一些数学历程

2024 年 1 月 9 日

目录

1 拉丁方

1.1 定义：拉丁方

一个$n \times n$的拉丁方指的是一个$n \times n$的矩阵，其中的元素取自n元集X，且不会在任何行列中出现两次。

一个显著的例子是，矩阵A是拉丁方当且仅当其每一行每一列都是一个X上的置换。

例子 一个把$0, 1$作为元素的2×2的拉丁恰好有两个：

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{和} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

然后我们给出一些4×4的拉丁方

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad \text{和} \quad B = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix}$$

1.2 定义：哈达玛积

若$A = [a_{ij}]$和$B = [b_{ij}]$是$m \times n$矩阵，那么他们的哈达玛积记为$A \circ B$，它是$m \times n$矩阵且其中的第ij元素是有序对(a_{ij}, b_{ij})

在交换环中，我们一般用乘法来代替哈达玛积的记法。

1.3 正交

设两个拉丁方$A = [a_{ij}]$和$B = [b_{ij}]$，它们的元素分别取自集合$\mid X \mid = n = \mid Y \mid$，当我们说其正交时，指的是其所有元素，也就是有序对(a_{ij}, b_{ij})是互异的。

例如对2×2的且元素由$0,1$组成的哈马达积有

$$A\circ B=\begin{bmatrix}01 & 10\\ 10 & 01\end{bmatrix}.$$

就不是正交的，因为它只有两个不同的有序对，定义要求4个。

现在我们给出一个正交的例子：

$$A\circ B=\begin{bmatrix}00 & 11 & 22 & 33\\ 12 & 03 & 30 & 21\\ 23 & 32 & 01 & 10\\ 31 & 20 & 13 & 02\end{bmatrix}$$

1.4 引理

令$A=[a_{ij}]$是拉丁方，其中的元素位于n元集X。若$x\mapsto x'$是X的置换，则$A'=[(a_{ij})]'$是拉丁方，因此，若$x=a_{ij}$是A中的第ij个元素，则x'是A'中的第ij个元素。更多的，若A和$B=[(b_{ij})]$是正交的拉丁方，则A'和B也是正交的。

证明： A的第i行$(a_{i1},a_{i2},\cdots,a_{in})$是$X$中的一个置换，相对的$A'$的第$i$行也是一个置换。类似的我们有$A$，$A'$的列也是$X$上的一个置换，因此$A'$是拉丁方。

若A'和B不是正交的，则存在$A'\circ B$中的两个元素是相等的，我们设为$(a'_{ij},b_{ij})=(a'_{k\ell},b_{k\ell})$，那么就有$a'_{ii}=a'_{k\ell}$和$b_{ij}=b_{k\ell}$。得到$a_{ij}=a_{kl}$与$A$是拉丁方矛盾。因此$A'$和$B$正交。

1.5 引理

1. 若k是有限域且$a\in k^{\times}=k-\{0\}$，则$|\ k\ |\times|\ k\ |$矩阵

   $$L_a=[l_{xy}]=[ax+y]$$

   其中$x,y\in k$，且矩阵是拉丁方。

2. 若$a,b\in k^{\times}$和$b\neq a$，则L_a和L_b是正交的拉丁方。

证明： 考虑L_a的第x行是由元素$ax+y$组成的，其中x是固定的，和其元素都是不同的。若有$ax+y=ax+y'$，则有$y=y'$是成立的，类似的，我们对列也进行一样的讨论，则有$ax=ax'$。由于$a\neq 0$，则$x=x'$。

证明2： 我们设存在两对一样的元素：

$$(ax+y, bx+y) = (ax'+y', bx'+y')$$

因此$ax+y=ax'+y'$和$bx+y=bx'+y'$我们可以得到等式

$$a(x-x') = y'-y = b(x-x')$$

由于$a\neq b$，则由消去律得到$x-x'=0$进一步的得到$y'-y=0$使得$x=x'$和$y=y'$。因此L_a和L_b是正交的拉丁方

1.6 推论

对每个素数的阶$p^e>2$，这里存在一对正交的$p^e\times p^e$的拉丁方。

证明： 利用伽罗瓦定理，我们就可以找到这么一个域k有$|k|=p^e$，对于另一对正交的拉丁方，我们需要有$|k^\times|\geq 2$，那么，$p^e-1\geq 2$有$p^e\geq 2$，最后利用引理1.15就可以了。

我们展示一下，如何用一个小的拉丁方创造一个大的。令K和L是集合，其中$|K|=k$和$|L|=l$。若$B=[b_{ij}]$是一个$l\times l$的且元素位于L中的矩阵，则aB是一个$l\times l$的矩阵，其中第ij个元素是ab_{ij}。若$A=[a_{st}]$是$k\times k$矩阵，且其中元素位于K。则我们把A和B的$A\otimes B$称为克罗内克积，它是$kl\times kl$矩阵。

$$\begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1k}B \\ a_{21}B & a_{22}B & \dots & a_{2k}B \\ \dots & \dots & \dots & \dots \\ a_{k1}B & a_{k2}B & \dots & a_{kk}B \end{bmatrix}.$$

1.7 定理：欧拉

若$n\not\equiv 2 \mod 4$，则这里存在一对$n\times n$的正交拉丁方。

证明： 在这里我们仅仅给出证明的主要步骤。首先，若A, B是拉丁方，则$A \otimes B$也是拉丁方。其次我们证明A, A'是正交的拉丁方，且若B, B'是正交的拉丁方，则$A \otimes B$和$A' \otimes B'$是正交的$kl \times kl$的拉丁方。

一个正整数n是奇数当且仅当$n \equiv 1 \mod 4$或者$n \equiv 3 \mod 4$，在其他的例子中，我们设$n = p_1^{e_1} \cdots p_t^{e_t}$，其中$p_i$是奇素数。而正数$n \equiv 0 \mod 4$当且仅当$n = 2^e m$，其中$m$是奇数且$e \geq 2$。因此$n \not\equiv 2 \mod 4$当且仅当$n = 2^e p_1^{e_1} \cdots p_t^{e_t}$其中$e \neq 1$且$e$是奇素数。利用推论1.6，则对每个$i$都有一对正交拉丁方$p_i^{e_i} \times p_i^{e_i}$，接着我们对其进行处理，对每个$i$都做克罗内克积，那么我们就得到了一个$n \times n$的拉丁方。

注意： 除了$2, 6$其他的数字都存在正交的拉丁方对。

2 魔法

我们现在来使用正交的拉丁方构造一些方阵。

2.1 定义：幻方

一个$n \times n$的幻方指的是$n \times n$矩阵$A = [a_{ij}]$我们考虑所有数字$0, 1, \cdots, n^2 - 1$,其中的行的和还有列的和是一样的，因此，这里有一个数σ，它被称为幻数并使得

$$\sum_{j=1}^{n} a_{ij} = \sigma \text{ for all } i \quad \text{and} \quad \sum_{i=1}^{n} a_{ij} = \sigma \text{ for all } j.$$

成立

2.2 命题

若A是$n \times n$幻方，则它的幻数是

$$\sigma = \frac{1}{2} n(n^2 - 1)$$

证明： 我们记p_i是所有A的第i行的和，则$p_i = \sigma$对所有i成立，有

$$\sum_{i=1}^{n} p_i = n\sigma$$

则有

$$n\sigma = 1 + 2 + \cdots + (n^2 - 1) = \frac{1}{2}(n^2 - 1)n^2$$

因此，$\sigma = \frac{1}{2}n(n^2 - 1)$

2.3 定义：魔方

一个魔方指的是一个幻方，其中的反对角线和对角线的和都等于幻数。

2.4 命题：

若$A = [a_{ij}]$和$B = [b_{ij}]$是正交的拉丁方且元素从$0, 1, \cdots, n-1$中选取的，则矩阵$M = [a_{ij}n + b_{ij}]$是$n \times n$的幻方。

证明： 由于A, B是正交的拉丁方，那么它们的哈达玛积$A \circ B$互异。我们知道每个数的n进制数都是唯一的，这很好的保证了$1, 2, \cdots, n-1$都出现在M中。现在，由于A是拉丁方，说明每行都是$0, 1, \cdots, n-1$的一些排列并且对每个行和列的和有$s = \sum_{i=0}^{n-1} i = \frac{1}{2}(n-1)n$，类似的讨论我们可以得到$B$的行列和也是$s$。因此$M$的每个行和列的和等于$sn + s$，所以$M$是一个幻方。

2.5 定义：对角拉丁方

一个$n \times n$拉丁方$A = [a_{ij}]$，其中的元素在集合X内且$| X |= n$是对角拉丁方，这是在说其对角线和反对角线都是X的一个置换。

2.6 引理

若$n \in N$是非3倍数的奇数，则这里存在一个正交的$n \times n$的对角拉丁方对

证明： 给定n，我们要使用的方法要求正整数$a > b$且对每个$a, b, a-b, a+b$都是与n互素的。若我们选择$a = 2$和$b = 1$，则$(2, n) = 1$将得到n是奇数的。而$b = 1 = a - b$不会限制n是什么数，不过若$a + b = 3$则有n必定不为3的倍数。

那么首先，构造一个$n\times n$的拉丁方，方便我们标记行列，因此$0\le i,j\le n-1$。定义A是$n\times n$矩阵，其中第ij个元素位于同余类$[ib+ja] \mod n$，即：

$$A=\begin{bmatrix} 0 & a & 2a & \cdots & (n-1)a \\ b & b+a & b+2a & \cdots & b+(n-1)a \\ 2b & 2b+a & 2b+2a & \cdots & 2b+(n-1)a \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-1)b & (n-1)b+a & (n-1)b+2a & \cdots & (n-1)b+(n-1)a \end{bmatrix}.$$

现在我们就来证明A是一个对角拉丁方。注意每行都是一个置换。对i固定，若$ib+ja=ib+ja'$，我们可以得到$(j-j')a\equiv 0 \mod n$，但$(a,n)=1$，由消去律得到$[j]=[j']$。类似的证明我们也可以得到$[i]=[i']$，对于主对角线，若$ib+ia=i'b+i'a$，则$i(b+a)=i'(b+a)$由$(b+a,n)=1$得到$[i]=[i']$，最后，对反对角线，若$ib+(n-i)a=i'b+(n-i')a$，则有$i(b-a)=i'(b-a)$。并且因为$(b-a,n)=1=(a-b,n)$有$[i]=[i']$。因此A是拉丁方并且是对角拉丁方。

其次，我们来证明A^T也是一个对角拉丁方。我们证明A,A^T是正交的。记A^T的ij元素为$jb+ia$。那么$A\circ A^T$的哈马达积的ij元素是$(ib+ja,jb+ia)$，为了证明，我们不妨设$(ib+ja,jb+ia)=(i'b+j'a,j'b+i'a)$，那么就有$ib+ja=i'b+j'a\ \ jb+ia=j'b+i'a$。现在，注意我们的元素都是在$I_n$中的。得到$[(i-i')a]=[j'-j]b$和$[(j'-j)a]=[(i-i')b]$对第一个等式乘$[b]$，第二个乘$[a]$。有$[(j'-j)a^2]=[(i-i')ab]=[(j'-j)b^2]$。现在，令$a=2,b=1$，就有$[4(j'-j)]=[j'-j]$得到$3(j'-j)\equiv 0 \mod n$，但$(3,n)=1$，有$j'-j\equiv 0 \mod n$得到$[j]=[j']$，类似的讨论可以得到$[i]=[i']$，因此$A^T$也是对角拉丁方

2.7 命题：

若$n\in N$是奇数且不为3的倍数，则存在一个$n\times n$的魔方。

证明： 令$A=[a_{ij}]$和$B=[b_{ij}]$是正交的对角拉丁方。利用引理2.6还有命题2.4，则可以得到一个矩阵$M=[a_{ij}n+b_{ij}]$是幻方且$\sigma=s(n+1)$，其中$s=\sum_{i=0}^{n-1} i$而且其对角线是$\{0,1,\cdots,n-1\}$的一个置换。所以，对角线的

和是$s(n+1)$，用同样的方法可以得到反对角线的和也是一样的。因此是一个魔方。

2.8 定义：正交集

$n\times n$拉丁方的集合$A_1,A_2,\cdots,A_t$叫正交集，指的是其中每对拉丁方都是俩俩正交的。

2.9 引理

若$A_1,A_2,\cdots,A_t$是$n\times n$的拉丁方的正交集，则$t\le n-1$

证明： 我们有一个不失一般性的证明，假设A_v的每个元素位于$X=\{0,1,\cdots,n-1\}$中，置换A_1的元素使得它第一行是$0,1,\cdots,n-1$。由引理1.4有A_1'也是拉丁方，且与每个$A_2,\cdots,A_t$正交。我们假设矩阵的第一行的排列都是按照自然顺序来的。

若$v\neq\lambda$，则哈达玛积的第一行如下：

$$(0,0),(1,1),\ldots,(n-1,n-1)$$

我们断言A_v和A_λ是没有相同的第$2,1$元素的。否则就存在k有$a_{21}^v=k=a_{21}^\lambda$使得

$$(a_{21}^v,a_{21}^\lambda)=(k,k)$$

得到矛盾。因为(k,k)是第一行出现的元素。所以不同的A_v的$(2,1)$位置仕有不同的元素，但任意A_v中$(2,1)$元素只有$n-1$个选择，这是因为0已经在位置$(1,1)$上出现，因此之多存在$n-1$个不同的A_v

为此我们得到一个新的定义

2.10 定义：完全正交集

一个$n\times n$的拉丁方的完全正交集得是$n-1$个拉丁方组成的正交集。

2.11 代理：

若$q=p^e$，则这里存在$q-1$个由$q\times q$拉丁方构成的完全正交集。

证明： 若k是含有q个元素的有限域，则存在$k^{\times}$含有$q-1$个元素。利用引理1.5，则这样的拉丁方有$q-1$个，且每对都是正交的。

3 射影平面

有一个反直觉的事情，当我们研究透视图的时候，水平线似乎在地平线上相交。这暗示我们需要再普通平面上加一条“无穷远处的直线” 每条直线都平行于一条过原点O的直线l，对每条这样的直线，我们可以定义一个新的点ω_t，并构造一个新的集合

$$P^2(R) = R^2 \cup H$$

其中$H = \{\omega_t : l\text{是过O的一条直线}\}$，然后我们在$P^2(R)$中定义新的直线：$H$是一条直线（无穷远处的直线，叫地平线），我们对$R^2$中的每条直线$L$，定义$L^* = L \cup \{\omega_t\}$，其中$l$是过原点且和$L$平行的直线。

我们来证明$P^2(R)$的每对直线相交在一点。若$L^* = L \cup \{\omega_t\}$，则$L^* \cap H = \{\omega_t\}$。现在我们考虑两条直线$L^*$和$M^*$，其中$L^*, M^*$是两条直线$L, M$并上$\{\omega_t\}$得到的。若$L, M$平行，那么交集只有$\omega_t$，反之则相交在某个点$Q$上。

每两个不同的点Q，$R \in P^2(R)$确定的直线也是成立的，若$Q = \omega_t$而$R = \omega_m$，则Q, R确定H，若$Q = \omega_t$，$R \in R^2$，则Q, R确定与l平行的普通直线L^*，最后，若$Q, R \in R^2$，则Q, R确定平面上的一条普通直线L，因而确定新直线L^*

我们现在使用有限平面$k \times k$代替平面$R \times R$，其中k是q个元素的有限域，那么我们可以把这个平面看成是加法阿贝尔群的直和。定义过原点$O(0,0)$的直线l为下属形式的子集

$$l = \{(ax, ay) : a \in k, (x, y) \neq O\}$$

那么我们可以在此基础上定义一个直线陪集：

$$(u, v) + l = \{u + ax, v + ay : a \in k\}$$

由于k是有限的，我们可以做些计算，平面上存在q^2个点，且直线上存在q个点，每条直线都是过原点的直线的一个陪集，他们和l有相同的方向。且含的点与原来的线相同。存在q^2-1个点$V \neq O$，且每一点确定过原点的一条直线$l = OV$。由于l上有q个点，所以l除去O剩下$q-1$个，且每个点都能确

定l，那么就有

$$(q^2-1)/(q-1)=q+1$$

个方向，我们可以把这$q+1$个新的点ω_t加到$k\times k$上。每个点表示一个方向。即每个点表示过原点的一条直线l，并定义H，无穷远处的直线为

$$H=\{\omega_t: l\text{是过原点的一条直线}\}$$

并定义k上的射影平面

$$P^2(k)=(k\times k)\cup H$$

3.0.1 例子

想象一下，当你站在马路中间往前面看，或者是在轨道往前面看，我们会发现轨道的前段一直延伸到正前方，并且轨道之间是互相平行的，但我们的眼睛告诉了我们平行线在无穷远处相交。