们没有更简单的公式来表示它。**整数划分问题有递归的解。**

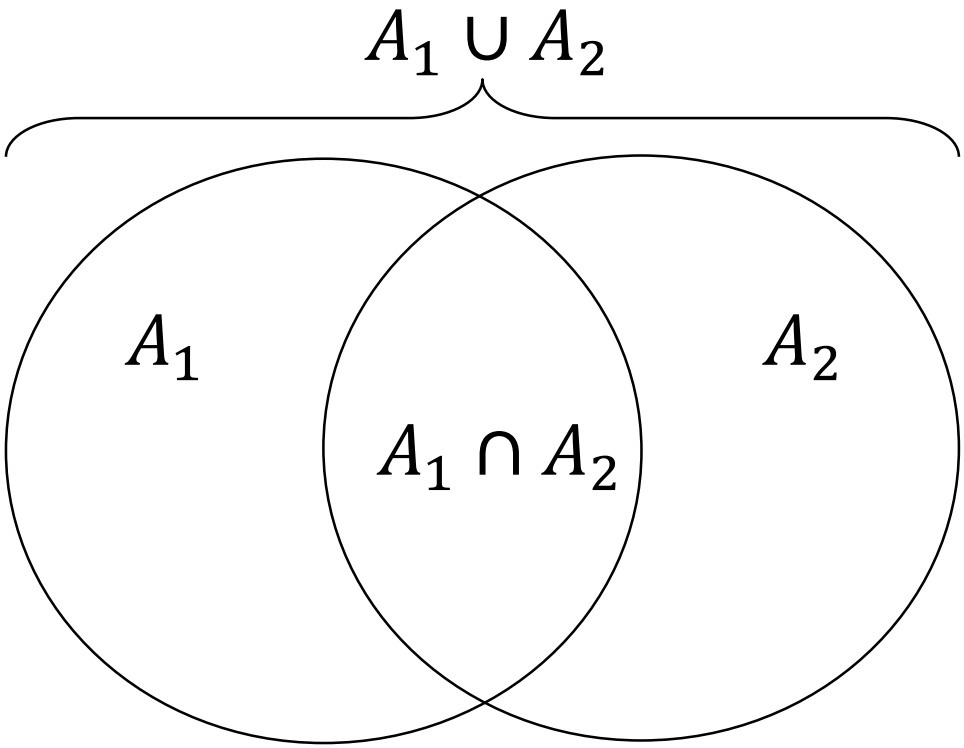
第三章 组合数学

- 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

3.2 容斥原理与鸽笼原理—容斥原理

容斥原理：从集合 A_1 或 A_2 中选择一个元素的方法有

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$



3.2 容斥原理与鸽笼原理—容斥原理

定理3.10 设 $A_1, A_2, \ldots, A_n$ 为有限集合，则

（1） $|A_1 \cup A_2 \cup \cdots \cup A_n|$

$$= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j|$$

$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots$$

$$+ (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|$$

（2） $|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup A_2 \cup \cdots \cup A_n}|$

$$= N - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

这里 N 为所讨论元素的总数。

3.2 容斥原理与鸽笼原理—容斥原理

例 1 求由 a,b,c,d,e,f 这6个字符构成的全排列中不允许出现 cdf 和 ab 的排列的数量。

解：全排列 $|A| = 6!$。令 A_1, A_2 分别表示 A 中出现 cdf 和 ab 的排列集合，则 $|A_1| = 4!$, $|A_2| = 5!$，$|A_1 \cap A_2| = 3!$，故根据容斥原理，

$$|\overline{A_1} \cap \overline{A_2}| = |A| - |A_1| - |A_2| + |A_1 \cap A_2|$$
$$= 6! - 5! - 4! + 3! = 582$$

3.2 容斥原理与鸽笼原理—容斥原理

例 2 求1-1000的整数中被3或5整除的数的个数。

解：令 A_1, A_2 分别表示1-1000的整数中3的倍数集合和5的倍数集合，则

$$|A_1| = \left\lfloor \frac{1000}{3} \right\rfloor = 333 , |A_2| = \left\lfloor \frac{1000}{5} \right\rfloor = 200,$$

$|A_1 \cap A_2| = \left\lfloor \frac{1000}{15} \right\rfloor = 66$，故根据容斥原理，

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$
$$= 333 + 200 - 66 = 467$$

3.2 容斥原理与鸽笼原理—鸽笼原理

- 有 20 只鸽子要飞往 19 个鸽巢栖息，则鸽巢中至少有1 个鸽巢里最少栖息着 2 只鸽子。

鸽巢原理（抽屉原理）
如果是 $k+1$ 个或更多的物体放入 k 个盒子， 那么至少有一个盒子包含了至少 **2** 个物体。

证 假定 k 个盒子中没有一个盒子包含的物体多于 1 个， 那么物体总数至多是 k， 这与至少有 $k+1$ 个物体矛盾。

3.2 容斥原理与鸽笼原理—鸽笼原理

推论3.11

一个从有 $k+1$ 甚至更多的元素的集合到 k 个元素集合的函数 f 不是一对一函数。

例 3 在一组 367 个人中一定至少有 2 个人有相同的生日，这是由于只有 366 个可能的生日。

例 4 在 27 个英文单词中一定至少有 2 个单词以同一个字母开始，因为英文字母表中只有 26 个字母。

例 5 证明：对每个整数 n，存在一个数是 n 的倍数且在它的十进制表示中只出现 0 和 1。

解 令 n 是正整数。考虑 $n+1$ 个整数

$$1, 11, 111, \ldots, \overbrace{11\cdots1}^{n+1}$$

当一个整数被 n 整除时存在 n 个可能的余数。因为上表中有 $n+1$ 个整数，由鸽巢原理，必有两个整数在除以 n 时有相同的余数。这两个整数之差的十进制表示中只含有 0 和 1，且它能被 n 整除。

- **广义鸽巢原理**

当物体数超过盒子数的**倍数**时可以得出更多的结果。

广义鸽巢原理
如果是 N 个物体放入 k 个盒子， 那么至少有一个盒子包含了至少 $\lceil N/k \rceil$ 个物体。

证 假定 k 个盒子中任何一个盒子包含的物体都小于 $\lceil N/k \rceil$ 个， 那么物体总数至多是

$$k \cdot \left(\left\lceil \frac{N}{k} \right\rceil - 1 \right) < k \left(\left(\frac{N}{k} + 1 \right) - 1 \right) = N$$

问题：把一些物体分到 k 个盒子中要使得某个盒子至少含有 r 个物体，求这些物体的**最少**个数。

解 当有 N 个物体时，只要 $\lceil N/k \rceil \geq r$，一定有 r 个物体在同一个盒子里。满足 $N/k > r-1$ 的最小正整数 N，即

$$\boldsymbol{N = k(r-1)+1}$$

是满足 $\lceil N/k \rceil \geq r$ 的最小正整数。

例 6 在 100 个人中至少有

$$\left\lceil \frac{100}{12} \right\rceil = 9$$

个人生在同一个月。

例 7 如果有5 个可能的成绩A 、B 、C 、D 和F ，那么在一个离散数学班里最少有多少个学生才能保证至少6 个学生得到相同的分数？

解 需要的最少学生数是使得 $\lceil N/5 \rceil = 6$ 的最小整数 N。经计算，

$$N = 5(6-1) + 1 = 26$$

- **鸽巢原理的简单应用**

例 8 证明在不超过 $2n$ 的任意 $n+1$ 个正整数中一定存在一个正整数被另一个正整数整除。

解 对任意不超过 $2n$ 的正整数 $a_1, a_2, \ldots, a_{n+1}$，我们写成形式 $a_j = 2^{k_j} q_j$，$j = 1,2, \ldots, n+1$，其中整数 $k_j \geq 0$, 奇数 $q_j < 2n$。

由于小于 $2n$ 的正奇数一共有 n 个，所以**由鸽巢原理**，$q_1, q_2, \ldots, q_{n+1}$ 中必有两个相等。于是，存在整数 i 和 j 使得 $q_i = q_j = q$，即

$$a_i = 2^{k_i} q, \qquad a_j = 2^{k_j} q$$

因此，$a_i \mid a_j$ 如果 $k_i < k_j$；$a_j \mid a_i$ 如果 $k_j < k_i$。

- **鸽巢原理的简单应用**

例 9 假定一组有 6 个人，任意两个人或者是朋友或者是敌人。证明在这组人中或存在 3个人彼此都是朋友，或存在 3 个人彼此都是敌人。

解 令 A 是6 个人中的一人，则从广义鸽巢原理得出组里其他 5 个人中至少有 $\lceil 5/2 \rceil = 3$ 个人是A 的朋友，或至少有 3 个人是 A 的敌人。

1. 假定 B 、C 和 D 是 A 的朋友。
   - 如果这 3 个人中有 2 个人也是朋友，那么这 2 个人和 A 构成彼此是朋友的3 人组。
   - 否则， B 、C 和 D 构成彼此为敌人的3 人组。
2. 假定 B 、C 和 D 是 A 的敌人。类似证明。

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

3.3 母函数

假定 $S=\{a,b,c\}$，现从集合 S 中任取 r 元素做排列和组合。

情形 1：不允许重复的排列数为 $\begin{cases} P(3,r) & r\leqslant 3 \\ 0 & r>3 \end{cases}$；

不允许重复的组合数为 $\begin{cases} C(3,r) & r\leqslant 3 \\ 0 & r>3 \end{cases}$。

情形 2：允许重复但重复无限制的排列数为 3^r；

允许重复但重复无限制的组合数为 $C(r+2,r)$。

情形 3：允许重复但元素 a,b,c 的重复数有限制，这样的排列与组合如何计数？

3.3 母函数

- 母函数可以用来解决允许重复并且重复有限制的组合问题。

例1 有红球2个，白球1个，黄球1个，问有多少种不同的组合方案？

解：用 r, w, y 代表红、白、黄三种颜色的球，$1, r, r^2$ 分别代表红球取0个，取1个，取2个的情形，令

$$\begin{aligned} A(x) &= \left(1 + rx + r^2x^2\right)(1 + wx)(1 + yx) \\ &= 1x^0 + (r + w + y)x^1 + \left(r^2 + rw + ry + wy\right)x^2 \\ &+ \left(r^2w + r^2y + rwy\right)x^3 + r^2wyx^4 \end{aligned}$$

表明：取 i 个球的组合方案数为 x^i 的系数。如：取2个球的组合方案有4种，分别为：r^2, rw, ry, wy。

3.3 母函数

- 母函数可以用来解决允许重复并且重复有限制的组合问题。

例1（续）有红球2个，白球1个，黄球1个，问有多少种不同的组合方案？

解：如果只需计算组合方案数，可以考虑如下多项式

$$A(x)=(1+x+x^2)(1+x)(1+x)$$
$$=1+3x+4x^2+3x^3+x^4$$

故所求的方案数为 $1+3+4+3+1=12$。

3.3 母函数

de Moivre

- 1730年左右，de Moivre用母函数来求解Fabonacci数列通项公式

Euler

- 1748年，Euler发展了母函数，并用于解决分配问题

Laplace

- 19世纪初，Laplace深入研究了母函数，并用于处理概率问题

- 目前母函数已在组合数学中有广泛应用，如求解组合数、排列数、递推关系通项公式等

3.3 母函数

定义3.12 序列 $a_n = a_0 a_1 a_2 \ldots$ 的母函数定义为

$$A(x) = a_0 + a_1 x + a_2 x^2 + \ldots$$

有限序列 $a_0 a_1 a_2 \ldots a_m$ 的母函数定义为无限序列 $a_0 a_1 \ldots a_m 0\,0 \ldots$ 的母函数。

例2 序列 $C(n,0), C(n,1), \ldots, C(n,n)$ 的母函数为：

$$C(n,0) + C(n,1)x + \ldots + C(n,n)x^n = (1+x)^n$$

例3 序列 $1,1,1,\ldots$ 的母函数为：

$$1 + x + x^2 + \ldots = \frac{1}{1-x}$$

3.3 母函数

例4 若有1克的砝码3枚，2克的砝码4枚，4克砝码2枚，问能称出13克有几种方案？

解：设 a_n 表示重量为n的方案数，则其母函数

$$\begin{aligned}A(x)&=(1+x+x^2+x^3)(1+x^2+x^4+x^6+x^8)(1+x^4+x^8)\\&=1+x+2x^2+2x^3+3x^4+3x^5+4x^6+4x^7\\&\quad+5x^8+5x^9+5x^{10}+5x^{11}+4x^{12}+4x^{13}\\&\quad+3x^{14}+3x^{15}+2x^{16}+2x^{17}+x^{18}+x^{19}.\end{aligned}$$

由于 x^{13} 的系数是4，故共有4种方案能称出13克。

3.3 母函数

例5 某单位有8位男同志，5位女同志，现要组织一个由偶数个男同志和数目不少于2个的女同志组成的小组，问有多少种不同的组合方案?

3.3 母函数

解：设 a_n 表示由n个同志组成的方案数，则其母函数为

$$\begin{aligned}A(x)&=\left(1+C(8,2)x^2+\ldots+C(8,8)x^8\right)\cdot\\&\quad\left(C(5,2)x^2+C(5,3)x^3+C(5,4)x^4+C(5,5)x^5\right)\\&=(1+28x^2+70x^4+28x^6+x^8)(10x^2+10x^3+5x^4+x^5)\\&=10x^2+10x^3+285x^4+281x^5+840x^6+728x^7+630x^8\\&\quad+350x^9+150x^{10}+38x^{11}+5x^{12}+x^{13}\end{aligned}$$

总的方案数为 $10+10+285+281+840+728+630+350+150+38+5+1=3328$