组合数学
第十章 组合设计拉丁方

主要内容

- 1. 正交拉丁方
- 2. 研究历史
- 3. 正交拉丁方的构造
- 4. 有限域与正交拉丁方

拉丁方

定义: 若A是由n个元素构成的n阶方阵,

其中每个元素在每行每列各出现一次,

则称A是**拉丁方**.

设$A=(a_{ij})$, 每个元素每行(列)只出现一次:

$a_{ij}=a_{ik} \Rightarrow j=k$ （$a_{ji}=a_{ki} \Rightarrow j=k$）

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$$

36名军官问题

(18世纪)36军官问题: 6个地区, 6种军衔各一名.

将这36名军官排成6×6方阵, 使得

1)每行每列都有任一地区的军官;

2)每行每列都有任一军衔的军官.

i :军衔, j :地区, 军官对应数偶(i, j), $i, j \in [0,5]$

问题等价于构造数偶(i,j)排成的6阶方阵, 使得

1) 数偶第一个数字构成拉丁方;

2) 数偶第二个数字构成拉丁方;

3) 每个数偶只出现一次.

正交拉丁方

定义:设$A=(a_{ij})_{n\times n}$,$B=(b_{ij})_{n\times n}$是两个n×n拉丁方.

令$C=((a_{ij}, b_{ij}))_{n\times n}$,若C的$n^2$对数偶互不相同,

则称A与B正交.

36军官问题等价于构造两个正交的6阶拉丁方.

例: 3阶正交拉丁方

$$A=\begin{bmatrix}0&1&2\\1&2&0\\2&0&1\end{bmatrix}\quad B=\begin{bmatrix}0&1&2\\2&0&1\\1&2&0\end{bmatrix}\quad C=\begin{bmatrix}(0,0)&(1,1)&(2,2)\\(1,2)&(2,0)&(0,1)\\(2,1)&(0,2)&(1,0)\end{bmatrix}$$

正交拉丁方的实际意义

正交的拉丁方的一个应用: 药物配合试验

三种治发烧药和三种治感冒药, 对三位病人试验, 要求三天内每人都服这几种药, 比较配合疗效.

这时就可用上面讨论过的3阶正交拉丁方.

$$C = \begin{bmatrix} (1,1) & (2,3) & (3,2) \\ (2,2) & (3,1) & (1,3) \\ (3,3) & (1,2) & (2,1) \end{bmatrix}$$

行:人, 列:天

(i,j): i,发烧药

j, 感冒药

举例 (N(5) = 4)

令N(n)为两两正交*n*阶拉丁方最大个数.

N(1)=2

N(2)=1

N(3)=2

N(4)=3

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

Euler的猜测

记N(n)为两两正交的n阶拉丁方的最大个数.

定理1: 若$n>1$,则$N(n)\leq n-1$.

定理2: 若$n=p^a$, p是素数,$a>0$, 则N(n)=n-1.

定理3: 若n是奇数, 则N(n)≥2.

定理4: 若N(m)≥2,N(n)≥2, 则N(mn)≥2.(自学)

推论: 若n≥2且n≠4k+2, k≥0, 则N(n)≥2.(?)

Euler(1707~1783)猜测:

对任意n=4k+2, k≥0, N(n)=1.

Euler猜测的解决

1900年 Tarry(法) 验证了N(6)=1.

1959年 Parker(美) 证明 N(10)≥2.

1959年 Bose(印), Parker, Shrikhande(印)

证明 N(4k+2)≥2, 任意k>1.

$\mathrm{N}(n) \le n\text{-}1$

定理1: $n>1$, $\mathrm{N}(n) \le n-1$. 即若$A_1,A_2,\ldots,A_k$是MOLS (两两正交拉丁方), 则必有 $k\le n-1$.

置换的定义与表示:

置换: 有限集(例如{1,2,…,n})上的一一对应.

表示: $p(1)=a_1$, $p(2)=a_2,\ldots$, $p(n)=a_\mathrm{n}$,

注: $a_1a_2\ldots a_n$是$1,2,\ldots,n$的一个排列

则以 $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ 来表示该置换

置换

设 p是$\{1,2,\ldots,n\}$上一置换,

$A=(a_{ij})_{n\times n}$是矩阵, $a_{ij}\in\{1,2,\ldots,n\}$

定义 $p(A)=(\,p(a_{ij})\,)_{n\times n}$,

例:

$$p=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\quad A=\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\\ 3 & 1 & 2\end{bmatrix}\quad p(A)=\begin{bmatrix}3 & 1 & 2\\ 1 & 2 & 3\\ 2 & 3 & 1\end{bmatrix}$$

p(A)性质讨论

1. 若A是拉丁方, p是置换, $p(A)$是拉丁方吗?

   $p(i)$在每行每列只出现一次.

2. 若A是拉丁方, 则A与$p(A)$是否正交?

   A与$p(A)$组成的数偶只有: (i, p(i)), i=1,…,n

3. 若A与B正交, 则$p(A)$与B是否正交?

   由于p是一一映射,所以

$$(p(i_1), j_1)=(p(i_2), j_2) \Leftrightarrow (i_1, j_1)=(i_2, j_2)$$

$$p(\mathrm{A})\text{与B不正交} \Leftrightarrow \text{A与B不正交}$$

N(n) ≤ n-1的证明

定理: 两两正交的n阶拉丁方不超过n-1个.

证明: 取k个n阶MOLS: $A_1, A_2, \ldots, A_k$

取置换 p_i,使得$p_i(A_i)$的第一行为0,1,…,n-1:

$$\begin{bmatrix} 0 & 1 & \cdots & n-1 \\ i_1 & \cdot & \cdots & \cdot \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} 0 & 1 & \cdots & n-1 \\ i_2 & \cdot & \cdots & \cdot \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 & \cdots & n-1 \\ i_k & \cdot & \cdots & \cdot \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}$$

则 $p_1(A_1),\ldots,p_k(A_k)$两两正交,且第二行第一个元素

满足: 1) 不等于0; 2) 互不相等.

所以 $k \le n-1$.

观察

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

p=5,k=1 p=5,k=2 p=5,k=3 p=5,k=4

每行分别左移1,2,3,4格

p阶方阵$A_1,A_2,\ldots,A_{p-1}$:

$A_k=(a_{ij}^{(k)})_{p\times p}$, $k=1,2,\ldots,p-1$.

$a_{ij}^{(k)}=k\cdot i+j \bmod p$, $i, j\in[0,p-1]$

定理: 设p为素数, 则N(p)=p-1.

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{bmatrix}$$

p=4, k=2

定理: 设p为素数, 则N(p)=p-1.

证明:$A_k=(a_{ij}^{(k)})_{p\times p}$, $k=1,2,\ldots,p-1.$

$a_{ij}^{(k)}=k\cdot i+j \bmod p$, $i,j= 0,1,\ldots,p-1$

先证A_k是拉丁方: $a_{ij}^{(k)} = a_{it}^{(k)} \Rightarrow j\equiv t \bmod p \Rightarrow j=t$

$a_{ij}^{(k)} = a_{sj}^{(k)} \Rightarrow k(i-s)\equiv 0 \bmod p \Rightarrow i=s$

再证A_g,A_h正交: 若$(a_{ij}^{(g)},a_{ij}^{(h)})=(a_{rs}^{(g)},a_{rs}^{(h)})$

则 $g(i-r)+(j-s)\equiv 0 \bmod p$, $h(i-r)+(j-s)\equiv 0 \bmod p$

得 $(g-h)(i-r)\equiv 0 \bmod p \Rightarrow i=r$

$\Rightarrow j=s$ 得证.

key: $a\cdot b=0 \bmod p \Rightarrow a=0$或$b=0 \bmod p$. (p=4?)

定理2: $n=p^a$, p素数,$a>0 \Rightarrow N(n)=n-1$

定义: 设集合F对可交换运算+和×封闭, 满足

(1) <F,+>是群(记其么元为0),

(2) 乘法分配律: a×(b+c)=a×b+a×c

(3) <F,×>是半群,

(4) 消去律: a×b=0 ⇒ a=0或b=0.

则称<F,+,×>是一个域. F有限:有限域(Galois域GF)

注: (3)+(4)等价于<F\{0},×>是群.

命题: 若n阶有限域存在, 则N(n)=n-1.

定理: p素数,a正, p^a阶GF存在. GF的阶是素数幂.

GF的构造方法

以$GF(n)$记n阶有限域.

对素数p, $GF(p)=<\{0,1,\ldots,p-1\}, +\bmod p, \times\bmod p>$

对$a>0$, 取a阶多项式$x^a+c_1x^{a-1}+\ldots+c_a$, 满足:

- 各次项系数取值于$GF(p)$
- 在$GF(p)$上不能分解

记其任一个根为γ, 令

$$F = \{b_0+b_1\gamma+\ldots+b_{a-1}\gamma^{a-1} : b_0,b_1,\ldots,b_{a-1}\in[0,p-1]\}$$

则$GF(p^a)=<F, +\bmod p, \times\bmod p>$.

举例:阶为2^2的有限域

$p=2, a=2$

$GF(p) = GF(2) = Z_2 = <\{0,1\}, + \bmod 2, \times \bmod 2>$,

取a阶多项式为x^2+x+1,

令γ为方程$x^2+x+1=0$的根,

$$F(p^a) = F(4) = \{ b_0+b_1\gamma \mid b_0,b_1\in\{0,1\} \}$$

$$=\{0,1, \gamma, 1+\gamma\}$$

所以$<\{0, 1, \gamma, 1+\gamma\}, + \bmod 2, \times \bmod 2>$是域.

举例:阶为2^2的有限域

GF(4)=<{0, 1, γ, 1+γ}, + mod 2, × mod 2>是域.

其中γ为方程$x^2+x+1=0$的根

加法表:

	0	1	γ	1+γ
0	0	1	γ	1+γ
1	1	0	1+γ	γ
γ	γ	1+γ	0	1
1+γ	1+γ	γ	1	0

乘法表:

	0	1	γ	1+γ
0	0	0	0	0
1	0	1	γ	1+γ
γ	0	γ	1+γ	1
1+γ	0	1+γ	1	γ

举例:阶为3^3的有限域

GF(3)=Z_3={0,1,2},令γ为$x^3+2x+1=0$的根,令

$$F=\{a + b\,\gamma + c\,\gamma^2 : a,b,c\in Z_3\}$$

<F, + mod 3, × mod 3>是27阶有限域.

例: $\gamma(1+ 2\gamma^2) = \gamma + 2\gamma^3 = \gamma + 2\gamma + 4 = 1.$

$$(2 + \gamma + 2\gamma^2)(1 + \gamma^2)=1.$$

利用有限域构造MOLS举例

回顾 $A_k=(a_{ij}^{(k)})_{n\times n}$, $a_{ij}^{(k)}=k\cdot i+j \bmod p$,

设有n阶有限域< $F=\{0, b_1, \dots, b_{n-1}\}$, +, ×>,

则$A_k=(a_{ij}^{(k)})_{n\times n}$, $k=1,\dots,n-1$,

$a_{ij}^{(k)}=b_k\times b_i+b_j$, 其中$b_0=0$, $i, j\in[0,n-1]$

$$A_1=\begin{bmatrix} 0 & 1 & \gamma & 1+\gamma \\ 1 & 0 & 1+\gamma & \gamma \\ \gamma & 1+\gamma & 0 & 1 \\ 1+\gamma & \gamma & 1 & 0 \end{bmatrix} A_2=\begin{bmatrix} 0 & 1 & \gamma & 1+\gamma \\ \gamma & 1+\gamma & 0 & 1 \\ 1+\gamma & \gamma & 1 & 0 \\ 1 & 0 & 1+\gamma & \gamma \end{bmatrix} A_3=\begin{bmatrix} 0 & 1 & \gamma & 1+\gamma \\ 1+\gamma & \gamma & 1 & 0 \\ 1 & 0 & 1+\gamma & \gamma \\ \gamma & 1+\gamma & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$