DM Part 5

五. 組合設計簡介

在歷史上組合數學對於研究如何設計實驗使得成效更好，有很大的貢獻 。研究實驗設計中所隱函的數學 (Combinatorics in Experimental Designs) 一般稱之爲組合設計；而研究組合設計就不得不先介紹最具有影響力的拉丁方陣。

1. 拉丁方陣 (Latin Square)

例1. 假如我們要設計一個實驗來研究 5 種藥物，$\alpha, \beta, \gamma, \delta, \epsilon$，對人體的影響，(每天可以吃一種)，我們應該如何安排才可以避免所得到的結論過於偏差。顯然，我們找一個人來做實驗，會因爲他個人體質的關係，而造成有偏差的結論；如果找太多人，又會造成太多的重複；因此，有一種設計方式是找到 5 個人來實驗，而且在 5 天內完成。表 1(a) 的安排，看起來十分容易，而且似乎達到實驗效果。然而，有些藥可能會對隔日，或以後的身體狀況有很大的影響力，而容易造成在服用該種要之後，其它的藥效果不彰，譬如催吐藥。於是服用的先後次序也要考量，如此一來，偏差自然減少。因此，表 1(b) 的安排顯然就比較好，一方面每天都可以看到 5 種藥對人體的可能影響，同時每個人每天所服用的藥也都不相同。這樣的設計又稱爲是拉丁方陣設計或簡稱爲拉丁方陣 (Latin Square)。

人	M	Tu	W	Th	F
甲	α	β	γ	δ	ϵ
乙	α	β	γ	δ	ϵ
丙	α	β	γ	δ	ϵ
丁	α	β	γ	δ	ϵ
戊	α	β	γ	δ	ϵ

表 1(a)

人	M	Tu	W	Th	F
甲	ϵ	δ	γ	β	α
乙	δ	γ	β	α	ϵ
丙	γ	β	α	ϵ	δ
丁	β	α	ϵ	δ	γ
戊	α	ϵ	δ	γ	β

表 1(b)

定義 1.1. 用 1, 2, $\cdots$, n 爲元素所安排的 n 階方形陣列 $A=[a_{ij}]_{n\times n}$, 如果在每一行及每一列中, 每個元素都恰好出現一次, 則 A 稱爲是一個 n 階拉丁方陣。如果對所有的 $1\leq i,\ j\leq n$, $a_{ij}=a_{ji}$, 則此拉丁方陣爲對稱的拉丁方陣; 若是對於每一個 $1\leq i\leq n$, $a_{ii}=i$, 則爲等冪 (Idempotent) 拉丁方陣。

在表 1(b) 中, 如果用 1,2,3,4,5 分別代表 $\epsilon,\gamma,\alpha,\delta,\beta$, 則所得到的陣列 (Array) 爲一對稱且等冪的 5 階拉丁方陣。爲了便於解釋, 以後拉丁方陣中的元素, 我們都用 $\{1,2,\cdots,n\}$ 中的元素來表示。(若是經由代數方法製造, 則用 $Z_n=\{0,1,\cdots,n-1\}$。)

(性質 1) 各階的拉丁方陣都存在。
(性質 2) 各階的對稱拉丁方陣都存在。
(性質 3) 各階的等冪拉丁方陣都存在。
(性質 4) 只有奇數階的等冪對稱拉丁方陣存在。

我們可以利用 n 階拉丁方陣 $A=[a_{ij}]$ 來定義一個運算 $*$, $i*j=a_{ij}$ 則 $*$ 爲一二元運算, 而且滿足: 對於任何 $a,b\in\{1,2,\cdots,n\}$, $a*x=b$ 和 $y*a=b$ 在 $\{1,2,\cdots,n\}$ 中都有唯一解。假如 $*$ 爲一二元運算, 同時方程式 $a*x=b$ 及 $y*a=b$ 在 S 中都有唯一解, 則我們把這一個代數結構 $(S,*)$ 稱爲是擬似群 (Quasigroup)。

(性質 5) 具有結合律的擬似群爲一群 (Group)。
(性質 6) 一個擬似群不一定可結合。

例2.

$*$	1	2	3	4
1	1	2	3	4
2	3	1	4	2
3	4	3	2	1
4	2	4	1	3

$$2*(1*2)=2*2=1$$
$$(2*1)*2=3*2=3$$

接下來我們看一個問題。

問題1. 假設有 16 位軍官要參加國慶閱兵的分列式，他們代表著 4 個兵種的 4 個官階，也就是說由步兵、砲兵、通訊兵、工兵，各派出一位少尉、中尉、上尉、少校參加。分列式將以四列、四行的方形排列前進。如果我們要求每一列（每一行）都要有四個兵種的代表而且是四個不同的官階，問要如何安排？

在回答這個問題之前，我們先來看一個定義。

定義 1.2. 我們稱 $L=[l_{ij}]$ 和 $M=[m_{ij}]$ 爲兩個互相垂直的拉丁方陣，如果下列的兩個條件滿足：

(i) L 和 M 爲同階 (n 階) 的拉丁方陣；

(ii) $\{(l_{ij},m_{ij})|\,1\le i,\ j\le n\}=I_n\times I_n$，$I_n=\{1,2,\cdots,n\}$。

例3. 下面的三個拉丁方陣，彼此互相垂直。

1	4	3	2
4	1	2	3
3	2	1	4
2	3	4	1

4	1	2	3
3	2	1	4
1	4	3	2
2	3	4	1

3	2	1	4
1	4	3	2
4	1	2	3
2	3	4	1

由（互相）垂直拉丁方陣的定義，我們可以發現問題 1 是在問：是否存在兩個互相垂直的 4 階拉丁方陣，答案顯然是肯定的。不過同樣的問題對於 6 階拉丁方陣就不同了。在 1900 年左右 Terry 已經用苦力式的方法

發現；根本不存在有這樣的兩個 6 階拉丁方陣，理論上的證明則等了 80 多年才完成。對於垂直拉丁方陣的研究，一直是組合設計的重要課題，我們在第 3 節再仔細討論。

以直觀的方式來看拉丁方陣，我們可以把一個 n 階拉丁方陣 $L=[l_{ij}]$ 的 n 列看成是 n 個排列，其形式如下：第 i 列 $\begin{pmatrix} 1 & 2 & 3 & \cdots & j & \cdots & n \\ a_{i1} & a_{i2} & a_{i3} & \cdots & a_{ij} & \cdots & a_{in} \end{pmatrix}$，$i=\ 1,2,\cdots,n$。因此，一個拉丁方陣可以由第一列先選好之後再第二列，第三列，$\cdots$，只要維持每一個位置，譬如第 j 個，出現的元素都不一樣即可。

例4. 不同的 4 階拉丁方陣有 576 個。

答. 第一列的選擇有 24 種，第二列的選擇有 $D_4=9$ 種。如何找出全部的 4 階拉丁方陣，除了利用電腦外，也可以用分類的方式求出來。

我們比較希望知道的是：一列一列往下找，一定可以找到 n 個來形成一個拉丁方陣嗎？會不會到了哪個位置，譬如 $n-k$ 列之後，就無法繼續找了呢？在回答這個問題之前，我們先介紹一個定義。（註）在圖的應用中，我們已經提及它，在此作完整說明。

定義 1.3. 假設 $\{S_1,\ S_2,\ \cdots,\ S_n\}$ 爲 n 個正整數集的子集合族；如果 $x_i\neq x_j,\ 1\leq i\neq j\leq n$，且 $x_i\in S_i$，$i=\ 1,2,\cdots,n$，則我們稱 $(x_1,\ x_2,\ \cdots,\ x_n)$ 爲 $\{S_1,\ S_2,\ \cdots,\ S_n\}$ 的一個相異代表系 (System of Distinct Representatives, SDR)。

例5. $S_1=\{1,\ 2,\ 3\}$，$S_2=\{2,\ 3\}$，$S_3=\{1,\ 4,\ 5\}$，$(3,\ 2,\ 1)$ 爲 $\{S_1,\ S_2,\ S_3\}$ 的一個 SDR。

例6. $S_1=\{2,\ 3\}$，$S_2=\{2\}$，$S_3=\{2,\ 3\}$，$S_4=\{1,\ 2,\ 3,\ 4\}$；則不存在有任何的 SDR。

顯然，若是 $S_1,\ S_2,\ \cdots,\ S_n$ 有一相異代表系，則任取 k 個 $S'_{ij}s$，$\left|\bigcup_{j=1}^{k} S_{ij}\right|\geq k$。此必要條件實際上也是 SDR 存在的充分條件，當然對於集合個數及集合的基數需要略做規範。下面的定理是 P. Hall 所發現，也簡稱爲 P. Hall 定理。（註）組合數學史上有兩位是以 Hall 爲姓的數學家，一位是 Marshall, 另一位爲 Philip，本定理是在 1935，Philip 所證明的結果，我們也會有機會提到 M. Hall。

定理 1.4. (P. Hall, 1935)

集合族 $F = \{S_1, S_2, \cdots, S_n\}$ 有 SDR 的充要條件爲任意 k 個 F 中的元素之聯集至少含有 k 個元素 , $k = 1, 2, \cdots, n$ 。

證明. ($\Rightarrow$) 很容易 。

($\Leftarrow$) 用歸納法 (討論集合的個數) 。$n = 1$ 時顯然成立 , 假設 $n = 1, 2, \cdots, m$ 時成立 。令 $\{S_1, S_2, \cdots, S_{m+1}\}$ 爲一集合族 , 而且在此集合族中的任意 k 個集合的聯集至少含有 k 個元素 , $k = 1, 2, \cdots, m+1$ 。對於任意選定的 k , 假如任意 k 個集合的聯集都含有至少 $k+1$ 個元素 , 令 $x_{m+1} \in S_{m+1}$。則$\{S_1 \setminus \{x_{m+1}\}, S_2 \setminus \{x_{m+1}\}, \cdots, S_{m+1} \setminus \{x_{m+1}\}\}$ 有 SDR $(x_1, x_2, \cdots, x_m)$ (由歸納假設) , 因此有一 SDR , $(x_1, x_2, \cdots, x_m, x_{m+1})$ 。在另一方面 , 如果存在有一 k , 及 k 個集合 , 它們的聯集恰含 k 個集合 , 不失一般性 , 令 $\left|\bigcup_{j=1}^{k} S_i\right| = k$ 且 $S = \bigcup_{j=1}^{k} S_i$ 。由假設 $S_{k+1} \setminus S, \cdots, S_{m+1} \setminus S$ 均不爲 ϕ , 且 $\{S_{k+1} \setminus S, S_{k+2} \setminus S, \cdots, S_{m+1} \setminus S\}$ 有一 SDR $(x_{k+1}, x_{k+2}, \cdots, x_{m+1})$ (?), 而由歸納假設 $\{S_1, S_2, \cdots, S_k\}$ 也有一 SDR $(x_1, x_2, \cdots, x_k)$; 合併之後 $\{S_1, S_2, \cdots, S_{m+1}\}$ 有一 SDR , 所以得證 。 ■

在定理 1.4 中的條件 "任意 k 個集合的聯集至少含有 k 個元素" 又簡稱爲 Hall 的條件 (Hall's condition) 。於是滿足 Hall 的條件之集合族就存在有一個相異代表系 (SDR) , 這樣的特性在應用上有很多 , 我們可以用它來證明 , 以排列堆積的方式一定可以完成一個拉丁方陣 。

定義 1.5. 在一個 $r \times s$ 陣列中如果每個元素皆來自 $S = \{1, 2, \cdots, n\}$, 而且每一個元素在每一行每一列中最多只出現一次 , 則此長方形陣列又稱爲是一個基於 S 的 $r \times s$ 拉丁長方形 (Latin rectangle) 。

定理 1.6. (M. Hall, 1945) 任一個基於 $S = \{1, 2, \cdots, n\}$ 的 $r \times n$ 拉丁長方形都可以把它繼續伸展成一個 n 階的拉丁方陣 。

證明. 令 $r \times n$ 拉丁長方形爲$M = [m_{ij}]_{r \times n}$, $S_j = S \setminus \{m_{1j}, m_{2j}, \cdots, m_{ij}\}$, $j = 1, 2, \cdots, n$ 利用定理 1.4 $\{S_1, S_2, \cdots S_n\}$ 有一個 SDR (?) , 所以第 $r+1$ 列即可填好 ; 繼續同樣的方法可證明本定理 。 ■

如果我們希望打一個基於 $S = \{1, 2, \cdots, n\}$ 的 $r \times s$ 拉丁長方形 A 向右且向下伸展成爲一個 n 階的拉丁方陣 (圖 1.1) , 結果就要比定理 1.6 複雜許多 。例 7 中的 A 就無法伸展成 7 階的拉丁方陣 。

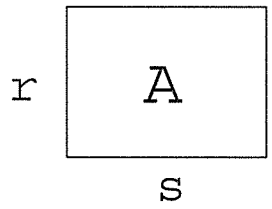

圖 1.1

例7.

$$A = \begin{array}{|cccc|}\hline 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \\ \hline \end{array}$$

顯然地那是因爲放在 A 中的元素沒有預先規定條件所造成的，下面的定理可以說明這件事。

定理 1.7. (H.J. Ryser, 1951)

令 R 爲基於 $S = \{1, 2, \cdots, n\}$ 的 $r \times s$ 拉丁長方形，$R(i)$ 代表 i 在 R 中出現的次數；則 R 可以伸展成一個 n 階拉丁方陣的充要條件爲對於所有的 $i = 1, 2, \cdots, n$；$R(i) \geq r + s - n$。

證明. 充分條件的證明在此省略。

(必要條件) 如圖 1.2 所示，任一個元素 i 在 $C \cup D$ 中必定出現 $n-r$ 次，而在 B 中至多出現 $n-s$ 次，所以在 R 中，i 至少出現 $n-[(n-r)+(n-s)] = r+s-n$ 次，所以 $R(i) \geq r + s - n$。 ■

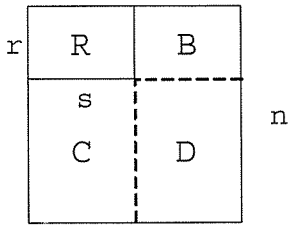

圖 1.2

由定理 1.7, 我們更容易看出例 7 的 A 爲何不能伸展成 7 階拉丁方陣。($R(5) = 0 < 4 + 4 - 7$。) 然而 , 例 7 的 A 卻可以伸展成 8 階 , 9 階 , $\cdots$, 的拉丁方陣 。

定義 1.8. 如果我們可以將 M 伸展而得到 L , 則我們稱一個拉丁方陣 M 可以嵌入於一個拉丁方陣 L 。

例8. 例 7 中的 A 可以嵌入於

A	A+4
A+4	A

, $A + 4 = [a_{ij} + 4]$, $A = [a_{ij}]$ 。

推論 1.9. 任一個 m 階拉丁方陣皆可嵌入於一個 $n(\geq 2m)$ 階拉丁方陣中 。

證明. 由定理 1.7 可得證 。

以代數的角度來看推論 1.9 , 嵌入的拉丁方陣實際上是一個子擬似群。所以我們發現一個現象 , 即子擬似群與擬似群的關係和子群與群的關係不盡相同 。

推論 1.10. 若是 $(Q_1, *)$ 爲 $(Q, *)$ 的子擬似群 , 則 $2|Q_1| \leq |Q|$ 。

證明. 由定理 1.7 可得證 。

(**註**) $|Q_1|$ 不一定是 $|Q|$ 的因數 , 這與 Lagrange 定理 (有限群與子群的關係) 不同 。

2. 區組設計 (Block Design)

在例 1 中，被實驗的對象 $\alpha, \beta, \gamma, \delta, \epsilon$ 所成的集合又稱爲處理元集 (Treatments)，而它的任一個子集合皆稱爲是一個區組，而把一個處理元集中的元素用來安排成"元素個數一樣" 的許多個區組 (可能只有一個)，稱爲是一個區組設計 (Block Design)。當每個區組實際上是整個處理元集時，此設計又稱爲是一個完全區組設計 (Complete Block Design)，若是區組的元素少於處理元集個數，則此設計爲不完全區組設計 (Incomplete Block Design)。我們可以把拉丁方陣看成是一個完全區組設計，以行或以列爲區組皆可。爲了方便表示，我們通常以 $(V, \mathfrak{B})$ 代表一個區組設計，V 爲處理元集，而 $\mathfrak{B}$ 爲區組族 (collection of blocks)。下面的例子就是一個不完全區組設計。

例9. $V = \{1,2,3,4,5,6,7\}$，$\beta = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}$。

(**註**) 在有限幾何的研究中，V 爲點集合，$\mathfrak{B}$ 爲線集合。

如果我們仔細觀察例 9，還可以發現下列的現象：

(1) V 中的任兩個元素，剛好共同出現在一個集合。(以幾何觀點而言，即爲任兩點決定一線。)

(2) $\mathfrak{B}$ 中的任兩個區組，恰好有一共同的元素。(兩線交於一點。)

顯然，並非所有的區組設計都會具有上述的兩種性質；滿足 (i) 及 (ii) 的不完全區組設計的確是非常特別，它是一種對稱設計 (Symmetric Design)。滿足 (i) 的現象是研究區組設計的學者最有興趣的一種設計。

定義 2.1. 在一個不完全區組設計中，如果任意兩點所共同出現的區組數爲一固定數 "λ"，則此設計稱爲是平衡不完全區組設計 (Balanced Incomplete Block Design)，簡稱 BIBD。

例 9 即爲一 BIBD，其中 $\lambda = 1$。如果我們假設在一個 BIBD 中，$|V| = v$, $|\mathfrak{B}| = b$，對於 $\mathfrak{B}$ 中的任一個區組皆有 $K(> 0)$ 個元素，而且 V 中的每個元素都出現在 $r(> 0)$ 個區組中，同時任意兩點所共同出現的區組有 $\lambda(> 0)$ 個，則此 BIBD 又稱爲是 (v, b, r, k, λ)–設計，而且滿足下列兩個條件。

(i) $\lambda(v-1)/(k-1)$ 爲正整數 ;

(ii) $\lambda(v-1)v/(k-1)k$ 爲正整數 。

証明 (i) , (ii) 並不難 , 實際上 $r=\lambda(v-1)/(k-1)$, $b=\lambda v(v-1)/k(k-1)$。除上述兩個性質 , 我們也可以證明下列定理 。

定理 2.2. 在一個 (v,b,r,k,λ)–設計中 , $bk=vr$ 且 $\frac{\lambda(v-1)}{k-1}$ 及 $\frac{\lambda v(v-1)}{k(k-1)}$ 皆爲正整數 。

證明. 由兩方向計數 , (Two-way Counting) 即可證明 。$bk=vr$ (把全部的區組排出來 , 再計算元素出現的總數 。) 另兩部分當成作業 。 ■

當 $k=3$ 時 , 上述設計又稱爲是三元素系統 (Triple System) 。和三元素系統有關的著名問題 , 是在 1847 年由柯克曼所提出的安排 15 個女學童排路隊上學的問題 。

問題 2.(Kirkman's schoolgirl problem)

有一個老師 , 他班上有 15 位女學生 , 他希望把這 15 位女學生排成三人一列的路隊上學 ; 在 7 天中 , 每天每位女學生都和同列的兩位同學相識; 問如何安排才能使她們在七天後 , 每位女學生都能認識全部其他的 14 位同學 , 亦即每天和不同的兩位同學一列 。

答. 這比一個三元素系統的要求更多 ; 不過 , 至少要是一個三元素系統 。(你能找到答案嗎 ?)

如果把問題 2 改成九個學生 , 則它的答案可分成 4 組 。下面就是其中的一種安排 。

例10.

123	159	168	147
456	267	249	258
789	348	357	369

現在再以幾何的觀點來看上面的結構 , 則平行線存在 (交集爲空集合的兩線) 。同時過直線外一點必定存在唯一的一線包含此點且與給定的直線平行 , 這也就是平行公設啊 ! 我們將分別以投影平面 (Projective Plane), 仿射平面 (Affine Plane) 來稱呼例 9 , 例 10 兩種具有特殊性質的 BIBD 。

以下我們分成三部分來分別介紹互相垂直的拉丁方陣 , 投影平面及仿射平面 。

3. 彼此互相垂直的拉丁方陣 MOLS(Mutually Orthogonal Latin Squares)

由於我們需要用到有限體 (Finite Field) 的觀念，因此先介紹這個代數結構。

定義 3.1. 一個集合 F 及兩個運算 $+,\cdot$，構成一個代數結構 $(F,+,\cdot)$ 爲一體 (Field) 假如下列的條件成立：

(i) $(F,+)$ 爲一交換群，

(ii) $(F,\cdot)$ 爲一交換群，其中 F^* 爲 F 扣除加法單位元素 0，及

(iii) 分配律成立，$a\cdot(b+c)=a\cdot b+a\cdot c$，$a,b,c\in F$。

如果 F 爲一有限集合，則此體稱爲一有限體。

定理 3.2. 一個有限體 $(F,+,\cdot)$ 存在的充分必要條件爲 $|F|=p^k$，p 爲質數，k 爲正整數。

証明. 請參考代數課本。

對於上述定理的證明，在此略述綱要。在必要條件方面，F 可以看成是佈於 Z_p 的一個向量空間，如果是 k 維，則 $|F|=p^k$。另一方向，我們需要證明存在有一個在 Z_p 上不可分解 (Irreducible) 的 k 次多項式，例如 x^2+x+1 在 Z_2 上不可分解，因此存在一個有限體它的元素個數爲 2^2。

有了定理 3.2，就可以得到垂直拉丁方陣的研究上最重要的定理。

定理 3.3. 對於所有的質數 p 及正整數 k，都存在有 p^k-1 個彼此互相垂直的 p^k 階拉丁方陣。

證明. 由定理 3.2，我們知道對於任意的質數方 p^k，都存在有一個體 $(F,+,\cdot)$，其中 $|F|=p^k$。因此 $|F^*|=p^k-1$。對於 F^* 中的任意一個元素 h，定義一個 $p^k\times p^k$ 的陣列 $L^{(h)}=\left[l_{ij}^{(h)}\right]$ 使得 $l_{ij}^{(h)}=i\cdot h+j$，$i,j\in F$。首先，我們核對 $L^{(h)}$ 爲一拉丁方陣 (?) 然後再判斷任給 $h,h'\in F^*$ 與 $L^{(h')}$ 是否垂直。假設 $l_{ij}^{(h)}=l_{i'j'}^{(h)}$，且 $l_{ij}^{(h')}=l_{i'j'}^{(h')}$ 則 $i\cdot h+j=i'\cdot h+j'$，且 $i\cdot h'+j=i'\cdot h'+j'$，所以 $(i-i')\,h=(j'-j)$，且 $(i-i')\,h'=(j'-j)$ 因爲 $h\neq h'$，所以 $i=i'$，於是 $j=j'$。因此我們證明了 $L^{(h)}$ 與 $L^{(h')}$ 垂直。 ■

這個定理也說明存在有三個互相垂直的 4 階拉丁方陣 (例 3) , 然而對於不是質數方階的情況 , 是否存在有互相垂直的拉丁方陣 , 就沒有這麼容易了。譬如 $6, 10, 12, \cdots$ 。首先 , 我們可以回答 12 階的情況。

定義 3.4. 令 $A = [a_{ij}]$ 及 $B = [b_{ij}]$ 分別爲 l 階及 m 階之拉丁方陣 , 則 $A \times B$ 稱爲是 A 與 B 的卡迪遜積 (Cartesian Product) , 可以定義成 $[(A, b_{ij})]_{m \times m}$, 其中 (A, b_{ij}) 爲一 l 階拉丁方陣 , 它的 (i', j') 位置之元素爲 $(a_{i'j'}, b_{ij})$ 。

因此 $A \times B$ 爲一 $l \cdot m$ 階拉丁方陣 , 下面例子是由 3 階拉丁方陣與 4 階拉丁方陣的乘積所得到的 12 階拉丁方陣。

例11.

$$A = \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline \end{array} \qquad B = \begin{array}{|cccc|}\hline 1 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \\ 2 & 3 & 4 & 1 \\ \hline \end{array}$$

(1,1) (2,1) (3,1) (2,1) (3,1) (1,1) (3,1) (1,1) (2,1)	(1,4) (2,4) (3,4) (2,4) (3,4) (1,4) (3,4) (1,4) (2,4)	(1,3) (2,3) (3,3) (2,3) (3,3) (1,3) (3,3) (1,3) (2,3)	(1,2) (2,2) (3,2) (2,2) (3,2) (1,2) (3,2) (1,2) (2,2)
(A,4)	(A,1)	(A,2)	(A,3)
(A,3)	(A,2)	(A,1)	(A,4)
(A,2)	(A,3)	(A,4)	(A,1)

我們不難把上面的拉丁方陣轉變成以 $1,2,\cdots,12$ 所填出來的拉丁方陣 (?) 。

定理 3.5. 若是 A_1 與 A_2 爲互相垂直的 l 階拉丁方陣 , B_1 與 B_2 爲互相垂直的 m 階拉丁方陣 , 則 $A_1 \times B_1$ 與 $A_2 \times B_2$ 爲互相垂直的 $l \cdot m$ 階拉丁方陣。

証明. 由乘積的定義可以直接核對 。

推論 3.6. 當 $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}$ 時 , 存在有 $\min\limits_{i=1}^{s} \{p_i^{k_i} - 1\}$ 個互相垂直的 n 階拉丁方陣 。

証明. 由定理 3.2 及 3.5 可得證 。
(**註**) 存在有多少個並不代表一共就只有這麼多 , 譬如推論 3.6 , 存在有兩個互相垂直的 12 階拉丁方陣 ; 但是目前已經可以找到 3 個 。

由推論 3.6 , 我們不難看出眞正有問題的是那些是 2 的倍數 , 但是它不是 4 的倍數 , 即所有的 $n \equiv 2 \pmod 4$ 。第一個面對的數 2 , 很容易看出沒有兩個互相垂直的拉丁方陣 ; 那麼 6 呢 ? 於是尤拉在看到這個現象 , 在努力尋找 6 階互相垂直的拉丁方陣失敗之後 , 他猜測 (很久以前) ; 對於所有 $n \equiv 2 \pmod 4$, 皆不存在有任何互相垂直的 n 階拉丁方陣 。

到了 1900 年 , Terry 他證實了尤拉的第一個猜測數字 $n = 6$ 是對的 。據說 , 他是把所有的 6 階方陣都 "適當" 地列出之後 , 兩兩比較而得到證明的 。然而 , 尤拉也只有猜對這個數而已 , 在 1960 的兩篇論文中 , 三位作者證明了下列結果 。(証明省略) 。

定理 3.7. (Parker, Bose, Shrikhande, 1960)
對於所有的正整數 $n \neq 2, 6$, 都存在有兩個互相垂直的 n 階拉丁方陣。

可是 MOLS 的研究並未因此而大功告成 , 對於不是質數方的數 , 究竟有多少個 MOLS's 目前仍然是個謎 。值得一提的是 MOLS 也是非常有用的工具 , 我們將會再提到它 。

4. 投影平面 (Projective Plane)

實驗設計可以應用的幾何上是一個非常有趣而且重要的發展。投影平面就是其中的一個重要例子。再第二節的例 9，我們曾提及，在一個設計中（不一定是區組設計），可以把 V 的元素當作點，$\mathfrak{B}$ 中的區組當作線，如此一來有了點線及點線關係，就有幾何的存在。例 9 有下列兩個特性:

(P_1) 任兩點決定唯一的線。

(P_2) 任兩線交於唯一的點。

定義 4.1. 滿足 (P_1) 及 (P_2) 的設計 $(V, \mathfrak{B})$ 稱爲投影平面。若是 $|V| < +\infty$，則稱爲是有限投影平面 (Finite Projective Plane)。如果 V 中存在有 4 個點且任 3 點皆不在同一線上 (P_3)，則 $(V, \mathfrak{B})$ 爲非退化 (Nondegenerate) 投影平面，反之則爲退化投影平面。

在本節討論的都是非退化的有限投影平面，也就是滿足 (P_1)，(P_2) 及 (P_3)。例 9，可以用下圖來表示出來。

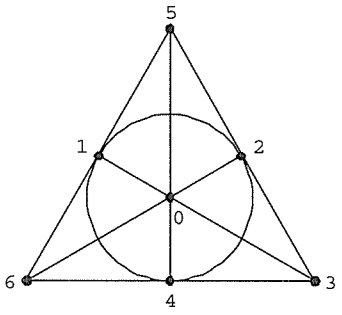

圖 4.1 : The Fano Plane.

值得在此說明的是 (P_2) 基本上和歐幾里德的平行公設是相違背的，因爲，過線外一點找不到不和此線相交的線。因此我們可以定義出一套不同的幾何，即投影幾何。投影幾何的發展可以追溯到西元第四世紀 Pappas 的研究，然後才導至十九世紀 Boole, Cayley 及 Sylvester 不變量代數理論的產生，接下來有 Tensor Calculus（張量微積分）的成果，最後才會有愛因斯坦的萬有引力 (Gravitation) 理論。

接下來我們探討一下投影平面的基本性質。

定理 4.2. 在投影平面中，存在有四條線，其中任三條皆不令有共同的交點 (P_4)。

証明. 由 (P_3)，存再有四個點 x, y, z, w 任三點皆不在同一線上。令 l_1, l_2, l_3, l_4，分別爲由 x 與 y，y 與 z，z 與 w 及 w 與 x 所決定的線。由於任三點皆不在同一線上，所以此四條線皆不相同。不失一般性，假設 l_1, l_2 與 l_3 有一共同交點 u，因爲 y 不在 l_3 上，$u \neq y$，如此一來 l_1 與 l_2 交於 y 及 u 不同的兩點，此與 (P_2) 矛盾，故得證。 ■

仔細觀察定理 4.2 中的 (P_4) 及 (P_3) 之間的關係，及 (P_1) 與 (P_2) 的關係，我們不難發現，它們只是點、線的角色互換而已。這種點、線互換的特性，也稱爲是對隅性 (Duality)。由於證明投影平面的特性時都要用到 (P_1)，(P_2) 及 (P_3)，所以加 (P_4)，對隅的結果也都會成立，所以下面的定理自然成立。

定理 4.3. (對隅性原則)

投影平面的任何敍述如果是一個定理，則它的對隅敍述也是一個定理。

接下來是投影平面的一些特性。

定理 4.4. 在投影平面中，每一點都會落在一樣多的線上，每一線也會有一樣多的點。

証明. 我們只要證明每一線都含有一樣多的點即可。(對隅性原則)。令 L, L' 爲任意兩線；則存在有一點 x，x 不在 L 及 L' 上。(?) 於是對於 L 上的任一點 a，通 a, x 的線必交 L' 於一點 a'，我們 a' 爲 a 經過 x 在 L' 上的投影，所以 L 上的點與 L' 上的點有 $1-1$ 的對應，故得證。 ■

定理 4.5. 在投影平面中，通過一點的線數等於每一線上的點數。

証明. 任選一線 L 及不在 L 上的一點 x，對於 L 上的任一點 y 定義 $L(y)$ 爲通過 y, z 的線，於是 y 與 $L(y)$有 $1-1$ 的對應故得證。 ■

推論 4.6. 在一個投影平面中，如果每條線上有 $m+1$ 個點，則此平面共用 m^2+m+1 個點及 m^2+m+1 條線。

証明. 令 x 爲任一點，由對隅性，通過 x 的線有 $m+1$ 條，因此總點數爲 $(m+1)\cdot m+1$，故得證。 ■

讀了這麼多投影平面的特性，究竟有投影平面存在嗎？例 9 就是一個 2 階的投影平面 (Order 2)，每一線有 $m+1$ 個點的投影平面是 m 階投影平面。下面是 3 階的例子。

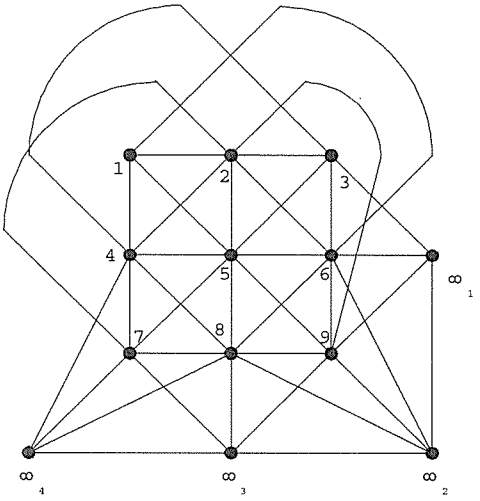

圖 4.2

定理 4.7. 對於 $m \geq 2$，一個 m 階投影平面存在的充要條件爲一個 $(m^2+m+1, m^2+m+1, m+1, m+1, 1)-$ 設計存在。

要證明這個定理，我們需要知道對稱設計的一些特性。

定義 4.8. 一個 $(b, v, r, k, \lambda)-$ 設計在 $b = v$ 的情況下稱爲是對稱設計，簡記爲 $(v, k, \lambda)-$ 設計。

對稱設計有很多特性，其中最重要的一個性質是下面的定理所敍述的特性。

定理 4.9. 在一個 $(v, k, \lambda)-$ 設計中，任意兩個區組的交集恰含有 λ 個元素。

証明. 省略。

現在，定理 4.7 也就不難證明（作業）。然而，定理 4.7 卻留下了一個同樣困難解決的問題，即 "$(m^2+m+1, m+1, 1)-$ 設計何時存在 ?" 。這方面的研究，一直到今天，仍然是組合數學最想知道答案的一個問題。儘管一般而言，沒有明確的答案，不過在一些特殊情況已經有了結果。

定理 4.10. (Bose,1938)

在 $m \geq 2$ 的情況下，m 階投影平面存在的充要條件爲 $m-1$ 個 m 階彼此互相垂直的拉丁方陣存在。

証明. 省略。

因此由定理 3.3，當 m 爲質數方的形式，都存在有一個 m 階的投影平面。另一個定理則是把一些不可有投影平面的階數找出來，証明省略。

定理 4.11. (Bruck, Ryser 1949)

在 $m \equiv 1$ or $2 \pmod 4$ 時，令 d 爲 m 的最大平方因數，如果 $\frac{m}{d}$ 可以被 $4k+3$ 形式的質數整除，則不存在有 m 階的投影平面。

例如 $m=6$，$m=54$，$m=3t^2, 6t^2$ 等都是例子。下面的定理則是更明確地把投影平面存在的必要條件找出來。它的證明也在此省略。

定理 4.12. (Bruck-Ryser-Chowlam, 1950)

$(v, k, \lambda)-$ 設計存在的必要條件是：

(1) 假如 v 是偶數，則 $k-\lambda$ 爲一平方數。

(2) 假如 v 是奇數，則 $x^2 = (k-\lambda)\, y^2 + (-1)^{(v-1)/2}\, \lambda z^2$ 有不全爲 0 的整數解，x, y, z。

投影平面存在的必要條件，由定理 4.7 的角度來看，即爲此定理的特別情況。

（**註**）n 階投影平面的研究，對於 $n \leq 10$，目前已全部解決，即 $n = 6, 10$ 不存在，$n=1$ 退化，其它階數階存在。

5. 仿射平面 (Affine Plane)

一個 BIBD $(V, \mathfrak{B})$ 如果它的 b 個區組可以分解成 t 個部分，使得在每一個部分每一個 V 中的元素都恰好出現一次，即此設計爲可分解的 BIBD (Resovable BIBD)。一個可分解的 BIBD 又稱爲是仿射可分解的 BIBD，如果來自不同部分的區組都會交於固定個數的元素。例 10 就是一個例子，例 11 則是一個可分解但不是仿射的 BIBD。

例11.

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

例 11 同時也是問題 2 的一組答案。

定理 5.1. 任意的 $(k^2, k^2+k, k+1, k, 1)$–設計皆爲仿射可分解的 BIBD。

証明. 令 B_0 爲設計 $(V, \mathfrak{B})$ 中的任一個區組。因爲 $\lambda = 1$，所以 B_0 和其它區組的交集最多只有一元素。由 $r = k+1$，所以對於 B_0 中的任一個元素尙有 k 個不同於 B_0 的區組包含此元素，因此在 $(V, \mathfrak{B})$ 中有 $(k^2+k)-k\cdot k-1 = k-1$ 個區組和 B_0 的交集爲空集合，現在考慮這些區組中任一個元素，它和 B_0 中的任一個元素共同出現於一個區組，一共有 k 個，所以，還有一個區組 B' 含有此一元素，但是 $B' \cap B_0 = \phi$；因爲對於不在 B_0 的 k^2-k 個元素而言，每個元素都要出現在一個不與 B_0 相交的區組中，而且一共只有 $k-1$ 這樣的區組，所以 k^2-k 個元素必定是分配在彼此不相交的 $k-1$ 個區組上，於是和 B_0 形成一個分解族 (Resolution class)，即 V 中的每一個元素都恰好出現一次。由於 B_0 爲對任意選擇的區組，所以每一區組都是在某一個分解族中，這證明了 $(V, \mathfrak{B})$ 是可分解的 BIBD。由上面的證明也不難看出來自不同分解族的兩個區組必定會交於一點，所以 $(V, \mathfrak{B})$ 是仿射可分解的 BIBD，故得證。 ■

我們可以利用定理 5.1 的設計來建構一個對稱的 $(k^2+k+1, k+1, 1)$–設計，也就是 k 階的投影平面。它的方法如下：令上述設計的 $k+1$ 個分解族分別爲 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{k+1}$，現在令 $V' = V \cup \{\infty_1, \infty_2, \cdots, \infty_k\}$，$\mathfrak{B}' = \{B' | B' = B \cup \{\infty_i\},\ B \in \varepsilon_i, i = 1, 2, \cdots, k+1\} \cup \{\infty_1, \infty_2, \cdots, \infty_{k+1}\}$。於是

$(V', \mathfrak{B})$ 爲所求。圖 4.2 就是利用例 10 的仿射可分解設計所建構出來的 3 階投影平面。

定義 5.2. 一個 $(k^2, k^2+k, k+1, k, 1)$–設計又稱爲是 k 階的仿射平面 (Affine Plane)。

現在我們可以把上面建構的方式反過來，也就是利用 k 階的投影平面來建構 k 階的仿射平面 (?)。於是就得下面的定理。

定理 5.3. k 階的投影平面存在若且唯若 k 階的仿射平面存在。

定理 5.4. 一個k 階仿射平面存在的充要條件爲 $k-1$ 個彼此互相垂直的k 階拉丁方陣存在。

証明.
($\Leftarrow$) 令 $L_3, L_4, \cdots, L_{k+1}$ 爲 $k-1$ 個彼此互相垂直的k 階拉丁方陣，同時 R 爲第 i 列全部填 i 的 k 階陣列。現在考慮 $k+1$ 個陣列 $L_1(=R)$, $L_2(=R^*)$, $L_3, L_4, \cdots, L_{k+1}$ 及 $A = [a_{ij}]_{k\times k}$, $a_{ij} = (i-1)k+j$。我們利用 $k+1$ 個拉丁方陣來定義 $k+1$ 個分解族：第 i 個分解族的第 j 個區組 $B_{ij} = \{x |\, L_i(i', j') = j$ 且 $a_{i'j'} = x\}$。由垂直拉丁方陣的定義可以證明這些區組所成的集合形成一個 k 階的仿射平面。(?)
($\Rightarrow$) 反過來，我們要利用 $k+1$ 個分解族來建構 $k-1$ 個彼此互相垂直的k 階拉丁方陣。令 $R_l, R_c, R_1, R_2, \cdots, R_{k-1}$ 爲仿射平面的 $k+1$ 個分解族；首先，我們將每個分解族的區組給定順序，即第一個區組至第 k 個區組；然後第 t 個拉丁方陣可以用下列方式填入：若是 R_l 的第 i 個區組與 R_c 的第 j 個區組的交集 $\{ak+b\}$, $0 \le a \le k-1$, $1 \le b \le k$；則在 L_t 的 (a, b) 位置上填入 y，其中 y 來自 R_l 第 i 個區組與 R_t 的第 j 個區組之交集 $\{xk+y\}$, $0 \le x \le k-1$, $1 \le y \le k$。此種填法可以得到 $k-1$ 個彼此互相垂直的k 階拉丁方陣。故得證。 ∎

由定理 5.3 及 5.4，我們可以得知k 階投影平面，k 階仿射平面及 $k-1$ 個 MOLS(k) 的存在是等價的關係。

作業.

41. 我們以 $GF(q)$ 代表一個具有 q 個元素的有限體。先建構一個有限體 $GF(4)$, 再利用它來產生三個互相垂直的 4 階拉丁方陣 。
42. 令 N_m 代表不同 m 階拉丁方陣的個數。已知 $N_1 = 1$, $N_2 = 2$, $N_3 = 12$, 求 N_4 。
43. 証明定理 1.6 。
44. 試證在一個 (v, b, r, k, λ)–設計中 , $\lambda(v-1)/(k-1)$ 及 $\lambda v(v-1)/k(k-1)$ 皆爲整數 。
45. 証明定理 3.5 。
46. 試證在一個 (v, b, r, k, λ)–設計中 , $b \geq v$ 。

    提示 :

    (a) 定義一個設計 $(V, \mathfrak{B})$ 的相接矩陣 $A = [a_{ij}]_{v \times b}$, 其中 $a_{ij} = 1$ 假如 $x_i \in B_j$, $1 \leq i \leq v$, $1 \leq j \leq b$, $V = \{x_1, x_2, \cdots, x_v\}$ 且 $\mathfrak{B} = \{B_1, B_2, \cdots, B_b\}$, 另外的位置 $a_{ij} = 0$ 。

    (b) 証明 $det(AA^T) = [r + (v-1)\lambda](r-\lambda)^{v-1}$ 。
47. 証明定理 4.7 。
48. 証明定理 4.9 。**提示 :** 令 J 爲 v 階全部爲 1 的方形矩陣 , 則 $AJ = KJ$, $AA^T = (k-\lambda)I + \lambda J$, $A^{-1}J = K^{-1}J$, $A^TA = (k-\lambda)I + \lambda k^{-1}JA$, 且 $JA = kJ$ 。
49. 利用 m 階互相垂直拉丁方陣存在的理由 , 証明一個 l 階的拉丁方陣, $l \leq m$, 一定可以伸展成一個 (l+m) 階的拉丁方陣 。