

組合設計講義

Combinatorial Designs

(Lecture Notes)



傅恆霖 (Hung-Lin Fu) 教授 編著

國立交通大學應用數學系

序

組合設計 (Combinatorial Design) 主要是在研究實驗設計 (Experimental Design) 中的數學結構，隨著這方面知識的增加，除了在理論上可以推廣外，另一方面也能在應用上扮演重要的角色。近代訊息的傳遞仰賴數位化的字碼，而錯誤更正碼 (Error-Correcting Code) 的設計恰好與組合設計的建構相呼應，這種現象也使得組合設計的研究更為重要；另一方面，特殊的設計也可以在暗碼理論 (Cryptography) 中一展身手，誰知道，還有什麼領域會用到組合設計呢？

利用在交大應數系及淡江數學系開課教組合設計的機會，將筆記整理成講義，以供同學參考，希望能對同學的學習有所助益。

這本講義能夠完成，最大的功臣應該是交大應數系組合數學組研究生鄭凱鐘同學；他不斷地利用時間辛勤的打字、核對並修改，直到最後完成，再一次表示我最大的感激。其他，如淡江大學的高金美教授及高雄師大李珠矽教授也協助看稿，並提供修改意見，在此一併誌謝。最後，我一定要感謝已畢業的方瑗菱同學，由於她完成了史坦納三元系那一章的初稿，使我下定決心要繼續完成這講義。其他沒有提到名字的兩校同學們，謝了！！

目 錄

第一章	拉丁方陣	1
1.	基本性質	2
2.	拉丁長方陣與部分拉丁方陣.....	12
3.	極大部分拉丁方陣與臨界集.....	20
4.	垂直拉丁方陣	28
5.	全截集 (Transversal)	38
6.	特殊的拉丁方陣	47
7.	魔方陣 (Magic Square)	54
8.	Room 方陣	60
第二章	史坦納三元系	65
1.	史坦納三元系的建構 (直接建構法)	65
2.	遞迴建構法	68
3.	STS 的嵌入	73
4.	λ -層三元系	75
5.	可分解的三元系 (Kirkman Triple System)	78
6.	K_n 的裝填 (Packing)	80
7.	K_n 的覆蓋 (Covering)	82
8.	史坦納三元系圖	83
第三章	一般的組合設計	85
1.	配對平衡設計 (Pairwise Balanced Design, PBD)	85

2. 可分組設計 (Group Divisible Design , GDD)	90
3. 橫截設計 (Transversal Design)	95
4. 刪點橫截設計 (Truncated Transversal Design , TTD)	99
5. BIBD with $k=4$	103
6. 利用 PBD 推翻尤拉猜測	106
第四章 史坦納四元系	112
1. t -設計.....	113
2. 史坦納四元系的介紹.....	116
3. 兩倍式建構法 (Doubling Construction)	120
4. $SQS(v)$ 存在的充分條件.....	126
第五章 圈系	131
1. 4-圈系	131
2. 圈系的嵌入問題	138
3. Alspach 的問題	140
4. 具有指定殘留的圈系	143
5. 可分組圈系 (GDD Cycle System)	146
6. 圈系的嵌入問題	150
第六章 組合設計的應用	154
1. 錯誤更正碼	154
2. 設計與數碼 (Design and Code)	159
3. 暗碼學 (Cryptology)	162
4. 拉丁方陣與暗碼學	164

第一章 拉丁方陣

拉丁方陣 (Latin Square) 究竟是什麼時候發現的，到今天仍然沒有明確的答案。由於它的型式看起來比一般的魔方陣 (Magic Square) 簡單，所以有人相信它的存在應該有上千年的歷史，可是有文獻記載的年代卻是在十八世紀了。另一方面，由於一個有限群 (Finite Group) 的運算表可以形成一個拉丁方陣，所以也有人認為有抽象代數的存在，就有了這個看起來不太起眼的”組合設計”或”代數結構”。

能夠找到的最早參考文獻是討論把撲克牌中的四個大牌 A,K,Q,J 各四種花色，共十六張牌放在一個 4×4 的格子中，使得橫看直看，每樣花及每樣牌都出現的放置方法數，那文章發表於 1732 年。大約在 50 年後，尤拉 (Euler) 提出了相似的問題，他希望將來自六個軍種，六個官階的 36 位軍官排成 6×6 的陣列，使得橫看直看都可以有來自不同軍種的六個官階的軍官；同時經過一番奮鬥之後，他猜測這樣的陣列是不可能存在的。這個猜測，德利 (Tarry) 在 1900 年用直接比較所有可能 6 階拉丁方陣的方法，獲得證實，而真正利用理論的方式證明這個猜測又得等上 80 年哩！在拉丁方陣的研究中與此猜測相關的研究—互相垂直的拉丁方陣 (Orthogonal L.S.) 佔最大的比例，相關的文獻數以千計。

拉丁方陣除了本身具有很好的代數結構—擬似群 (Quasigroup)，同時在應用上也是十分的活躍，尤其在實驗設計 (Experimental Design) 方面；而應用於其他領域，如組合設計的建構，以及近代暗

碼及編碼的設計，也有不可思議的貢獻。

1. 基本性質

一個定義於 S 的 n 階拉丁方陣是一個 $n \times n$ 的陣列 $L = [l_{i,j}]$ ，其中所有的 $l_{i,j}$ 皆屬於一個具有 n 個元素的集合 S ，同時在 L 中每一行及每一列都具有 S 中的每一個元素。也就是說，如果 L 為一定義於 S 的 n 階拉丁方陣，則來自 S 的每一個元素在 L 中的每一行及每一列都恰好出現一次。顯然， S 可以是任意的集合，但是為了便於表示，以及與代數結構拉上關係，除非特別說明，我們都將令 $S = \mathbb{Z}_n$ 作為一個 n 階拉丁方陣的元素集。圖 1.1 分別為 2, 3, 4 及 5 階拉丁方陣的例子。

0	1
1	0

0	2	1
2	1	0
1	0	2

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

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

圖 1.1

從上面的例子，我們可以發現，如果利用拉丁方陣來定義一個運算，則可以得到一個二元運算，而且這個運算具有特殊性質。

引理 1.1. 令 $L = [l_{i,j}]$ 為一 n 階拉丁方陣，則由 $*(i, j) = l_{i,j}$ 所定義的函數 $*$ ： $\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ 為一二元運算，同時滿足對於任一個有序數對 (a, b) ， $a, b \in \mathbb{Z}_n$ ， $a * x = b$ 及 $y * a = b$ ，在 $\mathbb{Z}_n$ 中皆有唯一解。

證明： 可以由拉丁方陣的定義推得。 ■

定義 1.2. 令 S 為一非空的集合， $*$ 為 S 中的一個二元運算。如果對

於 S 中的任意兩個元素 a, b , $a * x = b$ 及 $y * a = b$ 在 S 中皆有唯一解，則代數結構 $(S, *)$ 稱為是一個擬似群 (Quasigroup)。

顯然，由引理 1.1，我們可以利用拉丁方陣來定義擬似群。當然，反過來，由一個具有 n 個元素的擬似群，我們也可以得到拉丁方陣。圖 1.2 為一般形式的擬似群。

$*$	0	1	2	...	j	...	$n-1$	
0					$\vdots$			
1					$\vdots$			
2					$\vdots$			
$\vdots$					$\vdots$			
i	...	...	...	...	$l_{i,j}$	...	...	$L = [l_{i,j}]$
$\vdots$					$\vdots$			
$n-1$					$\vdots$			

圖 1.2

由於一個群顯然具有擬似群的性質，所以，下列定理提供了很多拉丁方陣的例子。

定理 1.3. 有限群的運算表形成一個拉丁方陣。

證明： 群的基本性質。 ■

然而，拉丁方陣（擬似群）與群仍有一段距離；因為一個擬似群不一定具有結合律 (Associative Law)，於是判斷一個擬似群是否為一群就等於是在判斷擬似群中是否具有結合律。截至目前為止，最好的方法（演算法）需要測試 $3n^3/8$ 個有序對 (a,b,c) ，當然，在這個擬似群具有特殊結構時會好些，也就是不必測試那麼多次；或者，當這個擬似群的最小生成集 (Minimal Generating Set) 是已知時，也可以測試較少次，大約是 $n^2 \lceil \log_2 2n \rceil$ 。以下是衍生出來的幾個問題：

問題 1.1. 如何才能最快速地測試出一個擬似群具有結合律？

問題 1.2. 在一個擬似群中有些 (a, b, c) (好的序對), $(ab)c = a(bc)$ 是成立的, 但是在一個擬似群中最多可以有多少個好的序對 (最多 n^3 個), 而該擬似群仍然不具有結合律呢？

以下我們討論一些特殊的擬似群, 相對應的就是特殊的拉丁方陣。

定義 1.4. 若 $Q' \subseteq Q$, 且對於 Q 的運算 $*$, $\langle Q', * \rangle$ 也是擬似群, 則 Q' 稱為是 Q 的擬似子群, 以 $Q' \leq Q$ 表示。

和群不一樣的是當 Q 為有限擬似群且 $Q' \leq Q, |Q'| \mid |Q|$ 不一定成立, 參考圖 1.3 的例子。

0	1	3	4	2
1	0	2	3	4
3	2	4	0	1
4	3	1	2	0
2	4	0	1	3

圖 1.3

定義 1.5. 若 Q 為一擬似群, 且存在有一元素 $e \in Q$, 使得對於所有 Q 中的元素 a , $a * e = e * a = a$, 則 e 稱為是 Q 的單位元素; 具有單位元素的擬似群稱為是圈 (Loop)。

定義 1.6. 若 Q 為一擬似群, 且滿足對於 Q 中的任意兩個元素 a, b , $a * b = b * a$, 則 Q 為一可交換擬似群 (Commutative Quasigroup)。

爲了方便起見，以下我們用 ab 代表 $a * b$ 。

定理 1.7. 若 Q 爲一圈，且滿足 $(ab)c = a(cb)$ ，則 Q 爲一交換群。

證明：因爲 Q 具有單位元素 e ，所以任意的兩個元素 b, c ，

$$(eb)c = e(cb) \Rightarrow bc = cb, \text{ 即 } Q \text{ 滿足交換律。}$$

於是 $(ab)c = a(cb) = a(bc)$ ，即 Q 有結合律。

有結合律之擬似群爲一群（作業），故得證。 ■

定義 1.8. 在一個擬似群 Q 中，若對於任意的兩個元素 a, b ，皆滿足 $a(ba) = b$ ，則 Q 稱爲是半對稱（Semi-symmetric）擬似群；若 $a(ab) = b$ 且 $(ab)b = a$ ，則 Q 稱爲是全對稱（Totally Symmetric）擬似群。當 $a^2 = a$ 時，則 Q 爲等冪（Idempotent）擬似群，而當 $a^2 = c$ （ c 爲定數）時，則 Q 爲冪等（Unipotent）擬似群。

下列幾個定理對於描述特殊的拉丁方陣很有幫助，有^(*)的證明於下一章再詳細說明。（拉丁方陣可以由擬似群的運算表求得。）

定理 1.9. 一個全對稱擬似群必爲可交換擬似群，也一定是一個半對稱的擬似群。

證明：因爲 $a(ab) = b$ 且 $(a(ab))(ab) = a$ ，所以 $b(ab) = a$ ，亦即 Q 爲半對稱。又 $ba = b(b(ab)) = ab$ ，因此 Q 爲對稱擬似群。 ■

^(*)**定理 1.10.** 一個等冪全對稱擬似群存在的充要條件爲此擬似群的元素個數 $n \equiv 1$ 或 $3 \pmod{6}$ 。

定理 1.11. 一個冪等可交換擬似群存在的充要條件爲此擬似群的元

素個數是偶數。

證明：由於出現在對角線的元素都一樣，所以其他的元素出現的次數必為偶數。而這類擬似群的存在等價於把 K_{2m} 分解成 $2m-1$ 個 1-因子(1-factor)(?)，由於後者一定辦得到，所以定理得證。 ■

為了對定理 1.11. 有更進一步的瞭解，我們再以一個例子加以說明。

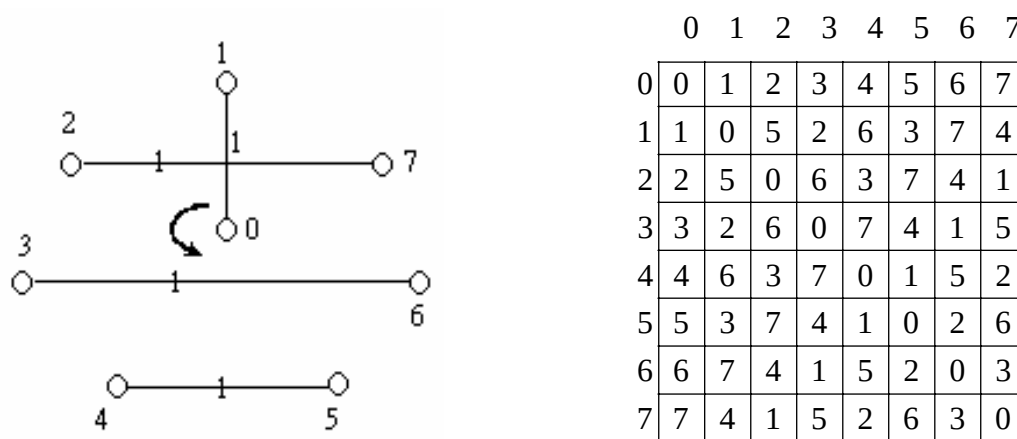


圖 1.4

有時候，我們也可以把上述 1-因子的分解（1-分解）（1-factorization）寫成

0	1	0	2	0	3	0	4	0	5	0	6	0	7
2	7	3	1	4	2	5	3	6	4	7	5	1	6
3	6	4	7	5	1	6	2	7	3	1	4	2	5
4	5	5	6	6	7	7	1	1	2	2	3	3	4

定理 1.12. 一個等幂對稱擬似群存在的充要條件為此擬似群的元素個數是奇數。亦即一個 n 階對稱等幂拉丁方陣存在的充要條件為 n 是奇數。

證明：由於每個元素出現的次數為 $1+2k$ （ $2k$ 來自對稱性），所以 n 為奇數。至於它的存在性可以利用 $\langle \mathbb{Z}_n, + \rangle$ 這個群的運算表加以排列即

可，該排列爲

$$\begin{pmatrix} 0 & 2 & 4 & \cdots & n-1 & 1 & 3 & 5 & \cdots & n-2 \\ 0 & 1 & 2 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & n-1 \end{pmatrix}.$$



爲了說明定理 1.12，特提供一個例子，參考圖 1.5。

0	1	2	3	4		0	3	1	4	2
1	2	3	4	0		3	1	4	2	0
2	3	4	0	1	→	1	4	2	0	3
3	4	0	1	2		4	2	0	3	1
4	0	1	2	3		2	0	3	1	4

圖 1.5

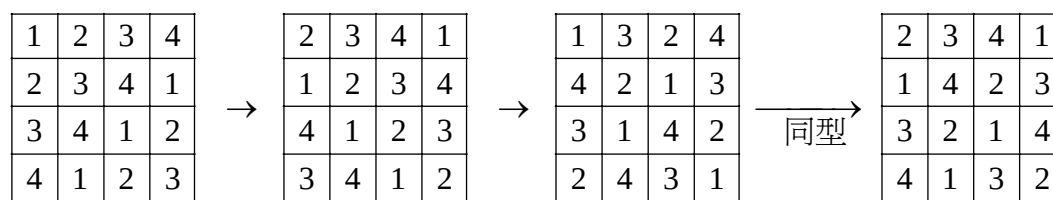
在這裡，我們注意到擬似群可以利用更換元素的方式來得到另一個。上述的例子是在固定運算的前兩個元素所得到的另一個擬似群。我們也可以更換第一或第二個位置，代數的術語爲側邊（Side line）及上邊（Head line）。

定義 1.13. 令 $\langle Q_1, \circ \rangle$ 及 $\langle Q_2, * \rangle$ 爲兩個擬似群，我們稱 Q_1 及 Q_2 爲同型（Isotopic）擬似群，以 $\langle Q_1, \circ \rangle \sim \langle Q_2, * \rangle$ 表示，若且唯若存在三個由 Q_1 映至 Q_2 的 1-1，映成函數 α, β, γ 使得對於所有的 $x, y \in Q_1$ ， $\alpha(x) * \beta(y) = \gamma(x \circ y)$ 。當 $\alpha = \beta = \gamma$ 時， Q_1 與 Q_2 同構（Isomorphic）。

定義 1.14. 兩個 n 階拉丁方陣 $L = [l_{i,j}]$ 及 $M = [m_{i,j}]$ 相等，記爲 $L = M$ ，若且唯若 $l_{i,j} = m_{i,j}$ ， $i, j \in \mathbb{Z}_n$ 。

定義 1.15. 兩個拉丁方陣若是能利用換列，換行或換元素而得到相等的拉丁方陣，則此二拉丁方陣稱爲是同型的拉丁方陣。

上述的換列，換行或換元素係指 Z_n 中元素的排列，以下是一個同型 4 階拉丁方陣的例子，及一個同構的例子。(圖 1.6 及圖 1.7)



$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

圖 1.6 同型拉丁方陣

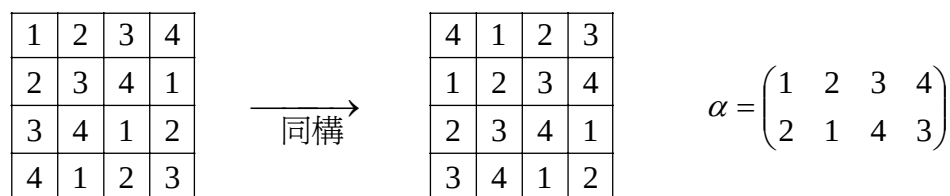


圖 1.7 同構拉丁方陣

所以我們可以探討下面三個問題：

問題 1.3. 不相等 n 階拉丁方陣有多少個？（個數以 L_n 表示）

問題 1.4. 不同型 n 階拉丁方陣有多少個？（個數以 r_n 表示）

問題 1.5. 不同構 n 階拉丁方陣有多少個？（個數以 L_n 表示）

在問題 1.3.方面，我們可以考慮另一種性質。當 $L \neq M$ 時， L 與 M 顯然在很多個位置 (i, j) ， $l_{i,j} \neq m_{i,j}$ ，相對地，有些位置所填的 $l_{i,j}$ 與 $m_{i,j}$ 是相同的，於是我們定義兩個拉丁方陣的交集。

定義 1.16. 令 $L = [l_{i,j}]$ 與 $M = [m_{i,j}]$ 為兩個 n 階拉丁方陣，則 $L \cap M = \{(i,j) \mid l_{i,j} = m_{i,j}, 1 \leq i, j \leq n\}$ ， $\text{Spec}(n) = \{t \mid |L \cap M| = t, L \text{ 與 } M \text{ 為 } n \text{ 階拉丁方陣}\}$ 。

顯然， $0 \in \text{Spec}(n)$ 且 $n^2 \in \text{Spec}(n)$ ，下面的敘述也很容易證明。

引理 1.17. $\text{Spec}(n) \subseteq \{0, 1, 2, \dots, n^2\} \setminus \{n^2-5, n^2-3, n^2-2, n^2-1\}$ 。

實際上，對於 $n \geq 5$ ，我們也可以得到等號。由於證明較複雜，在此省略。

定理 1.18.[Fu] $\text{Spec}(n) = \{0, 1, 2, \dots, n^2\} \setminus \{n^2-5, n^2-3, n^2-2, n^2-1\}$ 。

在問題 1.4 及問題 1.5 的研究，我們可以先探討同型及同構的關係是否為一等價的關係；如果是，則不同型或不同構的拉丁方陣之個數，也就是等價類的個數。

定理 1.19. 同型 (Isotopism) 為一等價關係。

證明：反身性的性質很明顯，所以我們先看對稱性。令 $\langle Q_1, * \rangle \sim \langle Q_2, \circ \rangle$ ，且對於所有 $x, y \in Q_1$ ， $\alpha(x) \circ \beta(y) = \gamma(x * y)$ 。現在，對於任意兩個元素 $x', y' \in Q_2$ ，存在有 $x, y \in Q_1$ ，使得 $\alpha(x) = x'$ ， $\beta(y) = y'$ 。由於 $x' \circ y' = \gamma(x * y)$ ，所以 $x * y = \gamma^{-1}(x' \circ y')$ ，亦即 $\alpha^{-1}(x') * \beta^{-1}(y') = \gamma^{-1}(x' \circ y')$ ，因為 $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$ 存在，所以 $\langle Q_2, \circ \rangle \sim \langle Q_1, * \rangle$ 。接下來，再看遞移律，令 $\langle Q_1, * \rangle \sim \langle Q_2, \circ \rangle$ 且 $\langle Q_2, \circ \rangle \sim \langle Q_3, \cdot \rangle$ 。因此，存在有 $\alpha_1, \beta_1, \gamma_1$ ； $\alpha_2, \beta_2, \gamma_2$ 滿足同型的條件。現在，對於 Q_1 中的任兩個元素 x, y ，令 $x'' = \alpha_2(\alpha_1(x))$ 及 $y'' = \beta_2(\beta_1(y))$ ，

$$x'' \cdot y'' = \alpha_2(\alpha_1(x)) \cdot \beta_2(\beta_1(y)) = \gamma_2(\alpha_1(x) \circ \beta_1(y))$$

$$= \gamma_2(\gamma_1(x * y)) = (\gamma_2 \circ \gamma_1)(x * y),$$

$$\text{因此, } (\alpha_2 \circ \alpha_1)(x) \cdot (\beta_2 \circ \beta_1)(y) = (\gamma_2 \circ \gamma_1)(x * y),$$

所以 $\langle Q_1, * \rangle \sim \langle Q_3, \cdot \rangle$ 。 ■

推論 1.20. 同構 (Isomorphism) 爲一等價關係。

在這裡特別說明一下，當 $\langle Q_1, * \rangle$ 爲一群時，若 $\langle Q_2, * \rangle$ 與 $\langle Q_1, \circ \rangle$ 同構，則 $\langle Q_1, \circ \rangle$ 亦爲一群 (?)。當然，群與群的同構爲擬似群同構的一個特殊情況。

作業

1. 證明具有結合律的擬似群必為一群。
2. 舉例說明一個擬似群可以不必是一個群。
3. 證明不相等的四階拉丁方陣有 576 個。
4. 試求 $\text{Spec}(5)$ 。
5. 試求 $f_{\alpha\alpha\alpha}$ 。(4 階不同型拉丁方陣個數)
6. 令 S_n 代表所有 Z_n 的排列所成的集合，對於 S_n 中的任一個排列 α_i ，以 $\alpha_i = (\alpha_i(0), \alpha_i(1), \dots, \alpha_i(n-1))$ 表示。令 $\alpha_1, \alpha_2, \dots, \alpha_m$ ， $m < n$ 為 m 個 S_n 中的排列，滿足對於所有的 $x \in Z_n$ ， $\alpha_{i_1}(x) \neq \alpha_{i_2}(x)$ ， $1 \leq i_1 \neq i_2 \leq m$ 。試證一定存在有一個拉丁方陣 $L = [l_{i,j}]$ ，其中 $l_{i,j} = \alpha_{i_1}(j-1)$ ， $1 \leq i \leq m$ 且 $1 \leq j \leq n$ 。
7. 假設 Q_1 與 Q_2 為同構的兩個擬似群，且 Q_1 為一群，試證 Q_2 亦為一個群。

2. 拉丁長方陣與部分拉丁方陣 (Latin Rectangle and Partial Latin Square)

從一個 n 階拉丁方陣，我們可以去掉數列而得到一個長方形陣列，它滿足在每一列所有 Z_n 中的元素都出現一次，而在每一行中， Z_n 中的元素最多出現一次。這樣的陣列，我們稱之為**拉丁長方陣**。顯然，我們知道拉丁長方陣的存在是不一定要先有拉丁方陣的存在。我們可以利用上一節作業 6 的概念，由排列來堆積出拉丁長方陣。然而，由以下的討論，我們將發現，任何的拉丁長方陣皆可以經由增加列而獲得一個拉丁方陣。

定義 2.1. 令 $S_1, S_2, \dots, S_n$ 為非空的 n 個集合。我們說集合族 $\{S_1, S_2, \dots, S_n\}$ 具有一組相異的代表元素 (System of Distinct Representatives , SDR)，若且唯若存在 n 個相異的元素 $a_1, a_2, \dots, a_n$ ，其中 $a_i \in S_i, i = 1, 2, \dots, n$ 。

以下的定理非常有名，通常稱之為 P. Hall 定理。

定理 2.2. $S = \{ S_1, S_2, \dots, S_n \}$ 具有SDR的充要條件為對於任意的 $1 \leq k \leq n$ ， S 中的任意 k 個集合的聯集包含至少 k 個元素 (Hall的條件)。

證明：(必要性) 很容易。

(充分性) 用歸納法。(對 n 歸納)，顯然，當 $n = 1$ 時成立。假設 $n = 1, 2, \dots, m$ 時皆成立。令 $\{S_1, S_2, \dots, S_{m+1}\}$ 為一個集合族，它滿足上述的條件。現在，在 $\{S_1, S_2, \dots, S_m\}$ 中，如果任意 h 個集合的聯集皆包含至少 $h+1$

個元素；則令 $x \in S_{m+1}$ 。再看集合族 $\{S_1 \setminus \{x\}, S_2 \setminus \{x\}, \dots, S_m \setminus \{x\}\}$ ，則任意 k 個集合的聯集必包含至少 k 個元素，所以此集合族有 SDR（歸納假設） $x_1, x_2, \dots, x_m$ ；於是再選 $x \in S_{m+1}$ ，就得到 $\{S_1, S_2, \dots, S_{m+1}\}$ 的一個 SDR。在另一種情況，如果存在有某 $k (\geq 1)$ 個集合 $S_1, S_2, \dots, S_k$ ，使得它們的聯集恰好包含 k 個元素。令 $S = \bigcup_{i=1}^k S_i$ ，然後考慮集合族 $\{S_{k+1} \setminus S, S_{k+2} \setminus S, \dots, S_{m+1} \setminus S\}$ ，則它有 SDR（？），再加上 $\{S_1, S_2, \dots, S_k\}$ 的 SDR，合併之後得到 $\{S_1, S_2, \dots, S_{m+1}\}$ 的 SDR。 ■

定理 2.2 也可以用圖論的方式加以證明。首先，我們建構一個二分圖 (A, B) ，其中 A 為 $\{S_1, S_2, \dots, S_n\}$ ， B 為 $\{x_1, x_2, \dots, x_l\}$ ， x_i 與 S_j 相連若且唯若 $x_i \in S_j$ ，於是 Hall 的條件可以看成任意 A 中的 k 個點，它們的相臨集至少有 k 個點。於是我們證明在滿足 Hall 的條件下，一定可以找到一個配對（Matching）它碰到 A 中的所有點。詳細證明請參考圖論課本，例如 D. West 所寫的圖論 [Introduction to Graph Theory]。

定理 2.3. 任何基於 Z_n 的 $r \times n$ ($r < n$) 拉丁長方陣均可以伸展成 n 階拉丁方陣。

證明：對於每一行定義一個集合 S_i 為尚未出現的元素所成的集合，然後證明 $\{S_1, S_2, \dots, S_n\}$ 有一個 SDR；再繼續這個步驟，直到填好 n 階拉丁方陣。所以，我們證明任意 k 個集合的聯集必含有 k 個以上的不同元素。不失一般性，令此 k 個集合 $S_1, S_2, \dots, S_k$ ，而已填好的部分稱

爲 A_k ；由定義 A_k 所填的元素，共有 rk 個，在加上多重集合 $S_1 \cup S_2 \cup \dots \cup S_k$ (multi-set) 中的元素一共有 kn 個，因此 $S_1 \cup S_2 \cup \dots \cup S_k$ 中有 $k(n-r)$ 個元素（可能相等），但是一個元素最多只能出現 $n-r$ 次，所以必含至少 k 個不同元素。 ■

接下來我們探討部分拉丁方陣 (Partial L.S.)。顧名思義，一個 n 階部份拉丁方陣是一個陣列，每個 Z_n 中的元素在此陣列中的每一行及每一列最多出現一次。一個佈於 Z_n 的滿填 $r \times s$ 部分拉丁方陣爲一 $r \times s$ 陣列， $r, s \leq n$ ，且 Z_n 中的每一元素在此滿填的陣列中，在每一行及每一列最多出現一次。圖 2.1 爲一佈於 Z_6 的滿填 3×3 部分拉丁方陣 (Completed Partial L.S.)。

1	2	4
6	5	3
2	1	5

圖 2.1

我們不禁要問這個陣列可以延伸（兩方向）爲 6 階拉丁方陣嗎？
首先，我們看必要性。

引理 2.4. 若是 R 代表一個滿填的 $r \times s$ 部分拉丁長方陣， $R(i)$ 代表元素 i 在 R 中出現的次數，則 R 可以被延伸爲一個 n 階拉丁方陣的必要條件爲 $R(i) \geq r + s - n$ 。

證明：先把已延伸好的拉丁方陣分成四部分，如圖 2.2。於是我們觀察 i 在其他部分出現的情形。因為 $B+C$ 為拉丁長方陣，每個元素恰好出現一次，所以 i 出現在 B 中最多 $n-s$ 次，因此 $R(i)+(n-s) \geq r$ ，即 $R(i) \geq r + s - n$ 。 ■

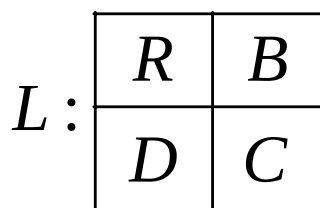


圖 2.2

定理 2.5. (Ryser) 一個滿填的 $r \times s$ 部份拉丁長方形 R ，可以被延伸為一個 n 階拉丁方陣的充分必要條件為 $R(i) \geq r + s - n$ 。

證明：必要性在引理 2.4. 已證明，不再重複。今假設 $R(i) \geq r + s - n$ 。令 $B^* = [b_{i,j}]$ 為 $r \times n$ 的 $(0,1)$ -矩陣，其中 $b_{i,j}=1$ 若且唯若 R 的第 i 列不含 j 這個元素。顯然， B^* 中的列和為 $n-s$ ，接著把 B^* 伸展成 n 階方陣 B' 使得列和與行和皆為 $n-s$ 。如此一來 B' 可以寫成 $n-s$ 個排列矩陣的和，於是 B 就可以填滿（圖 2.2）（？），再由定理 2.3.， R 可以伸展成一 n 階拉丁方陣。 ■

我們把 R 延伸成一個拉丁方陣 L ，就好像是把 R 嵌入於拉丁方陣 L 中，所以，一般也稱 R 嵌入（Embed）於 L 中。

由瑞射（Ryser）定理，我們很容易可以證明下面的定理。

定理 2.6. 若 $n \geq 2m$ ，則一個 m 階拉丁方陣可以嵌入於 n 階拉丁方陣中。

這個定理再次提醒我們若是 $Q' \leq Q$ (擬似群), $|Q'| \mid |Q|$ 是不一定對的。

我們不僅可以將一個拉丁方陣嵌入於另一個拉丁方陣, 我們也可以嵌入多個拉丁方陣於一個拉丁方陣中。最有用的一種這類型的拉丁方陣, 稱為是有洞的拉丁方陣, 其實這些洞是保留給較小的拉丁方陣。

定義 2.7. 互斥子集合 $H_1, H_2, \dots, H_k$ 的聯集為 Z_n 。我們稱拉丁方陣 $L = [l_{i,j}]$ 為一個具有洞的形式為 $|H_1| \times |H_2| \times \dots \times |H_k|$ 的有洞拉丁方陣, 如果它具有下列兩個性質:

1. 對於 H_l 中的任兩個元素 i, j , $1 \leq l \leq k$, (i, j) 是空白的位置。
2. 不是空白的位置填入 Z_n 中的元素, 使得每行, 每列, 每個元素最多出現一次, 而且若是 $t \in H_l$ (某一個 l), 則 t 不出現在第 t 行及第 t 列上面。

在上述定義中, 如果 $|H_1| = |H_2| = \dots = |H_k| = x$, 則它的形式以 x^k 表示。此時, 顯然 $n = kx$ 。我們將稱這個部分拉丁方陣為具有 $x \times x$ 洞的有洞拉丁方陣, 圖 2.3 是兩個例子。

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

		8	5	4	7	6	3
		6	7	8	3	4	5
8	6			7	2	5	1
5	7			1	8	2	6
4	8	7	1			3	2
7	3	2	8			1	4
6	4	5	2	3	1		
3	5	1	6	2	4		

(a)

(b)

圖 2.3 2^3 與 2^4 形式的有洞拉丁方陣

其實，你可以輕易地發現有洞的拉丁方陣是一個具有很多子拉丁方陣的拉丁方陣；而圖 2.3(a) 更是一個由一堆 2 階拉丁方陣所組合的 6 階拉丁方陣哩！對了，圖 2.3 的例子都是對稱的，但是這個性質並非必要。

以下，我們提供一個概念來說明 t^k 形式有洞拉丁方陣的存在性。

定義 2.8. 令 A 與 B 分別為 m 階及 n 階拉丁方陣，我們用 (x, B) 代表一個基於 $\{x\} \times Z_n$ 的 n 階拉丁方陣 $[(x, b_{i,j})]$ ，其中 $B = [b_{i,j}]$ 。我們定義 $A \times B = [(a_{i,j}, B)]$ ，其中 $A = [a_{i,j}]$ 。 $A \times B$ 稱為是 A 與 B 的乘積 (Direct Product)。

顯然 $A \times B$ 為 mn 階拉丁方陣，現在可以證明。

定理 2.9. 對於任意的正整數 t ，及 $k \neq 2$ ，皆存在有 t^k 形式的有洞拉丁方陣。

證明： 令 B 為 t 階拉丁方陣， A 為 k 階等冪拉丁方陣。再把 $A \times B$ 中的 $(a_{i,i}, B)$ 去掉，即為所求的有洞拉丁方陣。 ■

值得注意的是，如果我們要求此方陣具有對稱性，則當 k 是奇數時，並沒有任何困難求得（利用定理 2.9），但是，當 k 為偶數時，就沒有那麼容易了。不過，這樣的有洞拉丁方陣是有存在的可能。

定理 2.10.[Fu & Fu] 對所有的 $k \neq 2$ ， 2^k 形式的對稱有洞拉丁方陣

皆存在。

作業

1. 證明不相等的 n 階拉丁方陣至少有 $n!(n-1)!(n-2)! \dots 3!2!$ 個。
2. 利用圖論的方法證明 P. Hall 定理。
3. 如圖 2.4 所示，令 i 出現在 R 外面對角線 D 的次數為 $D(i)$ 。試證，如果 L 為固定 R 及 D 的 n 階拉丁方陣，則對於 $1 \leq i \leq n$ ， $R(i) \geq 2r - n + D(i)$ 。

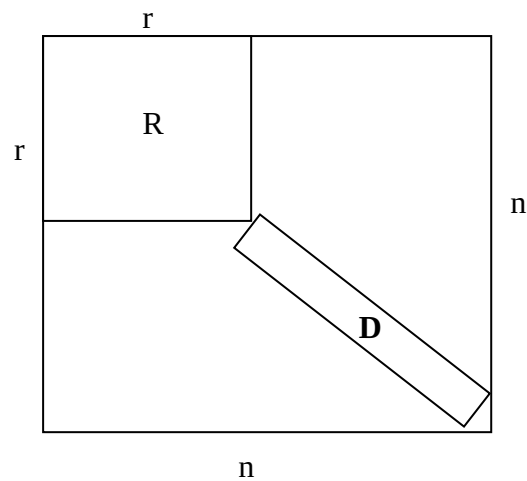


圖 2.4

4. 建構一個 $2n+2$ 階拉丁方陣，它含有一個 n 階的子方陣。
5. 建構一個 8 階 2^4 形的有洞拉丁方陣。
6. 建構一個最小階數拉丁方陣，它含有 2 階、3 階及 5 階子方陣。
7. 對於所有的 $n \geq 5$ ，證明必存在兩個 n 階拉丁方陣，它們只有一個位置相同。

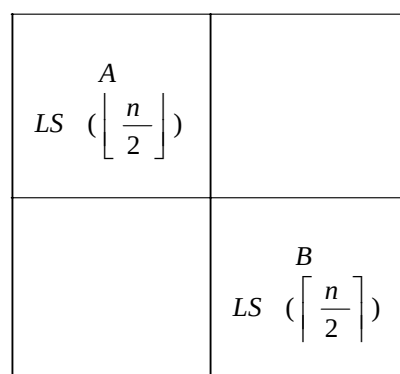
3. 極大部分拉丁方陣與臨界集

定義 3.1. 一個極大部分拉丁方陣 (Maximal P.L.S.) 為一個無法再填入任何元素的部分拉丁方陣，也就是說，再填入任一個元素就會造成至少有一列或一行，有一個元素至少出現兩次。

顯然，一個拉丁方陣也可以算是一個極大的拉丁方陣。為了研究這類方陣，我們定義 $Spec_M(n) = \{x \mid \text{存在有一個極大的部分拉丁方陣，它填了恰好 } x \text{ 個位置}\}$ 。所以 $\max.Spec_M(n) = n^2$ ，那麼 $\min.Spec_M(n)$ 呢？

定理 3.2. $\min.Spec_M(n) = \lfloor n/2 \rfloor^2 + \lceil n/2 \rceil^2$ 。

證明：首先，我們建構一個極大的部分拉丁方陣，它填了 $\lfloor n/2 \rfloor^2 + \lceil n/2 \rceil^2$ 個位置，如圖 3.1，因此 $\min.Spec_M(n) \leq \lfloor n/2 \rfloor^2 + \lceil n/2 \rceil^2$ 。



A 是基於 $Z_{\lfloor n/2 \rfloor}$ 的方陣，B 是基於 $\{\lceil n/2 \rceil - 1, \lceil n/2 \rceil - 2, \dots, n-1\}$ 的方陣

圖 3.1

接下來，證明另一方向。令一個極大部分拉丁方陣中，未填的位置有 t 個，以 $c_1, c_2, \dots, c_t$ 表示。現在考慮有序數對 (l, c_i) ， l 為已填的位

置，而且與 c_i 同行或同列， $1 \leq i \leq n$ 。由於 c_i 已不能再填，表示 (l, c_i) 至少有 n 對，所以，一共有 $\sum_{1 \leq i \leq t} (l, c_i) \geq tn$ 。再由行、列分別計算 (l, c_i) ，則得到 $2n \lfloor n/2 \rfloor \times \lceil n/2 \rceil \geq tn$ ，亦即 $t \leq \lfloor n/2 \rfloor \times \lceil n/2 \rceil$ 。

$$\begin{aligned} \text{於是} \quad \min. \text{Spec}_M(n) &\geq n^2 - 2 \lfloor n/2 \rfloor \times \lceil n/2 \rceil \\ &= (\lfloor n/2 \rfloor + \lceil n/2 \rceil)^2 - 2 \lfloor n/2 \rfloor \times \lceil n/2 \rceil \\ &= \lfloor n/2 \rfloor^2 + \lceil n/2 \rceil^2. \quad \blacksquare \end{aligned}$$

有了最小值，接著我們希望能決定 $\text{Spec}_M(n)$ 。以下是幾個可以用的技巧，我們分別以輔助定理表示出來。

引理 3.3. 若是 $x \in \text{Spec}_M(m)$ ，則對於所有的 $n \geq 2m$ ， $n^2 - m^2 + x \in \text{Spec}_M(m)$ 。

證明：令 M 為一嵌入於 n 階拉丁方陣 L 的一個 m 階拉丁方陣。由於 $x \in \text{Spec}_M(m)$ ，所以，必定存在一個極大的拉丁方陣 M' ，它恰好填了 x 個位置，現在，將 L 中的 M 取代為 M' ，則所得的部分拉丁方陣，為一 n 階拉丁方陣，而且填入的位置恰為 $n^2 - (m^2 - x) = n^2 - m^2 + x$ 。■

引理 3.4. 令 $[a, b]$ 代表由 a 至 b 的所有整數所成的集合， $I(n) = [\lfloor n/2 \rfloor^2 + \lceil n/2 \rceil^2, n^2] \setminus \{n^2 - 1\}$ ，則 $\text{Spec}_M(n) \subseteq I_M(n)$ 。

證明：顯然 $n^2 - 1 \notin \text{Spec}_M(n)$ ，加上定理 3.2.，所以得證。■

為了方便表示，我們用 $|L'|$ 代表部分拉丁方陣 L' 中所填的位置數。

定理 3.5. 對於 $n \geq 11$ ， $I(n)$ 中的每一個元素 x ，皆存在有一個極大的

部分拉丁方陣 L' 使得 $|L'| = x$ 。

證明：在此省略。 ■

問題 3.6. 決定 $\text{Spec}_M(10)$ 。

現在讓我們討論一下，一個可以繼續填成 n 階拉丁方陣的部份拉丁方陣。顯然，如果我們以往已填了 n 個位置，而且非常不小心，那麼極有可能永遠無法完成填好拉丁方陣的工作，如圖 3.2 所示，兩者都無法續完。當然，還有其他型式的部份拉丁方陣 M' ，它是無法續完的(?)。

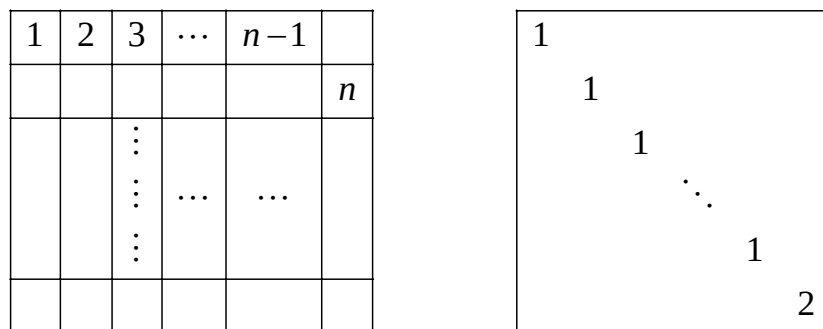


圖 3.2

但是，我們不難想像如果只填了 $n-1$ 個位置，那麼被填成一個 n 階拉丁方陣的機會就很大了。這個現象最早由 Evans 提出來是一個猜測，直到約 20 年後由 Smetaniuk 證明了這件事。

定理 3.7. (Evans 定理) 令 L' 為一填了 $n-1$ 位置的 n 階部分拉丁方陣，則 L' 必定可以被繼續填成一個 n 階拉丁方陣。

爲了要尊重 Evans，此定理雖由 Smetaniuk 證明，仍以他的名字稱此定理。這個定理不久再被安得生以一個更一般性的結果所涵蓋。

定理 3.8. (Lar Andersen) 一個填不到 $n+1$ 個位置的 n 階部分拉丁方陣除了下列的 13 種形式之外，皆可以繼續填成一個 n 階拉丁方陣。

這個定理的證明很長，詳細內容可以參考 L. Andersen 的論文。

由於可以繼續填完的現象，我們可以探討一種情況，當我們已經填了一些位置之後，剩下的位置就全部被唯一確定了；而這情況對於稍微少填一個位置卻不成立。例如，圖 3.3(a)為一個填了 4 個位置的 4 階拉丁方陣，顯然，要完成它只有一種方法，圖 3.3(b)。若是只填了 3 個位置，圖 3.3(c)，則唯一完成的現象就不見了。

1	2		
2			
			3

圖 3.3 (a)



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

圖 3.3 (b)

1	2		
2			

圖 3.3 (c)

定義 3.9. 一個 n 階拉丁方陣 C 稱為是臨界集 (Critical Set)，如果下列兩個條件同時滿足：

- (1) C 可以繼續填成一個 n 階拉丁方陣，而且此方陣是唯一的。
- (2) 去掉 C 中任何一個已填的位置，則無法唯一地填成 n 階拉丁方陣。

令 $C_M(n)$ 代表填了最多個位置的臨界集， $C_m(n)$ 為填了最少個位置的臨界集，則下列的結果並不難證明。

引理 3.10. 令 C 為一個 n 階臨界集，則 C 中填好的位置必定落在至少 $n-1$ 行上面，同時也落在至少 $n-1$ 列上面。

引理 3.11. 令 C 為一個 n 階臨界集，則 C 中填入的元素至少有 $n-1$

個是相異的。

定理 3.12. 對於所有的 $n \geq 5$ ， $C_m(n) \geq n + 1$ 。

證明：假設 $C_m(n) \leq n$ 。令 C 為填了 $C_m(n)$ 個位置的臨界集。由引理 3.11， $C_m(n)$ 必定不小於 $n-2$ ，所以我們分兩種情形討論：

(1) $C_m(n) = n-1$ 。由引理 3.10,11，我們知道這 $n-1$ 個元素必然都不相同，而且分佈於 $n-1$ 行及 $n-1$ 列上，所以我們可以找到一個位置，它與已經填入的位置不同行也不同列，現在不論這個位置填什麼，都可以利用安得生定理(3.8)證明它可以繼續填成一個 n 階拉丁方陣，所以 $C_m(n) \neq n-1$ 。

(2) $C_m(n) = n$ 。同理， C 中填入的位置必定落在至少 $n-1$ 行及 $n-1$ 列上，而且至少有 $n-1$ 個不一樣的元素，現在再觀察定理 3.8 的第 4~12 型，填入任何位置都不會造成其中一型，所以只要 $n \geq 5$ ，仍然可以繼續填成一個 n 階拉丁方陣，因此 $C_m(n) \neq n$ ，由(1),(2)我們推得對於 $n \geq 5$ ， $C_m(n) \geq n + 1$ 。

對於 $n < 5$ ，我們很容易可以求出 $C_m(n)$ 。

命題 3.13. $C_m(2) \geq 1$ ， $C_m(3) \geq 2$ ， $C_m(4) \geq 4$ 。

在研究 $C_m(n)$ 方面，一般相信以下的猜測是對的，只是要如何證明它就不是一件容易的事了。

猜測 3.14. 當 n 是偶數時， $C_m(n) \geq \frac{n^2}{4}$ ，而當 n 是奇數時， $C_m(n) \geq \frac{n^2-1}{4}$ 。

值得注意的是，我們也可以找到填了很多個位置的臨界集，也就

是說比 $C_m(n) \geq \frac{n^2}{4}$ 大很多。例如圖 3.4，我們可以找到填 9 個位置的 6 階臨界集，也可以找到填 15 個位置的 6 階臨界集。

0	1	2			
1	2				
2					
					3
				3	4

0	1	2	3	4	
1	2	3	4		
2	3	4			
3	4				
4					

圖 3.4

定義 3.15. $Spec_C(n) = \{ x \mid \text{填了 } x \text{ 個位置的 } n \text{ 階臨界集存在} \}$ 。

由上面例子，我們知道 $9 \in Spec_C(6)$ 而且 $15 \in Spec_C(6)$ ，其他還有嗎？研究 $Spec_C(n)$ 這個集合目前才在起步階段，所知道的結果不多，不過首要的工作應該是先決定 $C_M(n)$ 及 $C_m(n)$ ，而這兩個量分別都被相信是非常困難求出來的量；不過，對於有預定對象的拉丁方陣，譬如，要求所填滿的拉丁方陣具有循環性（Circulant L.S.），則上述圖 3.4 的結果已經是最好的了。

另一方面，由於臨界集在暗碼理論中可以獲得適切的應用，所以好的結果也會在應用領域有莫大的貢獻。

作業

1. 試求 $\text{Spec}_C(4)$ 及 $\text{Spec}_C(5)$ 。
2. 估計 $C_M(n)$ 。
3. 令 C 為 n 階拉丁方陣 $A \times B$ 的臨界集，其中 A 是 2 階拉丁方陣，試證 $|C| \geq n^2/4$ 。
4. 試證填了 7 個位置的 10 階拉丁方陣一定可以填滿成爲一個 10 階拉丁方陣。(不用 Andersen 定理)
5. 試證任何 n 階部份拉丁方陣均可以嵌入於一個 $m(\geq 2n)$ 階拉丁方陣中。

4. 垂直拉丁方陣

研究垂直拉丁方陣（Orthogonal L.S.）不但是研究組合設計的重心，在歷史上的記載，它是最早被提出來研究的問題；而且，它也是近代設計理論向前邁進的最大動力之一；由於要證明尤拉在垂直拉丁方陣上的猜測是錯誤的，組合數學家不斷地尋找比較好的方法來建構更多的互相垂直之拉丁方陣，以下以 MOLS（Mutually Orthogonal Latin Squares）簡稱之，同時，我們用 MOLS(n)表示彼此互相垂直的 n 階拉丁方陣。

定義 4.1. 令 $L = [l_{i,j}]$ 及 $M = [m_{i,j}]$ 為兩個 n 階拉丁方陣；如果 $\{ (l_{i,j}, m_{i,j}) \mid 1 \leq i, j \leq n \} = Z_n \times Z_n$ ，則我們稱 L 與 M 垂直，以 $L \perp M$ 表示。如果 $L_1, L_2, \dots, L_t$ 等 t 個 n 階拉丁方陣彼此兩兩互相垂直，則 $\{ L_1, L_2, \dots, L_t \}$ 稱為是一個彼此互相垂直的 n 階拉丁方陣族（A Collection of MOLS(n)）。

以下分別是 $n = 3$ 及 $n = 4$ 的例子，如圖 4.1。

1	2	0
2	0	1
0	1	2

1	2	0
0	1	2
2	0	1

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

0	1	2	3
3	2	1	0
1	0	3	2
2	3	0	1

圖 4.1

『互相垂直的 n 階拉丁方陣究竟會有多少個？』一直是研究組合設計的中心話題，我們先介紹幾個基本性質。

定義 4.2. 令 α 為 Z_n 的一個排列， $L = [l_{i,j}]$ 為一個 n 階拉丁方陣，我們定義 $\alpha(L) = L_\alpha = [\alpha(l_{i,j})]$ 。

兩指法則(Two Fingers' Rule) 令 $L = [l_{i,j}]$ 與 $M = [m_{i,j}]$ 為兩個 n 階拉丁方陣，則 $L \perp M$ 的充要條件為對於任意的兩個位置 (i, j) 與 (i', j') ，若是 $l_{i,j} = l_{i',j'}$ ，則 $m_{i,j} \neq m_{i',j'}$ 。

這個性質可以由定義直接證明，在此省略。

引理 4.3. 令 α, β 為 Z_n 的兩個排列，而且 n 階拉丁方陣 $L \perp M$ ，則

$$L_\alpha \perp M_\beta。$$

證明： 兩指法則。 ■

定義 4.4. 我們稱一個 n 階拉丁方陣 $L = [l_{i,j}]$ 為標準型 (Standard Form)，如果下列條件成立： $l_{1,j} = j-1, j = 1, 2, \dots, n$ ，若是 $l_{i,1} = i-1, i = 1, 2, \dots, n$ 也成立，則此拉丁方陣為雙標準型拉丁方陣。

有了標準型的概念，我們不難證明下面的定理。

定理 4.5. 令 $L_1, L_2, \dots, L_t$ 為 t 個彼此互相垂直的 n 階拉丁方陣，則 $t \leq n-1$ 。

證明： 由於元素的排列變換不會改變兩個拉丁方陣的垂直性，所以我們可以假設 $L_1, L_2, \dots, L_t$ 為 t 個具有標準型式的 $\text{MOLS}(n)$ ，現在，

考慮第二列的第一個位置，顯然 $L_1(2,1), L_2(2,1), \dots, L_t(2,1)$ 必須是全部不一樣的元素，加上 $L_i(2,1) \neq 0, i = 1, 2, \dots, t$ ，所以 $t \leq n-1$ 。 ■

定義 4.6. 若是 $L_1, L_2, \dots, L_{n-1}$ 為 $n-1$ 個 $\text{MOLS}(n)$ ，則 $\{L_1, L_2, \dots, L_{n-1}\}$ 稱為是一個互相垂直拉丁方陣的完全族 (A complete family of $\text{MOLS}(n)$)。

到目前為止，所有知道的完全族都被下面的定理所涵蓋。

定理 4.7. 令 n 為一質數的次方，則 $\text{MOLS}(n)$ 的完全族存在。

證明： 令 $\langle F, +, \cdot \rangle$ 為一個具有 n 個元素的有限體，同時 $L^{(t)}$ 為一 n 階陣列，其中 $L^{(t)}(i, j) = i \cdot t + j, t = 1, 2, \dots, n-1$ ，於是我們很容易地證明 $L^{(1)}, L^{(2)}, \dots, L^{(n-1)}$ 為 $n-1$ 個彼此互相垂直的拉丁方陣 (作業)。 ■

這個定理提供了很多的 $\text{MOLS}(n)$ ，然而，若是 n 不為質數次方時，我們能否也可以建構出完全族呢？顯然，第一個進入眼簾的是 $n = 6$ ，不要說是 $\text{MOLS}(n)$ 的完全族，是否有兩個互相垂直的 6 階拉丁方陣，都曾經絞盡不少組合數學家的腦汁哩！

尤拉顯然早就意識到互相垂直的 6 階拉丁方陣不容易找到，所以他猜測當 $n \equiv 2 \pmod{4}$ 時， $\text{MOLS}(n)$ 並不存在；當然這還需要加上下述的理由。

定理 4.8. 令 $A_1 \perp A_2$ 且 $B_1 \perp B_2$ ，則 $A_1 \times B_1 \perp A_2 \times B_2$ 。

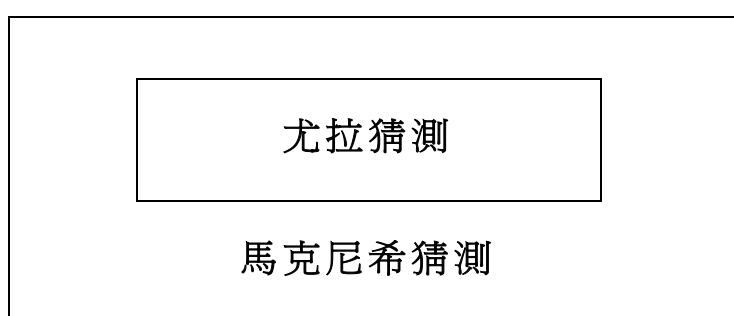
證明： 由兩指法則不難可以證明這個結果 (作業)。 ■

推論 4.9. 令 $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ ，其中 $p_1, p_2, \dots, p_t$ 為相異質數，而且 $r_i \geq$

1，則彼此互相垂直的 n 階拉丁方陣數 $M(n) \geq \min_{1 \leq i \leq t} \{p_i^{t_i} - 1\}$ 。

尤拉猜測 (Euler Conjecture) 對於所有的 $n \equiv 2 \pmod{4}$ ，不存在有兩個互相垂直的 n 階拉丁方陣。

馬克尼希猜測 (MacNeish Conjecture) 推論 4.9 中的不等式是等式。



馬克尼希猜測顯然是比尤拉猜測要求更多，然而，由於尤拉猜測的不正確性也宣告了馬克尼希猜測是錯誤的。

首先，我們先說說尤拉猜測正確的部分。當 $n = 2$ ，的確找不到互相垂直的 2 階拉丁方陣，而 $n = 6$ 時，證明找不到互相垂直的 6 階拉丁方陣則不一樣了。首先，在 1900 年左右 Tarry 花了九牛二虎之力，將所有的 6 階拉丁方陣在分類（排列）之後兩兩加以比較而宣稱下列結果。

定理 4.10. 不存在有任何的 MOLS (6)。

在半信半疑的情況下，大家接受了這個事實；然而，直到 1984 年，Doug Stinson 終於找到了一個簡短的證明，這篇論文發表在 JCT(A) 中，結束了人們的疑慮。至於尤拉猜測錯誤的部分，則是更精彩，除了 10 階拉丁方陣外，需要更好的組合設計來協助，這一個部分留待

第三章再介紹。以下是互相垂直的兩個 10 階拉丁方陣，E.T.Park與 Bose及 Shrikhande在 1959 年分別宣稱推翻了尤拉猜測，然而 Bose及 Shrikhande兩人的工作似乎獲得較明確的肯定，這應該歸功於他們完整的工作，也就是對於所有的 $n \equiv 2 \pmod{4}$ ， $n \geq 10$ ，都能建構 2 個 $\text{MOLS}(n)$ ，而不是只有 10 階拉丁方陣。

4	0	9	8	3	2	7	5	6	1
2	3	7	5	4	0	9	8	1	6
8	1	6	9	0	4	5	3	2	7
9	8	1	4	5	6	3	2	7	0
0	9	8	6	1	3	2	7	4	5
7	2	3	1	6	5	4	0	9	8
5	4	0	3	2	7	6	1	8	9
6	5	4	2	7	1	8	9	0	3
1	6	5	7	8	9	0	4	3	2
3	7	2	0	9	8	1	6	5	4

5	4	0	1	2	7	8	9	3	6
3	1	6	4	8	5	9	2	0	7
0	9	8	7	3	6	1	4	5	2
2	5	4	3	6	1	7	8	9	0
9	8	7	6	1	0	4	5	2	3
1	6	3	5	9	2	0	7	4	8
8	7	2	9	0	4	5	3	6	1
4	0	9	2	7	8	3	6	1	5
7	2	5	0	4	3	6	1	8	9
6	3	1	8	5	9	2	0	7	4

兩個互相垂直的 10 階拉丁方陣

定理 4.11. 對於所有的 n ，除了 1,2,6 之外， $M(n) \geq 2$ 。

證明： $n \equiv 2 \pmod{4}$ 留在第三章證明。 ■

垂直拉丁方陣需要利用組合設計來協助建構，而反過來，我們也可以利用它來建構組合設計，參考第二章。另一方面，在實驗設計上，它也扮演非常重要的角色。

定義 4.12. (正交表或垂直陣列 Orthogonal Array) 一個深度 (Depth) 為 k ，秩為 n 的正交表 $\text{OA}(k, n)$ 是一個 $k \times n^2$ 的陣列， $A=[a_{i,j}]$ ，

陣列中的元素來自 Z_n ，而且滿足任兩列的垂直有序對所成的集合恰為 $Z_n \times Z_n$ 。

以下是一個 $OA(4,3)$ 的例子。

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

由定義，如果我們令每一行代表一個向量，則由 $OA(k,n)$ 所定義出來的 n^2 個向量，彼此之間最多只有一個位置可能一樣，這樣的現象也適合應用於編碼理論。另外，下述的對應也是非常重要的。

定理 4.13. 一個 $OA(k,n)$ 與 $k-2$ 個互相垂直的 n 階拉丁方陣的存在性是等價的。

證明：可以直接由定義推得（作業）。 ■

一般而言，垂直陣列有一個更寬鬆的定義方式。

定義 4.14.（部分垂直陣列） 一個 $k \times m$ 的陣列 $B = [b_{i,j}]_{k \times m}$ 稱為是一個深度為 k 的部分 n 維垂直陣列 $POA(k,n)$ ，如果滿足下列的條件：

(1) $b_{i,j} \in Z_n$ 。

(2) 對於任意的 $1 \leq i_1 \neq i_2 \leq k$ 及 $1 \leq j_1 \neq j_2 \leq m$ ， $(b_{i_1, j_1}, b_{i_2, j_1}) \neq (b_{i_1, j_2}, b_{i_2, j_2})$ 。

由定義可以看出來 $m \leq n^2$ (?)，但是 k 卻有可能比 $n + 1$ 大 (?)。

除了垂直陣列外，我們也可以利用垂直拉丁方陣圖來增加對垂直拉丁方陣的瞭解。

定理 4.15. (垂直拉丁方陣圖, Orthogonal Latin Square Graph, OLSG)

一個 n 階拉丁方陣圖 (V, E) 是以一些 n 階拉丁方陣所成的集合 V 為點集合，而兩點相鄰的充要條件為對應的兩個拉丁方陣互相垂直。

究竟哪一個圖可以轉換成 OLSG 是在這方面研究的主要內容。例如完全兩部分圖即可能實現，見下圖 4.2，當然要每一部份的點數不太多。一旦點數多了，就需要階數較大的拉丁方陣才可以辦到。

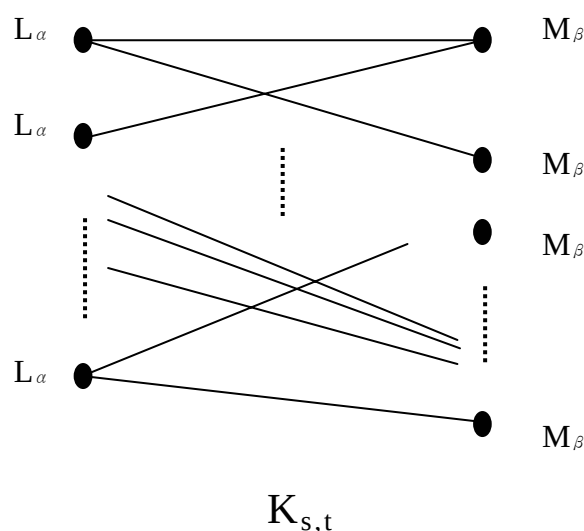


圖 4.2

定義 4.16. $Spec(G) = \{ n \mid \text{用 } n \text{ 階拉丁方陣可以建構出與 } G \text{ 同構的垂直拉丁方陣圖} \}$ 。

例： $G = P_3$ ，則 $Spec(G) = N \setminus \{1, 2, 6\} = N'$ 。

$G = C_4$ ，則 $Spec(G) = N'$ 。

由於下面的定理，我們可以確信任何圖都可以是 OLSG，只要 n 夠大即可。

定理 4.17.[Lindner et. al.] 任一個圖 G ，一定存在一個正整數 n_0 ，使得對於所有的 $n \geq n_0$ ， $n \in \text{Spec}(G)$ 。

上述定理的證明在此省略；如何找到較小的 n_0 是一個有趣，但不太容易的問題。例如：當 $G = P_4$ 時，最小的 n_0 是多少呢？爲了進一步瞭解 $\text{Spec}(P_4)$ ，下面的定理是有幫助的。

定理 4.18.[Heinrich and Zhu] 令 A_1 與 A_2 爲互相垂直的 n 階拉丁方陣，則只要 $m \geq 3n$ ， A_1 與 A_2 可以分別嵌入於兩個互相垂直的拉丁方陣 B_1 與 B_2 。

利用定理 4.18.，我們不難求出下面問題的結果。

命題 4.19. 對於所有的 $n \geq 12$ ， $n \in \text{Spec}(P_4)$ 。

證明：由定理 4.18，我們可以將兩個互相垂直的 4 階拉丁方陣 L_1 與 L_2 嵌入於兩個互相垂直的 n 階拉丁方陣 M_1 與 M_2 ，其中 $n \geq 2$ ，而且 L_1 與 L_2 爲一垂直 4 階拉丁方陣的完全族中的兩個，也就是說，另外存在有一個 4 階拉丁方陣 L_3 ， $L_3 \perp L_1$ 且 $L_3 \perp L_2$ ，由圖 4.3，我們可以看出來 $n \in \text{Spec}(P_4)$ 。 ■

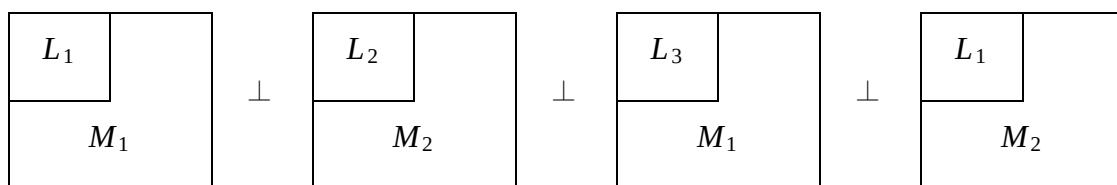


圖 4.3

垂直拉丁方陣尚有很多可以探討的性質，我們將在第三章再繼續介紹。

作業

1. 試證明當 n 為質數次方時， $M(n) = n-1$ 。
2. 試證明當 $M(n) \geq n-2$ 時， $M(n) = n-1$ 。
3. 試證若存在有一個 $OA(k,n)$ ，則必存在 $k-2$ 個 $MOLS(n)$ 。
4. 試求 $\min Spec(P_4)$ 。
- (*) 5. 令 L 與 M 為任意兩個 n 階拉丁方陣。定義 $L \wedge M$ 為集合
$$\{(l_{i,j}, m_{i,j}) \mid 1 \leq i, j \leq n\}$$
，我們稱 L 與 M 為 r -垂直若且唯若 $|L \wedge M| = r$ ，試求所有可能的 r 。
6. 試求 $\max\{|L \wedge M| \mid L, M \text{ 為 } 6 \text{ 階拉丁方陣}\}$ 。
- (*) 7. 試求 $Spec(P_5)$ 。
- (***) 8. 任給一個拉丁方陣 L ，若已知它和某一個拉丁方陣 M 互相垂直，試由 L 求出一個與 L 垂直的拉丁方陣。
9. 對於任一個數 $m=4k+2$ ， $k \geq 1$ ，試求出一個 m 階拉丁方陣 L ，它不會和其他的 m 階拉丁方陣垂直。
10. 令 L 與 M 為兩個互相垂直的拉丁方陣， L' 為由 L 交換第一列與第二列所得到的拉丁方陣。試證 L' 與 M 不互相垂直。

5. 全截集 (Transversal)

首先，我們假設有一個 $n \times n$ - 方格的田地，上面依拉丁方陣的架構，分別種植 n 種不同的植物各 n 株，如果它們彼此之間在同行或同列都有可能互相影響，試問，我們可不可能在這田地上選出 n 株品種不同而且不互相干擾的植物呢？換句話說，把這些實驗轉換成拉丁方陣之後，我們在尋找 n 個位置，不同行也不同列，它們填入的元素都不一樣。顯然，若是按等冪拉丁方陣的方式來種植，對角線上的位置恰好滿足我們所需要的性質。然而，就一般拉丁方陣而言，它的存在性是值得研究的問題。

定義 5.1. (全截集) 一個 n 階拉丁方陣中， n 個不同行不同列的位置，若是填入的元素也都不相同，則這 n 個位置稱為是此拉丁方陣的**全截集**。

為了方便解釋，我們用**截集**來代表 n 階方陣中的 n 個位置，它們兩兩都不在同一列上，也不在同一行上。這時候如果填入的元素都不一樣，按上述定義即為此拉丁方陣的一個全截集，不然我們稱之為部分截集或簡稱截集。

令 T 代表 n 階拉丁方陣 L 的一個截集，則我們以 $|T|$ 代表在此截集中不同元素的個數，於是 $|T| \leq n$ ，而等號成立時， T 為一個全截集。一個拉丁方陣一定會有一個全截集嗎？

命題 5.2. 令 L 為一個具有垂直對 (Orthogonal Mate) 的拉丁方陣，也就是存在有一 M ，使得 $L \perp M$ ，則 L 具有互斥的 n 個全截集。

命題 5.3. 令 A 與 B 分別為奇數階及 2 階拉丁方陣，則 $A \times B$ 不含任何的全截集。

證明： 我們可以把 $A \times B$ 看成是含有四個與 A 階數一樣的拉丁子方陣。如圖 5.1，則證明就很容易完成。(作業) ■

$0 \sim m-1$	$m \sim 2m-1$
$m \sim 2m-1$	$0 \sim m-1$

$2m \times 2m$

圖 5.1 $A \times B$

爲了研究截集 T 的大小，亦即 $|T|$ ，我們可以採用邊著色的概念來協助。

定義 5.4. (邊著色) 一個圖 G 的邊著色是一個由 $E(G)$ 映至 $\{1, 2, \dots\}$ 的函數 φ ，它滿足如果 $uv \in E(G)$ ，則 $\varphi(u) \neq \varphi(v)$ 。

所以， $|\varphi(E(G))|$ 爲該邊著色所使用的顏色數，我們令所需要的最少顏色數爲圖 G 的邊著色數，以 $\chi'(G)$ 表示。由定義，我們立刻得到以下的結論： $\chi'(G) \geq \Delta(G)$ 。至於 $\chi'(G)$ 的上界，Vizing 提供了最好的答案。

定理 5.5. (Vizing) 當 G 爲簡單圖時， $\chi'(G) \leq \Delta(G) + 1$ 。

定理 5.6. (Vizing) 如果 G 是重邊圖，而重邊度 (Multiplicity) 爲 μ ，則 $\chi'(G) \leq \Delta(G) + \mu$ 。

這兩個定理都是圖論的基本定理，在此不加以證明，但是我們將利用它來說明截集的大小。首先，我們發現一個 n 階拉丁方陣和 $K_{n,n}$ 的一個邊著色有對應的關係：即令 $l_{i,j}$ 爲邊 $\{i,j\}$ 所塗的顏色。因此，一個拉丁方陣的截集將對應於 $K_{n,n}$ 中的一個完全配對或是一因子 (1-factor)，於是，截集的大小就等於是這個配對上面的不同顏色數了。更清楚地說，一個全截集就對應一個塗上不同顏色的一個完全配對，又稱爲是一個彩虹 (Rainbow)。所以，我們把截集大小的研究轉換成彩虹的尋找，或者要是辦不到，就尋找具有越多顏色的配對越好。下列的定理最早由 Koksma 所獲得 (1968)。我們用拉丁方陣的性質來證明這個結果。下個定理再由圖著色方式證明。

定理 5.7. 令 T 爲一 n 階拉丁方陣的截集，則 $|T| \geq \frac{2}{3}n$ 。

證明： 令 $|T|=t$ ，不失一般性，我們可以假設填入不同數字爲 $0,1,2,3,\dots,t-1$ ，而且它們的位置可以經由換行或換列而出現在對角線上，如圖 5.2 所示。這時候在 D 中所填入的元素必然全部都是在 $\{0,1,2,\dots,t-1\}$ 這個集合中。所以，比 $t-1$ 大的元素出現在 C 中的個數恰爲 $(n-t)^2$ 。現在如果 $t + \sqrt{t} \geq n$ ，則只要 $n \geq 7$ ， $t \geq \frac{2}{3}n$ ，定理得證。(當 $n < 7$ 時可以由拉丁方陣看出來，不再多做核對)。所以，考慮 $t + \sqrt{t} < n$ 。因此 $(n-t)^2 > t$ ，由鴿籠原理， C 的 t 行中，至少有一行 (第 $j+1$ 行) 它含有兩個比 $t-1$ 大的元素 a 與 b 。

於是， j 一定不會出現在 D 中 (?)，所以 j 在 B 中出現 $n-t$ 次，

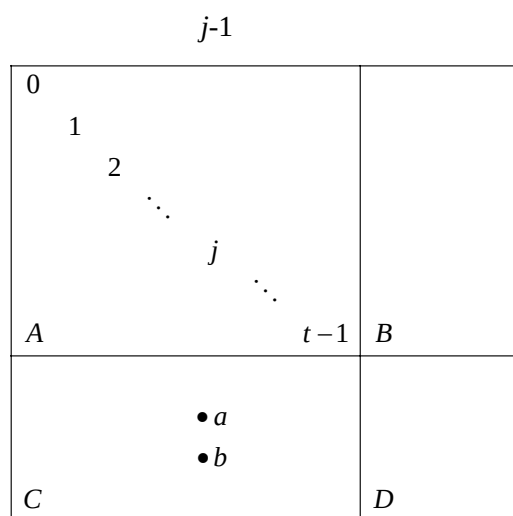


圖 5.2

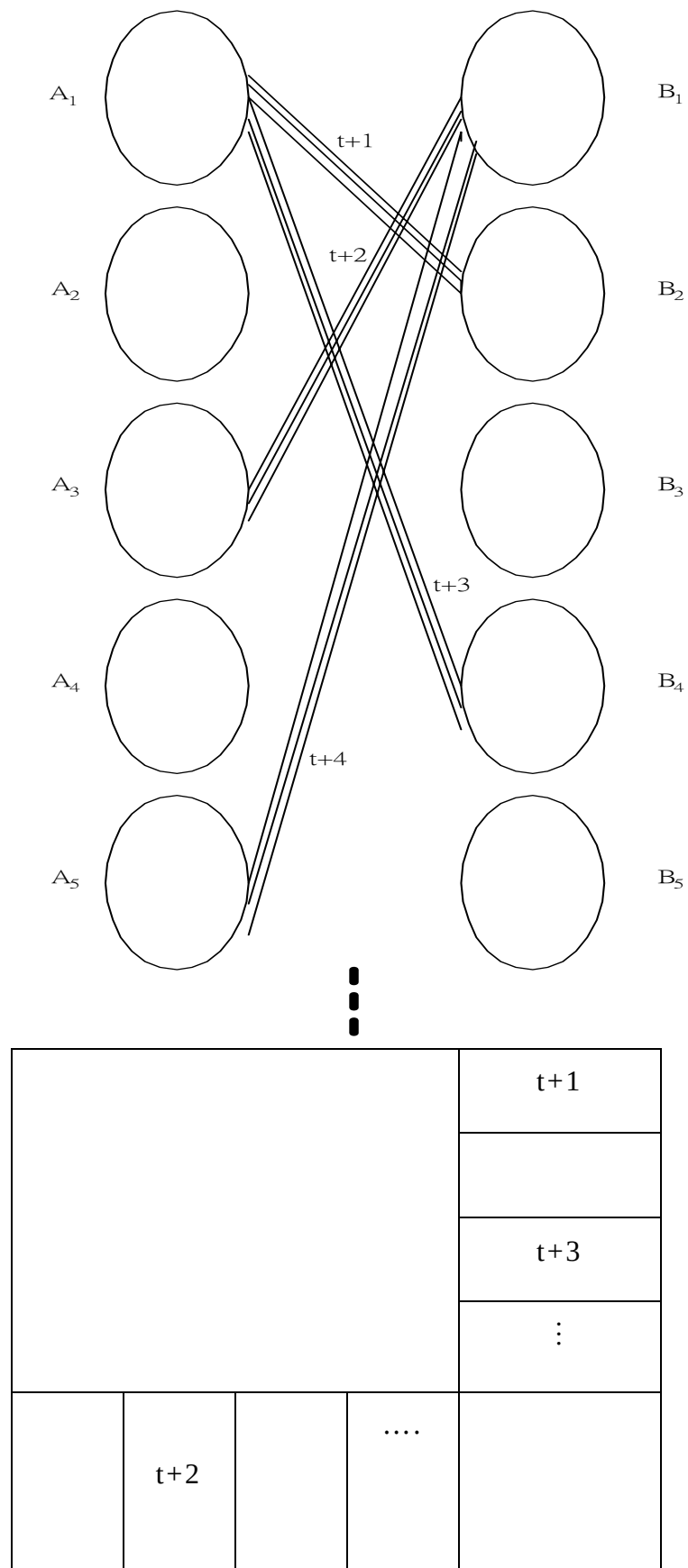


圖 5.3

Koksma 的結果不久分別被 Brouwer 及 Woolbright 改進，不久又被 Shor 改善，而最精確的計算則要歸功於林士強的努力。以下的定理證明是採用 Woolbright 的觀念，在此僅摘要地說明。

定理 5.8. 在一個 n 階拉丁方陣中必存在一個截集 T ， $|T| \geq n - \sqrt{n}$ 。

證明：如圖 5.3 所示，假設由 n 階拉丁方陣所轉換出來的完全二分圖 $K_{n,n}=(A,B)$ ， $A=\{a_1, a_2, \dots, a_n\}$ ， $B=\{b_1, b_2, \dots, b_n\}$ ，而 $K_{n,n}$ 上對應邊著色為 ϕ ，不失一般性我們假設 T 為最大的截集，且 $|T|=t$ ，而 T 所對應的不同顏色邊含 $a_1b_1, a_2b_2, \dots, a_tb_t$ ，顏色為 $1, 2, \dots, t$ 。現在看顏色 $t+1$ ， A_1 中的點，每點都會碰到 $t+1$ 這個顏色（？），所以將不在 B_1 ，而且連到 A_1 中點的那些點放在一起形成一集合 B_2 ， $|B_2| = n-t$ ，再看與 B_2 對應的點， A_2 （ $b_i \in B_2$ 若且唯若 $a_i \in A_2$ ），考慮 $t+2$ 這個顏色在 B_1 集合上的點所碰到的邊；則這些邊連到的集合 A_3 。（？）接著再看碰 A_1 的點，顏色為 $t+3$ ，則連到 B_4 中的點，一直到全部顏色都考慮到，則得到 $(n-t)^2 \leq t$ ， $n-t \leq \sqrt{t}$ ，於是 $|T| \geq n - \sqrt{t} \geq n - \sqrt{n}$ 。

定理 5.9.[Shor] 在一個 n 階拉丁方陣中，必存在一截集 $|T| \geq n - 5.53 (\ln n)^2$ 。

定理 5.10.[Fu and Lin] 在一個 n 階拉丁方陣中，必存在一截集 T ， $|T| \geq n - 5.51 (\ln n)^2$ 。

對於截集的大小，最有名的問題當屬於由 Ryser 所提出的截集猜測。

截集猜測：在 n 階拉丁方陣中，必存在一個截集 T ， $|T| \geq n-1$ ，而當 n 為奇數時，可以找到一個全截集。

到現在為止，定理 5.10 算是最好的結果，要獲得更好的結果勢必有更好的觀念才有希望，讓我們拭目以待。

從完全二分圖尋找彩虹的構想，我們可以找一個存在於完全圖中的彩虹，所不同的是，這雖然是一個證明很長的定理，但是，這個彩虹的確是存在，以下是發展的過程。

定理 5.11.[Woolbright] 對於 K_{2n} 的任何一個 $(2n-1)$ -邊著色，都可以找到一個具有 $n-1$ 個邊的配對，這 $n-1$ 邊的顏色都不相同。

定理 5.12.[Woolbright & Fu] 對於 K_{2n} 的任何一個 $(2n-1)$ -邊著色，都可以找到一個彩虹。

證明：證明的基本概念如下：首先，由定理 5.11，我們可以找到 $n-1$ 個邊 $a_1b_1, a_2b_2, \dots, a_{n-1}b_{n-1}$ ，它們的顏色分別為 $1, 2, \dots, n-1$ ，如圖 5.4(a)，令與此 $n-1$ 邊合成一個完全配對的邊 ab ，而且 ab 的顏色為 1。於是，我們考慮與 a, b 相鄰的邊，而且它們的顏色是 $n+1, \dots, 2n-1$ ，令這些邊所成的集合為 E ，則 $|E| = 2n$ 。由鴿籠原理，我們知道若非有一 a_ib_i 與 E 中的 4 個邊相鄰，就是有 a_ib_i 及 a_jb_j 它們分別與 E 中的 3 個邊相鄰，如圖 5.4(b)，接著就是換色的工作了，詳細可以參考 JCD，6，1998 的論文。 ■

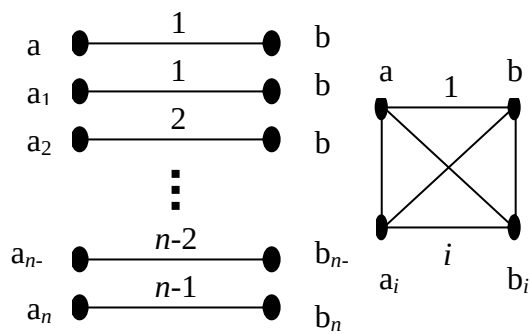


圖 5.4 (a)

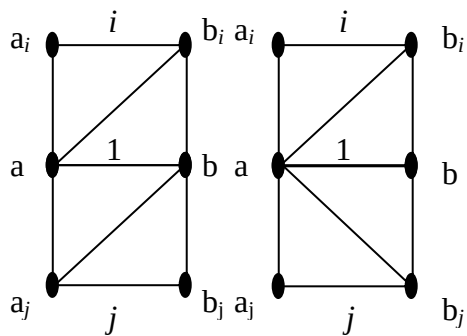


圖 5.4 (b)

這個定理回答了 A. Rosa 的問題，然而一個更一般性的問題卻一直尚未有明確的答案。

問題：對於 K_{2n} 的任何一種正規著色（即邊著色）是否都可以找到一個彩虹？

問題：對於 K_{2n} 的 $(2n-1)$ -邊著色，互斥的彩虹最多有幾個？

作業

1. 證明命題 5.3。
2. 試以簡單的論證，證明 n 階拉丁方陣的截集中一定有一個 T ， $|T| \geq \frac{1}{2}n$ 。
- (*)3. 試證有一個 T ， $|T| \geq \frac{3}{4}n$ 。
- (**)4. 試證 K_{2m+1} 的任一個 $(2m+1)$ -邊著色皆存在有一個配對，它有 m 個邊，而且這 m 個邊的顏色都不同。
- (***)5. 試證若是一個 n 階拉丁方陣有一個全截集 T ，則必定存在另一個與 T 互斥的全截集。
- (***)6. 試找出一個求最大截集的演算法。

6. 特殊的拉丁方陣

在討論特殊的拉丁方陣之前，我們再一次強調同型拉丁方陣的重要性，表面上看過去不一樣的兩個拉丁方陣，往往是同型(Isotopic) 的方陣。例如 4 階的 576 個拉丁方陣，實際上可以分成兩類同型的方陣，如圖 6.1，更不可思議的是 5 階的 161,280 個拉丁方陣也是可以分成兩類（作業）。

1	2	3	④
2	1	④	3
3	④	1	2
④	3	2	1

1	2	3	④
2	3	④	1
3	④	1	2
④	1	2	3

圖 6.1 不同型的 4 階拉丁方陣

由於拉丁方陣的分類，要研究特殊拉丁方陣顯然有些幫助，然而，不同型的拉丁方陣並非如 4 階，5 階一樣都是少數幾個而已，例如當我們考慮 6、7、8 階拉丁方陣時，它們分別有 22，563，及 1,676,257 個，當 $n = 9$ 時，數字也就非常龐大了，這也可以由目前已經算出來 9 階拉丁方陣的個數看出一二；Bammel 及 Rothstein 算出來 9 階拉丁方陣（用電腦）一共有 $19 = 9! * 8! * 377,597,964,258,816$ 個，於是不同的 9 階拉丁方陣至少有 $19 / (9!)^3$ 。由上面資訊，我們不難想像為何利用電腦來尋找出 3 個彼此互相垂直的 10 階拉丁方陣會這麼困難，但是，無論如何，對於低階拉丁方陣的特殊性，同型方陣的確貢獻不少，例如，5 階拉丁方陣的兩型中，一型就是由 Z_5 所產生的循環群。

當然，我們也可以討論所謂的同構方陣，亦即換行，換列，換元

素均採用同一排列，如此一來，不同構的方陣自然可能比不同型的方陣多；因為同構者必同，例如，5 階拉丁方陣就有 6 個同構類，

如圖 6.2。

1	2	3	4	⑤
2	3	4	⑤	1
3	4	⑤	1	2
4	⑤	1	2	3
⑤	1	2	3	4

1	2	3	4	⑤
2	1	4	⑤	3
3	⑤	1	2	4
4	3	⑤	1	2
⑤	4	2	3	1

1	2	3	4	⑤
2	1	⑤	3	4
3	4	2	⑤	1
4	⑤	1	2	3
⑤	3	4	1	2

1	2	3	4	⑤
2	1	4	⑤	3
3	4	⑤	1	2
4	⑤	2	3	1
⑤	3	1	2	4

1	2	3	4	⑤
2	1	4	⑤	3
3	4	⑤	2	1
4	⑤	1	3	2
⑤	3	2	1	4

1	2	3	4	⑤
2	3	4	⑤	1
3	⑤	2	1	4
4	1	⑤	3	2
⑤	4	1	2	3

圖 6.2 不同構的 5 階拉丁方陣

我們特別說明一下，不同構的 6 階拉丁方陣一共有 109 各。

除了同型，同構的分類之外，我們再說明一種”共軛”的概念，它

不像前兩者可以函蓋很多拉丁方陣，但是它也很自然地由一個方陣製造出另外的 5 個方陣，而這 6 個方陣之間維持著很高的相關性。

定義 6.1. 令 $L=[l_{i,j}]$ 為一個 n 階拉丁方陣對應於擬似群

$\langle Z_n, * \rangle$ ，則 L 可以定義成 $\{(x,y;z) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ 。

命題 6.2. 令 $L=\{(x,y;z) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ 為對應於 $\langle Z_n, * \rangle$ 的一個 n 階拉丁方陣，則 $L_{(12)}=\{(y,x;z) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ 亦為一拉丁方陣。同理 $L_{(13)}=\{(z,y;x) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ ， $L_{(23)}=\{(x,z;y) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ ， $L_{(123)}=\{(z,x;y) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ 及 $L_{(132)}=\{(y,z;x) \mid x,y \in Z_n \text{ 且 } x*y=z\}$ 皆為 n 階拉丁方陣。

證明：略。 ■

上述 5 個由 L 轉換而得到的拉丁方陣皆稱為是 L 的共軛 (Conjugate) 拉丁方陣；不過，我們要特別注意的是，很可能是 5 個共軛的拉丁方陣和原拉丁方陣是一樣的拉丁方陣。

命題 6.3. 令 L 為一拉丁方陣，則 L 的所有不同的共軛拉丁方陣個數 (含自己) 為 1，或 2，或 3，或 6。

證明：作業。 ■

由上面的命題，我們不難想像到所有共軛拉丁方陣都一樣的拉丁方陣必定要滿足以下的條件：

若 $x*y=z$ ，則 $x*(x*y)=y$ 且 $(x*y)*y=x$ 。.....(1)

以下的兩個定義在前面已敘述過，在此再一次提出說明。

定義 6.4. 滿足條件 (1) 的拉丁方陣稱為是全對稱 (Totally Symmetric) 拉丁方陣。

定理 6.5. 若拉丁方陣 L 所對應的擬似群 $(Z_n, *)$ 滿足對於所有的 $x, y \in Z_n$, $x*(y*x)=y$, 則 L 為一個半對稱 (Semi-symmetric) 拉丁方陣。

所以，從擬似群出發，只要增加條件就可以定義出很多不同的特殊拉丁方陣。這些著名的恆等式在泛代數 (Universal Algebra) 的研究中有較仔細的分析，下面就列出一些比較知名的式子。

- (1) $\forall a, a^2=a$ (Idempotent , 等冪) 。
- (2) $\forall a, b, a^2=b^2$ (Unipotent , 冪等) 。
- (3) $ab=ba$ (Commutative , 交換律) 。
- (4) $(ab)b=a$ (Sade's right "key" law) 。
- (5) $b(ba)=a$ (Sade's left "key" law) 。
- (6) $a(ba)=b$ (Right Semi-symmetry) 。
- (7) $(ab)a=b$ (Left Semi-symmetry) 。
- (8) $a(ab)=ba$ (Stein's first law) 。
- (9) $a(ba)=(ba)a$ (Stein's second law) 。
- (10) $a(ab)=(ab)b$ (Schröder's first law) 。
- (11) $(ab)(ba)=a$ (Schröder's second law) 。

(12) $(ab)(ba)=b$	(Stein's third law) °
(13) $ab=a$	(Sade's right translation law) °
(14) $ab=b$	(Sade's left translation law) °
(15) $(ab)c=a(bc)$	(Associative law) °
(16) $a(bc)=c(ab)$	(the law of cyclic associativity) °
(17) $a(bc)=c(ba)$	(Abel-Grassmann's law) °
(18) $(ab)(bc)=ac$	(Stein's fourth law) °
(19) $(ab)(ac)=bc$	(Stein's fifth law) °
(20) $(ab)(ac)=cb$	(Schweitzer's law) °
(21) $(ab)(ca)=[a(bc)]a$	(the Bruck-Moufang identity) °
(22) $[(ab)c]b=a[b(cb)]$	(the Moufang identities) °
(23) $[(bc)b]a=b[c(ba)]$	(the Moufang identities) °
(24) $[(ab)c]b=a[(bc)b]$	(Bol identity) °
(25) $[(ab)c]a=a[b(ca)]$	(the extra loop law) °
(26) $a[b(ca)]=cb$	(Tarski's law) °
(27) $a[(bc)(ba)]=c$	(Neumann's law) °
(28) $(ab)(ca)=(ac)(ba)$	(the specialized medial law) °

(29) $(ab)(cd)=(ad)(cb)$ (the first rectangle rule) 。

(30) $(ab)(ac)=(db)(dc)$ (the second rectangle rule) 。

(31) $(ab)(cd)=(ac)(bd)$ (the medial law) 。

除了利用擬似群結構來找特殊的拉丁方陣，另外，我們也可以利用組合性質來發現特殊的方陣。

定義 6.6. 令 $L=[l_{i,j}]$ 為一 n 階拉丁方陣。若是集合 $\{(l_{i,j}, l_{i,j+1}) \mid i \in Z_n, j \in Z_n \setminus \{n-1\}\} = (Z_n \times Z_n) \setminus \{(k,k) \mid k \in Z_n\}$ ，則 L 稱為是一個列完全 (Row-complete) 拉丁方陣。如果 $\{(l_{i,j}, l_{i+1,j}) \mid j \in Z_n, i \in Z_n \setminus \{n-1\}\} = (Z_n \times Z_n) \setminus \{(k,k) \mid k \in Z_n\}$ ，則 L 為一行完全 (Column-complete) 拉丁方陣。同時為列完全及行完全拉丁方陣的 L 稱為是完全拉丁方陣。

這樣的拉丁方陣拿來做實驗時也可以兼顧到相鄰兩種”作物”亦可以獲得適當的比較，以增加此實驗設計的正確性。下面的定理，一口氣舉出非常多的完全拉丁方陣，而它的基本概念來自於差集 (Difference set) 。

定理 6.7. 令 $n=2m$ ，則以 $(0, 1, 2m-1, 2, 2m-2, 3, \dots, m+1, m)$ 為第一列，而第 i 列 ($i=2, 3, \dots, n$) 為由第一列的每個元素加上第一列的第 i 個元素 (mod n) 所獲得；如此所得到的方陣為一完全拉丁方陣。

證明：可以由左右兩個元素的差看出來它是列完全拉丁方陣，再加上對稱的現象，所以定理證。 ■

如果是奇數階，要製造完全拉丁方陣就沒有這麼容易了。

問題：奇數階的完全拉丁方陣存在嗎？

作業

1. 試證圖 6.2 的 5 階拉丁方陣，除了第一個之外，其它的 5 個為同型的拉丁方陣。
2. 證明命題 6.3。
3. 試證全對稱拉丁方陣對於任何階數皆存在。
- (*)4. 試證一個 n 階等幂全對稱拉丁方陣存在的充要條件為 $n \equiv 1$ 或 $3 \pmod{6}$ 。
5. 舉例說明滿足 Schweitzer's law 的拉丁方陣（階數至少為 3）。
6. 舉例說明一個列完全拉丁方陣不一定是完全拉丁方陣。

7. 魔方陣 (Magic Square)

魔方陣的存在恐怕已有數千年了，由於它曾經被用來卜卦用，而且也在武俠小說中被形容成是一種非常高深而且神秘的數術，所以幾乎所有對數字有趣味的人都曾嘗試著去想想如何建構這令人著迷的方陣。在這一節中，我們主要是想介紹互相垂直的拉丁方陣可以用來建構這類的方陣。

定義 7.1. 一個 n 階魔方陣是一個 $n \times n$ 的陣列 $M=[m_{i,j}]$ ，同時滿足

(i) $\{ m_{i,j} \mid 1 \leq i, j \leq n \} = \{1, 2, \dots, n^2\}$ 及

$$(ii) \sum_{i=1}^n m_{i,j} (j=1, 2, \dots, n) = \sum_{j=1}^n m_{i,j} (i=1, 2, \dots, n) = \sum_{k=1}^n m_{k,k} = \sum_{k=1}^n m_{k,n-k+1}。$$

簡單地說，一個魔方陣的行和，列和，主對角線和及副對角線和都相等，於是這個和 $S_n = (\sum_{i=1}^{n^2} i)/n$ 。以下是 $n = 3, 4, 6$ 的例子。(圖 7.1)

4	3	8
9	5	1
2	7	6

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

35	1	6	26	19	24
3	32	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	5	24	12	14	16
4	36	29	13	18	11

圖 7.1. 魔方陣 ($n = 3, 4, 6$)

在討論魔方陣的建構之前，我們先看看一類要求較少的的**鬼方陣**，在這方陣中，仍然用 $1, 2, \dots, n^2$ 來填成 $n \times n$ 的陣列，不過，我們只要求行和和列和要全部相等。

引理 7.2. 如果存在兩個互相垂直的 n 階拉丁方陣，則 n 階鬼方陣存在。

證明：令 $L \perp M$ ， $L=[l_{i,j}]$ 及 $M=[m_{i,j}]$ ，現在我們建構鬼方陣 $G=[g_{i,j}]$ ，其中 $g_{i,j}=1+l_{i,j}+n*m_{i,j}$ 。由於 $l_{i,j}$ ， $m_{i,j} \in Z_n$ ，而且 $L \perp M$ ，所以 $\{g_{i,j} \mid 1 \leq i, j \leq n\} = \{1, 2, \dots, n^2\}$ ，而且行和和列和皆為 $n + \binom{n-1}{2} + n \binom{n-1}{2} = \frac{\sum_{i=1}^{n^2} i}{n}$ 。

■

我們不能保證對角線和的理由，顯然和 L 與 M 的選擇有關，為了能像引理 7.2 的形式，我們需要考慮比較特殊的拉丁方陣。

定義 7.3. 一個對角（Diagonal）拉丁方陣 $L=[l_{i,j}]$ 是一種特殊的拉丁方陣，它的主對角線及副對角線上的 n 個元素分別都不相同，也就是說 $\{l_{i,i} \mid i=1, 2, \dots, n\} = Z_n = \{l_{i, n-i+1} \mid i=1, 2, \dots, n\}$ 。

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

圖 7.2. 4 階對角拉丁方陣

我們不難發現 3 階對角拉丁方陣是不存在的，而一般的階數又如何呢？的確，對於 $n \geq 4$ ，對角拉丁方陣都存在，然而，要建構這些拉丁方陣是要花不小的力氣。在這裡就以 2 個比較特殊的情況加以說明。

引理 7.4. 對於所有不為 3 的倍數之奇數 n ，都存在一個 n 階對角拉丁方陣。

證明：令 $\alpha, \beta, \alpha + \beta, \alpha - \beta \pmod{n}$ （其中 $\alpha > \beta$ ）為 4 個與 n 互質的數，同時 $L = [l_{i,j}]$ ，為一個 n 階拉丁方陣，其 $l_{i,j} = (i-1)\beta + (j-1)\alpha$ 。則 L 為一對角拉丁方陣（？）。現在，由於 n 不為 3 的倍數且為奇數，所以令 $\alpha = 2, \beta = 1$ ，引理得證。 ■

引理 7.5. 假設 $n = 2^k$ ， $k \geq 2$ ，則存在一個 n 階對角拉丁方陣。

證明：首先當 $k=2$ 及 $k=3$ 時，4 階及 8 階對角拉丁方陣存在，如圖 7.3，再利用遞迴建構法，即可證明此引理（ $2^k = 2^{k_1} 2^{k_2} = n_1 * n_2$ ）。令 A 為 n_1 階對角拉丁方陣，而 $B_0, B_1, \dots, B_{n_1-1}$ 為同構的 n_2 階對角拉丁方陣，而且 B_i 為基於集合 $\{in_2, in_2+1, \dots, in_2+n_1-1\}$ ， $i=0, 1, 2, \dots, n_1-1$ 的方陣。於是，用 B_i 取代 A 中的 i ，我們得到一個 $n_1 n_2$ 階對角拉丁方陣（？）。

1	2	3	4	5	6	7	0
2	3	5	6	7	0	4	1
0	6	4	1	2	5	3	7
6	7	0	5	3	2	1	4
4	0	7	2	6	1	5	3
3	4	6	0	1	7	2	5
5	1	2	7	4	3	0	6
7	5	1	3	0	4	6	2

圖 7.3. 8 階對角拉丁方陣

顯然，我們需要更大的努力才能完成所有可能的對角拉丁方陣，在這裡我們只敘述最後的成果。

定理 7.6. 對於所有的 $n \geq 4$ ，皆存在有 n 階對角拉丁方陣。

可是只有一個 n 階對角拉丁方陣對於魔方陣的建構並沒有多大的用途；從觀察，我們可以看出來，兩個互相垂直的拉丁方陣就可以用來建構魔方陣。

定理 7.7. 若存在兩個 n 階互相垂直的對角拉丁方陣，則必存在一個 n 階魔方陣。

證明：和引理 7.4 相似。 ■

很幸運的是上述的拉丁方陣是存在的，這也間接證明了任意 n 階魔方陣皆存在。

定理 7.8. (Du, et.al.) 除了 2，3，6 之外，皆存在有兩個互相垂直的 n 階對角拉丁方陣。

除了上述基本的魔方陣，具有特殊性質的魔方陣也是研究學者的最愛。

定義 7.9. (泛對角的魔方陣，Pandiagonal) 一個魔方陣 $M =$

$[m_{i,j}]$ ，如果對於所有的 $j=0,1,2,\dots,n-2$ ， $\sum_{i=1}^n m_{i,(n-i)+j+1} = \sum_{i=1}^n m_{(n-i)+j+1,i} = \sum_{i=1}^n m_{i,i}$ ，則 M 又稱為是泛對角的魔方陣。

10	5	49	37	32	27	15
41	29	24	19	14	2	46
16	11	6	43	38	33	28
47	42	30	25	20	8	3
22	17	12	7	44	39	34
4	48	36	31	26	21	9
25	23	18	13	1	45	40

圖 7.4. 7 階泛對角的魔方陣

泛對角魔方陣的研究也有一些好的成果，但是有些階數是不存在的，以下是綜合的結果，至於如何建構可以參考林志杰同學（淡江）的碩士論文，他不但對已知的結果給予一個證明，更計算出他那一類型泛對角魔方陣的個數。

定理 7.10. n 階泛對角魔方陣存在的充要條件為 $n \geq 4$ 且 $n \not\equiv 2 \pmod{4}$ 。

證明：必要條件（作業）。

充分條件（省略）。



最後，我們補充說明，魔方陣可以用來建構特殊碼（Code），它具有相當好的性質。

作業

1. 建構一個 5 階魔方陣，同時它是泛對角的魔方陣。
2. 證明引理 7.4。
3. 證明引理 7.5。
4. 證明對於所有的 $n \equiv 2 \pmod{4}$ ， n 階泛對角魔方陣不存在。
- (*)5. 可否由一個 n 階的魔方陣，($n \neq 2, 6$)，求得兩個互相垂直的 n 階拉丁方陣，請解釋理由。

8. Room 方陣

這是一種和拉丁方陣相似的方陣，在近代設計理論的發展中是非常重要的。最早提出這個概念的是 T.G.Room，他在 1955 年左右說它是一種新型的魔方陣，其實它與魔方陣相去甚遠，以下的定義可以讓你有更多的瞭解。

定義 8.1. 一個 $2n$ 階的 Room 方陣是一個具有 $2n$ 個元素的 $(2n-1) \times (2n-1)$ 陣列，每個位置可以選擇填或不填；填入元素的位置每次填入兩個元素，填好之後， $2n$ 個元素中的任兩個恰好出現一次，而且每一行，每一列，每一個元素都恰好出現一次。

以下是兩個 8 階的 Room 方陣。

01			62		57	34
45	02			73		61
72	56	03			14	
	13	67	04			25
36		24	71	05		
	47		35	12	06	
		15		46	23	07

(a)

01	56	24		37		
	02	67	35		41	
		03	71	46		52
63			04	12	57	
	74			05	23	61
72		15			06	34
45	13		26			07

(b)

圖 8.1

從 $n = 4$ 開始舉例子，最主要的原因是當 $n = 2$ 及 $n = 3$ 的時候， $2n$ 階 Room 方陣並不存在（？）。而且值得一提的是圖 8.1 的兩個例子都是循環的例子，同時，我們不難發現，不論是從行看或列看都是 K_8 的 1-分解，所以下列的性質並不令人驚奇。

定理 8.2. 一個 $2n$ 階的 Room 方陣等價於存在兩個等冪對稱的 $2n-1$ 階拉丁方陣 L_r 及 L_c ，它們同時滿足下列兩個條件：

(i) 如果 $L_r(x,y)=L_c(x,y)=\alpha$ ，則 $x=y=\alpha$ 。

(ii) 若 $a \neq b$ ，則最多只有一個有序對 (x,y) 使得 $L_r(x,y)=a$ 且 $L_c(x,y)=b$ 。

證明：首先，如果一個 $2n$ 階的 Room 方陣存在，則可以換行及換列，使得在對角線的位置分別依次為 $0,1;0,2;\dots;0,2n-1$ 。現在，定義當 (x,y) 出現在第 a 列及第 b 行， $a \neq b$ ，令 $L_r(x,y)=a$ 以及 $L_c(x,y)=b$ 。接著，再令 $L_r(x,x)=L_c(x,x)=x$ ，則 L_r 及 L_c 為所求；反過來，有 L_r 及 L_c 亦可證明 Room 方陣存在，這裡需要 (i),(ii) 兩個條件來保證其存在性。■

上述定理所提到的兩個拉丁方陣，也被稱為是 Room 配對 (Pair)，對於 Room 方陣的建構有很大的幫助。

定理 8.3. 若是 $2m$ 階及 $2n$ 階的 Room 方陣存在，則 $(2m-1)(2n-1)+1$ 階的 Room 方陣亦存在。

證明：這裡主要是利用垂直拉丁方陣的乘積亦垂直的性質，細節省略。■

有關 Room 方陣的研究，經過了多年的努力，最後終於由 W.Wallis 綜合前人的努力及自己的成果證明了以下非常出名的結果。

定理 8.4. 除了 $n = 2$ 及 3 之外，任意的 $2n$ 階 Room 方陣皆存在。

為了建構特殊的設計，如圈系 (Cycle System)，我們需要一些特殊結構的 Room 方陣。

定義 8.5. (Skew Room Square) 一個 Room 方陣 R ，如果對於所有的 $1 \leq i < j \leq 2n-1$ ， $R(i, j)$ 與 $R(j, i)$ 恰有一個位置不是空的，而且 $R(i, i)$ 不是空的，則 R 稱為是一個階數為 $2n$ 的 Skew Room 方陣。

圖 8.1(a),(b) 為這樣的例子。為了達到特殊建構的目的，我們也可以研究特殊形狀 (Frame) 的 Room 方陣。

定義 8.6. ($2n$ 階 $\{S_1, S_2, \dots, S_t\}$ -Room 方陣 R)

R 滿足下列條件：

(1) $S_1 \cup S_2 \cup \dots \cup S_t = \{1, 2, \dots, 2n-1\}$ 。

(2) $R(i, j)$ 為空的若且唯若 $(i, j) \in S_k \times S_k$ ， $k=1, 2, \dots, t$ 。

(3) R 為一個 $2n$ 階的 Room 方陣。

為了方便起見， $\{S_1, S_2, \dots, S_t\}$ -Room 方陣的形式以 $\prod_{k=1}^t |S_k|$ 表示之。

例如下面的例子為一般形式 2^6 的 Room 方陣。

		4,t		3,e		7,9		2,6		8,1	
			5,t		4,e		8,0		3,7		9,2
4,8				6,t		5,e		9,1		0,3	
	5,9				7,t		6,e		0,2		1,4
1,3		6,0				8,t		7,e		2,5	
	2,4		7,1				9,t		8,e		3,6
9,e		3,5		8,2				0,t		4,7	
	0,e		4,6		9,3				e,t		5,8
2,t		1,e		5,7		0,4				6,9	
	3,t		2,e		6,8		1,5				7,0
6,7		8,9		0,1		2,3		4,5			
	7,8		9,0		1,2		2,4		5,6		

圖 8.2. 2^6 -Room方陣

作業

1. 試證 4 階及 6 階的 Room 方陣皆不可能存在。
2. 建構一個 2^4 -Room 方陣。
3. 驗證定理 8.2。

第二章 史坦納三元系

如何在一個具有 v 個元素的集合 $\mathbf{X}$ 中，找出一族 k 個元素的子集合 $\mathbf{B}$ ，使得 $\mathbf{X}$ 中任意的兩元素都恰好包含於 $\mathbf{B}$ 中的 λ 個集合是區組設計 (Block Design) 的主要工作；這樣的區組設計 $(\mathbf{X}, \mathbf{B})$ 在 $k < v$ 的情況下，稱為是平衡不完全區組設計 (Balanced Incomplete Block Design)，簡稱為 BIBD，也可以用 (v, k, λ) -設計表示之。這個設計的基礎集是 $\mathbf{X}$ ，而 $\mathbf{B}$ 則為所有區組所成的集合。

每一個 $\mathbf{X}$ 中的元素在不同區組出現的次數用 r 表示，則 $r = \frac{\lambda(v-1)}{k-1}$ 。 $\mathbf{B}$ 中區組數 $b = \frac{\lambda v(v-1)}{k(k-1)}$ 也可以直接計算出來。於是 $\frac{\lambda(v-1)}{k-1}$ 及 $\frac{\lambda v(v-1)}{k(k-1)}$ 皆為正整數自然是一個區組設計 $(\mathbf{X}, \mathbf{B})$ 存在的必要條件，以下皆以”自然的必要條件”稱之。是否所有滿足自然的必要條件之參數組 (v, k, λ) 皆可建構出一個 (v, k, λ) -設計，則是研究組合設計的主要問題。迄今雖然有一些反例，卻也是少數；一般而言，尚未完全解決。然而，當 $k=3$ 且 $\lambda=1$ 時，我們是可以辦到的；這樣的區組設計稱為是史坦納三元系，簡記為 $\text{STS}(v)$ ，其中 $|\mathbf{X}|=v$ 。若是 λ 不一定是 1，則稱為是指標為 λ 的三元系。

1. 史坦納三元系的建構（直接建構法）

早在 1847 年，柯克曼 (T.P.Kirkman) 即證明了以下的定理：

定理 1.1. $(v, 3, 1)$ -設計存在的充要條件為 $v \equiv 1$ 或 $3 \pmod{6}$ 。

這個定理的證明經過了一個半世紀的努力，目前已經可以用很簡短的方式來達成；第一種採用直接建構法，第二種則為遞迴建構法。本節先討論第一種建構法。

爲了說明直接建構法，我們先介紹可分組設計 GDD (Group Divisible Design) 的概念。GDD($\mathbf{X}, \mathbf{B}$)，和 BIBD 不同的地方是我們先將集合分成大小一樣的幾個組， $G_1, G_2, \dots, G_m$ ，使得 $|G_i| = n$ ，且來自同一組的任兩個元素會出現在恰好 λ_1 個區組中，而來自不同組的任兩個元素會出現在恰好 λ_2 個區組中。同一組的任兩個元素稱為是第一結合類 (Associates)，不同組的任兩個元素則稱為是第二結合類。爲了方便起見，我們將用 GDD($n, m; k; \lambda_1, \lambda_2$) 來代表區組大小爲 k 的可分組設計，或是用指標爲 (λ_1, λ_2) 的 GDD(n, m) 來表示，這個時候區組的大小是固定的正整數 k 。

例 1. 由於拉丁方陣的存在性，我們可以很容易建構出 GDD($n, 3; 3; 0, 1$)，同時除了 2 與 6 之外，對於其他的 n ，GDD($n, 4; 4; 0, 1$) 也是存在的，這與互相垂直拉丁方陣的存在相呼應。

和部分拉丁方陣相似的概念，如果我們找到一族 $\mathbf{G}'$ ，使得每一個元素對(同組或不同組)，分別最多出現在 λ_1 或 λ_2 個區組中，則 $(\mathbf{X}, \mathbf{G}')$ 稱為是一個部分可分組設計 (PGDD)。

例 2. 一個具有洞的形式爲 2^t -之拉丁方陣，對應於一個部分可分組設計 PGDD($2t, 3; 3; 0, 1$)，其中，如果 $H = \{\{1, 2\}, \{3, 4\}, \dots, \{2t-1, 2t\}\}$ 爲洞的集合，則當 $\{i, j\} \in H$ 時， $\{(i, l_1), (j, l_2)\}$ ， $1 \leq l_1 \neq l_2 \leq 3$ ，爲尚未出現於任何區組的元素對；這裡的 (i, l_1) 代表第 l_1 組的第 i 個元素。

在說明建構方法之前，我們還需要幾個例子。以下我們用 STS(v)

來代表一個 $(v, 3, 1)$ -設計。

例 3. STS(7)存在。令 $\mathbf{X}=\mathbf{Z}_7$ 及 $\mathbf{B}=\{\{1+i, 2+i, 4+i\} \mid i \in \mathbf{Z}_7\}$ 。

例 4. STS(9)存在。令 $\mathbf{X}=\mathbf{Z}_9$ 及 $\mathbf{B}=\{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}\}$ 。

例 5. STS(13)存在。令 $\mathbf{X}=\mathbf{Z}_{13}$ 及 $\mathbf{B}=\{\{1+i, 2+i, 5+i\}, \{1+i, 3+i, 8+i\} \mid i \in \mathbf{Z}_{13}\}$ 。

例 6. STS(15)存在。

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

現在我們可以直接建構一個 STS(v)， $v=6k+1$ 或 $v=6k+3$ 。首先，我們先建構一個部分可分組設計 PGDD($2k, 3; 3; 1, 1$)， $(\mathbf{X}, \mathbf{G}')$ 。令 $\mathbf{X}=\{(i, l) \mid i \in \mathbf{Z}_{2k}, l \in \mathbf{Z}_3\}$ ， $\mathbf{G}'=\{\{(i, l), (j, l), (L(i, j), l+1)\} \mid i \neq j, L \text{ 為具有 } 2^k \text{ 形式的有洞 (H) 對稱拉丁方陣, } k \geq 3\}$ 。對於 $H=\{(0, 1), \dots, (2k-2, 2k-1)\}$ ，再令 $\mathbf{X}_j=\{(2j-2, l_1), (2j-1, l_2) \mid l_1, l_2 \in \mathbf{Z}_3\} \cup V$ ， $V=\{\infty\}$ （或 $\{\infty_1, \infty_2, \infty_3\}$ ），則 $|\mathbf{X}_j|=7$ （或 9 ）， $j=1, 2, \dots, k$ 。

若 $(\mathbf{X}_j, \mathbf{B}_j)$ 為一 STS(7)（或 STS(9)），則 $(\mathbf{X}, \mathbf{G}' \cup (\bigcup_{j=1}^k \mathbf{B}_j))$ 為一 STS($6k+1$) 或 STS($6k+3$)。對於 STS($6k+3$) 的建構，我們需要規定在每一個 $\mathbf{B}_j$ 中皆含有 $\{\infty_1, \infty_2, \infty_3\}$ 這個區組。因為 L 的存在僅限於 $k \geq 3$ ，所以可直接建構的 STS(v) 只有在 $v \geq 19$ 才能辦到，上述 13 及 15 的例子

恰好補上空出的兩個位置。

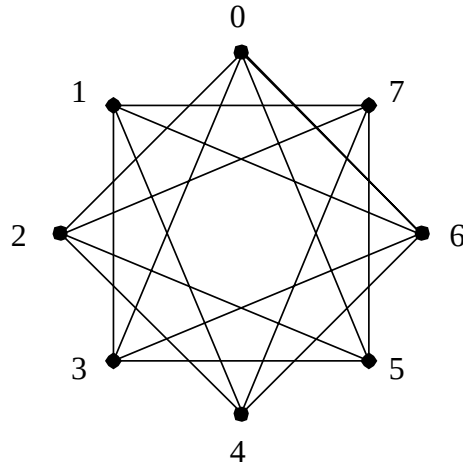
2. 遞迴建構法

接下來討論遞迴建構方式，首先，我們需要遞迴的條件，即如何由小的STS來建構大的STS。由觀察，不難發現，如果由STS(v)可以建構STS($2v+1$)及STS($2v+7$)，則全部的STS都可以經由STS(3)，STS(7)和STS(9)建構出來，所以 $v \rightarrow 2v+1$ ， $v \rightarrow 2v+7$ 為遞迴的主要條件。我們先看 $v \rightarrow 2v+1$ ，令 $\mathbf{X}=\mathbf{A}_1 \cup \mathbf{A}_2$ ，其中 $\mathbf{A}_1=\{a_i \mid i \in \mathbf{Z}_v\}$ ， $\mathbf{A}_2=\{b_j \mid j \in \mathbf{Z}_{v+1}\}$ 。考慮以 $\mathbf{Z}_{v+1}$ 為頂點集合的完全圖 $\mathbf{K}_{v+1}$ ，則這個完全圖可以分解成 v 個1-因子。令這些1-因子為 $F_0, F_1, \dots, F_{v-1}$ 。現在令 $\mathbf{B}_2=\{\{a_i, b_j, b_k\} \mid i \in \mathbf{Z}_v, \{j, k\} \in F_i\}$ ， $(\mathbf{A}_1, \mathbf{B}_1)$ 為一STS(v)，則 $(\mathbf{X}, \mathbf{B}_1 \cup \mathbf{B}_2)$ 為一個STS($2v+1$)。詳細核對在此省略。

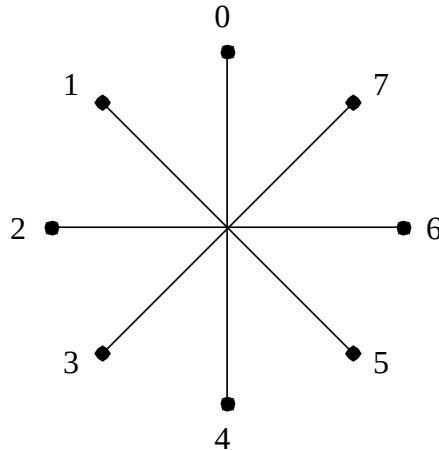
在這個建構中，我們用到了一個重要性質，即 $\mathbf{K}_{v+1}$ 可以分解成 v 個1-因子所成的集合。由邊著色的概念，只要 $v+1$ 為偶數就一定可以辦到。接下來我們來看 $v \rightarrow 2v+7$ ，這個遞迴建構需要用到較深入的定理，由於這個定理將不斷地被拿來用，因此我們詳細在此介紹。

令 G 為一個以 $\mathbf{Z}_n$ 為點的圖，則對於 $\{u, v\} \in E(G)$ ，定義 $|u - v|$ 為邊 $\{u, v\}$ 的差 (difference)。以下我們假設 G 為一完全圖。於是，不難看出具有差為 $d < n/2$ 的邊有 n 個；當 n 為偶數時，差為 $n/2$ 的邊具有 $n/2$ 個，而且這些邊形成一個完全配對或稱為是 G 的一個1-因子。差為 $d < n/2$ 的所有邊則形成一個2-因子。以下我們用 $G(D, n)$ 來表示在圖 G 中所有差為 D 中元素的所有邊所成的集合，即 $G(D, n) = \{\{u, v\} \in E(G) \mid |u - v| \in D\}$ 。

例 1. $G(\{2,3\},8)$ 的圖如下：



例 2. $G(\{4\},8)$ 的圖如下：



引理 2.1. 令 $V(G)=\mathbb{Z}_n$ 且 G 為一完全圖。假設 h 為 $D \cup \{n\}$ 的最大公因數，則 $G(D,n)$ 包含 h 個部分，而且每一部份皆和 $G(\{\frac{d}{h} | d \in D\}, \frac{n}{h})$ 同構。

證明：令 $S_i = \{i, i+h, i+2h, \dots, i+(n_1-1)h\}$ ， $hn_1=n$ ，同時 $G_i = \langle S_i \rangle_G$ ，

$H = G(\{\frac{d}{h} | d \in D\}, \frac{n}{h})$ 。定義一個由 S_i 映至 $V(H)$ 的 1-1 映成函數 φ_i ，使得

$\varphi_i(i+xh) = x$ ， $0 \leq x \leq n_1-1$ 。若 $\{i+x_1h, i+x_2h\}$ 為 G_i 的一個邊，則

$|(i+x_1h)-(i+x_2h)| \in D$ ，因此， $h|x_1-x_2| \in D$ ，即 $|x_1-x_2| \in D' = \{\frac{d}{h} | d \in D\}$ 。

因此 $\{x_1, x_2\}$ 為 H 中的一個邊。反過來說，當 $\{x_1, x_2\}$ 為 H 的一個邊時，

$\{i+x_1h, i+x_2h\}$ 亦為 G_i 的一個邊，所以 φ_i 為一個同構函數，也就是說，

對於任意的 $0 \leq i \leq h-1$ ， $G_i \cong H$ 。接下來我們證明 G_i 為 G 的一個部分 (Component)。假設 $v \in S_i$ ，則與 v 相鄰的邊 vw 必為差是 $d \in D$ 的邊，所以 $|v - w| = d = d'h$ ，這表示 $w = v \pm d'h \in S_i$ 。因此 G_i 中的點只和 G_i 中的其他點相連，再看 G_i 本身是否為一連通圖。假設 G_i 不是一個連通圖，亦即 H 不為連通圖。但是 $\text{g.c.d.}(\{\frac{d}{h} | d \in D\}) = 1$ ，令 $\{\frac{d}{h} | d \in D\} = \{d'_1, d'_2, \dots, d'_t\}$ ，則存在一組整數 $a_1, a_2, \dots, a_t$ ，使得 $\sum_{i=1}^t a_i d'_i = 1$ ，這表示任意 H 中的兩點 u_1, u_2 ，如果 $|u_1 - u_2| = x$ ，則 $\sum_{i=1}^t x a_i d'_i = x$ ，所以存在一個步徑 (Walk) 連通 u_1 及 u_2 (?)，於是 H 為連通圖，引理得證。 ■

在 $|D|=1$ 的特例下，我們可以得到以下的推論：

推論 2.2. $G(\{d\}, n)$ 中具有 $h = \text{g.c.d.}(\{d, n\})$ 個部分，同時每一個部分都是一個具 n/h 個邊的圈，除非在 $d = n/2$ 時，每一個部分都是 K_2 。

現在我們可以證明主要的定理。

定理 2.3. (Stern & Lenz) 假如 D 中包含有一個元素 d ，使得

$\frac{n}{\text{g.c.d.}(\{d, n\})}$ 為偶數，則 $G(D, n)$ 必然可以 1-分解。(第一類圖)

證明： 令 $D = \{d, d_1, d_2, \dots, d_k, \hat{d}_1, \hat{d}_2, \dots, \hat{d}_l\}$ ，其中 $\frac{n}{\text{g.c.d.}(\{d_1, n\})}$ 為奇數，

$\frac{n}{\text{g.c.d.}(\{\hat{d}_j, n\})}$ 及 $\frac{n}{\text{g.c.d.}(\{d, n\})}$ 為偶數， $1 \leq i \leq k$ ， $1 \leq j \leq l$ 。由推論 2.2.，

$G(\{\hat{d}_j\}, n)$ 是由偶數邊的圈所成的圖，所以它可以被分解成兩個 1-因子， $\hat{F}_{1,j}$ 和 $\hat{F}_{2,j}$ ，因此 $G(\{\hat{d}_1, \hat{d}_2, \dots, \hat{d}_l\}, n)$ 可以分解成 $2l$ 個 1-因子。如果 $G(\{d, d_1, d_2, \dots, d_k\}, n)$ 也可以 1-分解，定理就得證。

令 $h = \text{g.c.d.}(d, d_1, d_2, \dots, d_k, n)$ 。由引理 2.1.， $G(\{d, d_1, d_2, \dots, d_k\}, n)$ 中的每一個部分皆和 $H = G(\{\frac{d}{h}, \frac{d_1}{h}, \dots, \frac{d_k}{h}\}, \frac{n}{h})$ 同構，所以只要 H 可以 1-分解， $G(\{d, d_1, d_2, \dots, d_k\}, n)$ 就可以 1-分解。爲了方便表示，令 $d' = \frac{d}{h}$ ， $d'_i = \frac{d_i}{h}$ ， $n' = \frac{n}{h}$ ， $D' = \{d', d'_1, \dots, d'_k\}$ 。

首先，我們知道

$$(1) \quad h' = \text{g.c.d.}(D' \cup \{n'\}) = 1,$$

$$(2) \quad \frac{n'}{\text{g.c.d.}(\{d', n'\})} = \frac{\frac{n}{h}}{\text{g.c.d.}(\{\frac{d}{h}, \frac{n}{h}\})} = \frac{n}{\text{g.c.d.}(\{d, n\})},$$

$$(3) \quad \frac{n'}{\text{g.c.d.}(\{d'_i, n'\})} = \frac{n}{\text{g.c.d.}(\{d_i, n\})},$$

(2)，(3)分別爲偶數與奇數。再來 n', d'_i 爲偶數， d' 爲奇數（？）。同時當 $d' = \frac{n'}{2}$ 時， $G(D', n')$ 爲度是 $2k+1$ 的正則圖，另外當 $d' \neq \frac{n'}{2}$ 時， $G(D', n')$ 爲度是 $2k+2$ 的正則圖，附帶說明， d'_i 不會等於 $\frac{n'}{2}$ ，這是因爲 $\frac{n'}{\text{g.c.d.}(\{d'_i, n'\})}$ 是奇數的緣故。

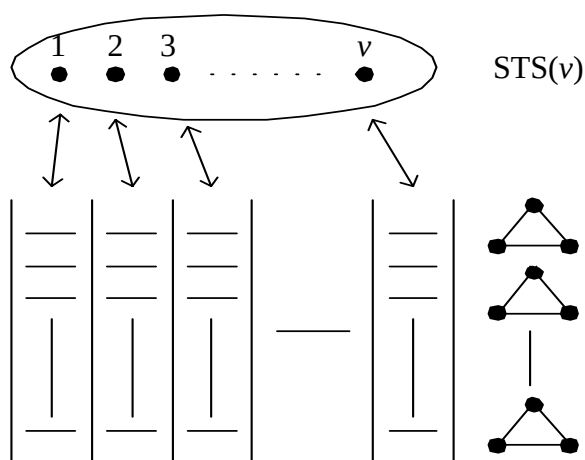
令 $H' = G(D' \setminus \{d'\}, n')$ ， $A = \{0, 2, 4, \dots, n'-2\}$ ， $B = \{1, 3, 5, \dots, n'-1\}$ ， $H'[A]$ 與 $H'[B]$ 分別是以 A, B 爲點集合在 H' 中導出的子圖 (Induced)。由於 d'_i 是偶數，在 H' 中， A 與 B 之間並無任何邊，而 $H[A]$ 和 $H[B]$ 則分別是度爲 $2k$ 的正則圖。由韋靖定理 (Vizing)， $H[A]$ 和 $H[B]$ 皆可利用 $2k+1$ 個顏色來做邊著色，由於 $H[A] \cong H[B]$ (？)，我們先塗 $H[A]$ 的邊，然後再對應地求出 $H[B]$ 的邊著色：令 $\{u, v\}$ 爲 $H[A]$ 中的一個邊，而且它塗上顏色 c ；則在 $H[B]$ 中，令邊 $\{u+d', v+d'\}$ 的顏色亦爲 c 。顯

然，在 $H[A]$ 中，若是用了 $2k+1$ 個顏色， $H[B]$ 也是用了 $2k+1$ 個顏色，而且是正規的邊著色。

最後，我們看具有差值為 d' 的邊如何加在 H' 中，使得 H 為一個第一類圖。因為 $H[A]$ 為一 $2k$ -正則圖，而我們用了 $2k+1$ 個顏色來做邊著色，因此對於 $H[A]$ 中的任一點 u ，都存在一個顏色 $c(u)$ 是 $2k+1$ 色中的一色，不出現在與 u 相鄰的邊上，於是在 $H[B]$ 中 $u+d'$ 所缺少的顏色亦為 $c(u)$ ；現在連接 u 與 $u+d'$ ，再塗上 $c(u)$ 即可得到另一個 1-因子。然而在 $d' < \frac{n'}{2}$ 情況下， u 與 $u-d'$ 仍會連接，此時加入一個新顏色 $2k+2$ 即可證明 H 為第一類圖。 ■

$v \rightarrow 2v+7$ 建構

由於 $v+7$ 是偶數，而且 $v+7 \geq 10$ ，因此令 $D = \{1, 2, \dots, \frac{v+7}{2}\}$ 。我們不難發現 $G(\{1, 2, 3\}, v+7)$ 可以分解成 $v+7$ 個三角形，而 $G(D \setminus \{1, 2, 3\}, v+7)$ 可以分解成 v 個 1-因子 $F_1, F_2, \dots, F_v$ 。仿照 $v \rightarrow 2v+1$ 的建構法，再加上 $v+7$ 個三角形就可以得到一個 $STS(2v+7)$ ，它具有一個子三元系 $STS(v)$ 。（如下圖）



3. STS 的嵌入

由遞迴建構的過程中我們發現一個 $\text{STS}(v)$ 可以嵌入於 $\text{STS}(2v+1)$ 或 $\text{STS}(2v+7)$ 中。是否一個 $\text{STS}(v)$ 可以嵌入於任一個 $\text{STS}(u)$ 中呢？這個問題終於在 20 多年前獲得答案，而且形成一族的問題 Doyen-Wilson Problem。在 1973 年 Doyen 和 Wilson 證明了下面的定理：

定理 3.1. 對於除以 6 餘 1 或 3 的兩數 u, v ，若 $u \geq 2v+1$ ，則一定存在一個 $\text{STS}(u)$ 它包含一個具有 v 個元素的子三元系。

這個定理的證明比較複雜，以下是如何利用定理 2.3 來證明的兩個例子。然後把它的摘要證明敘述在後面。

例 1. $\text{STS}(31) \supseteq \text{STS}(9)$ 。

在 K_{22} 的所有差值的集合 $\{1, 2, \dots, 11\}$ 中選出 $(1, 2, 3), (4, 5, 9)$ 兩組差值來形成三角形，剩下的差值集合為 $\{6, 7, 8, 10, 11\}$ ，由定理 2.3，我們知道， $G(\{6, 7, 8, 10, 11\}, 22)$ 可以分解成 9 個 1-因子，如此一來，例子即已證明好（？）。

（註）選出來的差值組 (x, y, z) 滿足 $x+y=z$ 或是 $x+y+z \equiv 0 \pmod{22}$ 。

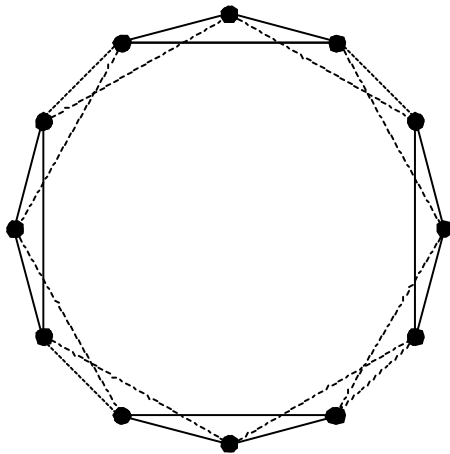
例 2. $\text{STS}(33) \supseteq \text{STS}(9)$ 。

在 $\{1, 2, \dots, 12\}$ 中選出 $(1, 2, 3), (4, 5, 9)$ 以及 8 本身來形成三角形，剩下的差值集合為 $\{6, 7, 10, 11, 12\}$ ，同上理由，例子得證。

接下來我們來看定理 3.1 的證明：由前面例子的觀察我們發現到當 $\frac{u-v}{2} - 3t = \frac{v+1}{2}$ 成立時（例 1 的形式），先在 $\{1, 2, \dots, \frac{u-v}{2}\}$ 中找到 t 組的差值組 (x_i, y_i, z_i) 使得 $x_i + y_i = z_i$ ， $1 \leq i \leq t$ ，再利用定理 2.3 即可。而這 t

組是否可以順利找到呢？它的答案是肯定的（？）。所以我們可以知道在 $\frac{u-(2v+1)}{2}$ 為 3 的倍數時，定理成立；這個式子也反應出 $v \rightarrow 2v+1$ ， $v \rightarrow 2v+7$ 建構法很容易處理。

例 2 就是不滿足上述條件的例子，即 $33-19=14$ 。所以我們分三種情況來討論。(i) $u-(2v+1) \equiv 0 \pmod{3}$ (ii) $u-(2v+1) \equiv 1 \pmod{3}$ (iii) $u-(2v+1) \equiv 2 \pmod{3}$ 。(i)已證明。現在看(ii)和(iii)。此時 $3|(u-v)$ ，因此利用例 2 的方法，先取出 t 組差值組 (x_i, y_i, z_i) ， $1 \leq i \leq t$ ，及差值 $\frac{u-v}{3}$ 來形成三角形，剩下的 $\frac{v+1}{2}$ 個差值，恰可導出 v 個 1-因子。另外，利用差值 1,2 所導出的子圖，我們可以先取出三角形，如下圖，再把剩下的部份分成兩個 1-因子也可以辦到。（多兩個 1-因子，先用 $\frac{u-v}{3}$ ；再多兩個，則用 (1,2) 的一半；再多兩個則取一個 (x_i, y_i, z_i) 即可。）定理得證。



虛線部份是哈密爾頓圖，因此可以分成兩個 1-因子。

例 3. $\text{STS}(43) \supseteq \text{STS}(9)$ 。

從 $\{1,2,\dots,15\}$ 中選出 $(4,5,9), (6,7,13), 10$ ，以及 $(1,2)$ 的一半，如上圖，剩下的部份恰好形成 13 個 1-因子。

4. λ -層三元系

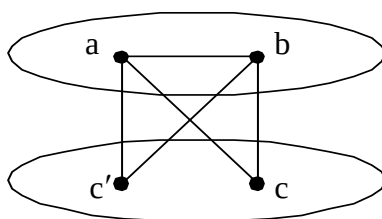
如果把三元系中的 λ ，即任兩元素出現的次數，改變成比 1 大，則它不再是所謂的史坦納三元系，我們稱它為指標為 λ 的三元系或簡稱為 λ -層三元系，2-層三元系可以由 STS 的拷貝兩次而獲得，但是，並非所有的 2-層三元系都可以如此建構出來。首先，2-層三元系存在的必要條件與 STS 存在的必要條件是不同的。

引理 4.1. 一個具有 v 個元素的 2-層三元系存在的必要條件為 $v \equiv 0$ 或 $1 \pmod{3}$ 。

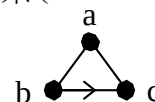
很快地我們可以證明這個必要條件也是充分條件。

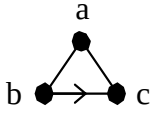
定理 4.2. 一個具有 v 個元素的 2-層三元系存在的充分必要條件為 $v \equiv 0$ 或 $1 \pmod{3}$ 。

證明：(直接建構法)利用 k 階等冪拉丁方陣，以及三個元素與四個元素的 2-層三元系即可證明它的充分性。(模仿史坦納三元系，但是同一層的 a 與 b ，若 $a \times b = c$ ， $b \times a = c'$ ，則 $\{(a,i), (b,i), (c,i+1)\}$ 與 $\{(b,i), (a,i), (c',i+1)\}$ 皆為三元集。) 如下圖。 ■



由於每一個配對都出現兩次，似乎可以考慮讓任何一個有序對 (a,b) 都出現恰好一次，這樣的三元系也稱為是有向的三元系 (Directed Triple System)，簡稱 DTS。這個時候若以有向的三角形





來表示 (a,b,c) ，則只有兩類不同的三角形，一是循環型，一是遞移型。全部都是循環型的三角形，我們稱之為孟德森（Mendelsohn）三元系 MTS，另一種為遞移三元系 DTS。

問題. 試證對於所有的 $v \equiv 0$ 或 $1 \pmod{3}$ ， $v \neq 6$ ，都存在具有 v 個元素的 MTS。

問題. 試證對於所有的 $v \equiv 0$ 或 $1 \pmod{3}$ ，都存在具有 v 個元素的 DTS。

（以上兩問題的建構法與 2-層三元系的建構法相似。）

當 λ 值更大時，建構方法也會有些不一樣；首先，令 $\lambda=6$ ，則下面的定理可以利用拉丁方陣的特性加以證明。

定理 4.3. 對於所有的正整數 $v \geq 3$ ，都存在一個具有 v 個元素的 6-層三元系。

證明： 令 $L=[l_{i,j}]$ 為一 v 階等冪拉丁方陣， $S=\{1,2,\dots,v\}$ 。當 $l_{x,y}=z$ 時，令 $\{x,y,z\} \in t$ ，則 (S,t) 為一 6-層三元系。 $\{x,y\}$ 出現在 6 個三元集分別是來自 $l_{x,y}=z$ ， $l_{y,x}=z$ ， $l_{x,w}=y$ ， $l_{w,x}=y$ ， $l_{y,u}=x$ ， $l_{u,y}=x$ 。（由於 L 是等冪，三元集不會造成有某兩個元素相同的現象。） ■

有了上述定理，對於 $\lambda > 6$ 的情況，都可以先以 6-層、6-層的方式處理，最後剩下 $0 \leq \lambda \leq 5$ ，而 $\lambda=5$ 與 $\lambda=1$ 的必要條件相同，因此重複 5 層即可，同理 $\lambda=4$ 與 $\lambda=2$ 的必要條件一樣，所以重複一次即可。所以我們只剩下 $\lambda=3$ 的情況。

定理 4.4. 具有 v 個元素 3-層三元系存在的充分必要條件為 $v \equiv 1, 3$ 或 $5 \pmod{6}$ 。

證明： 必要條件來自 v 本身一定要是奇數。在充分條件的部份則需要新的建構方式。首先當 $v=5$ 時，如下圖，所需要的 10 個三元集是 $\{a,b,1\}, \{a,b,2\}, \{a,b,3\}, \{a,1,2\}, \{a,2,3\}, \{a,1,3\}, \{b,1,2\}, \{b,2,3\}, \{b,1,3\}, \{1,2,3\}$ 。

然後再令 L 為 $2k+1$ 階的等冪對稱拉丁方陣，仿造史坦納三元系的建構方法，在三層元素間的三元集拷貝三份即可，見下圖。於是可以建構出 $6k+5$ 個元素的 3-層三元系。由此 $6k+1$ 與 $6k+3$ 個元素的 3-層三元系可以利用拷貝史坦納三元系而得到。因此，定理得證。 ■

5. 可分解的三元系 (Kirkman Triple System)

在第一節的例子中，可以找到特殊的 STS(9)及 STS(15)，它們的三元集可以被分成數組互斥三元集的集合，同時在每一組中，每一個元素都恰好出現一次；顯然也只有在 $v \equiv 3 \pmod{6}$ 時才可能找到這種形式的三元系，所以也稱為是可分解的三元系 (Resolvable) 或柯克曼三元系 (KTS)。雖然 $v=9$ 、 15 的例子在很久以前就已被發現，但是對於任意的 $v=6k+3$ 是否都存在 KTS(v) 則是近些年才獲得解決，而最早證明這個問題的是 Ray-Chadhuri 和 Wilson 在 1971 年所獲得。

定理 5.1. 對於所有的 $v \equiv 3 \pmod{6}$ 都存在有 KTS(v)。

為了證明這個定理，我們需要一個預備知識。

定義 5.2. (PBD) 配對平衡設計：一個 λ -層配對平衡設計， $(v, \mathbf{K}, \lambda)$ -設計， $(\mathbf{X}, \mathbf{B})$ ，為一個區組大小為 $\mathbf{K}$ 的元素，而任意 $\mathbf{X}$ 中的一個配對都恰好出現在 $\mathbf{B}$ 中的 λ 個區組中的設計，一般以 $(v, \mathbf{K}, \lambda)$ -PBD (Pairwise Balanced Design) 表示。

例. $\{\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3,4,5\}\}$ 為形成 $(5, \{2,4\}, 1)$ -PBD 的區組集合。

引理 5.3.[] 假如存在一個 $(v, \mathbf{K}, 1)$ -PBD 及對於所有的 $k \in \mathbf{K}$ ，KTS($2k+1$) 存在，則存在有一個 KTS($2v+1$)。

證明：令 $(Z_v, \mathbf{C})$ 為一個 $(v, \mathbf{K}, 1)$ -PBD。對於任一個 $C_b \in \mathbf{C}$ ，令 $(\{\infty\} \cup (C_b \times Z_2), t_b)$ 為 KTS($2|C_b|+1$)。則 $(\mathbf{X}, \mathbf{B}) = (\{\infty\} \cup (Z_v \times Z_2), \mathbf{B})$ 為一個 KTS($2v+1$)，其中 $\mathbf{B}$ 為下列三元集所成的集合：

(i) $\{\infty, (i, 0), (i, 1)\}$, $i \in Z_v$;

(ii) $t'_b = t_b \setminus \{\{\infty, (i, 0), (i, 1)\} \mid i \in C_b\}$ 中的三元集。

現在我們可以把 v 個平行族找出來。對於任一個 $i \in Z_v$, $\{\infty, (i, 0), (i, 1)\}$ 為 $KTS(2k+1)$ ($\{\infty\} \cup (C_b \times Z_2), t_b$) 的一個三元集, 其中 $i \in C_b$ 。令 π_i 為 $\{\infty, (i, 0), (i, 1)\}$ 與所有和這個集合在 $KTS(2k+1)$ 中形成平行族 (每個 C_b 都有一平行族) 的三元集所成的集合, 則 π_i 為 $(\mathbf{X}, \mathbf{B})$ 一個平行族, 於是定理得證。 ■

接下來, 爲了證明所有 $v \equiv 3 \pmod{6}$ 的 $KTS(v)$ 存在, 我們就需要建構適當的 PBD。以下引理是由 Brouwer 所證明。

引理 5.4. 對於所有的 $v \equiv 1 \pmod{3}$, $v \notin \{10, 19\}$, $(v, \{4, 7\}, 1)$ -PBD 存在。

有了上述引理, 加上 $v=9, 15, 21, 39$ 時, 都可以直接建構出 $KTS(v)$, 所以定理 5.1. 得證。

6. K_n 的裝填 (Packing)

當 $n \equiv 1$ 或 $3 \pmod{6}$ 時，具有 n 個元素的史坦納三元系存在；所以我們可以用一堆的三角形來裝填 K_n ，當然，在這個時候，沒有任何一個邊會被重複使用，而且也不會有任意一個邊不被使用到。然而，當 n 不是除以 6 餘 1 或 3 的數時，不管如何裝填，總是會有些邊無法被使用到，我們把剩下的邊集合所導出的子圖稱為這個裝填的殘留 (Leave)。能夠使殘留部份邊數最少的裝填又稱為是最大裝填 (Maximum Packing)。此時殘留的部份自然是最小殘留 (Minimum Leave)。以下我們先決定最小殘留的形式。

定理 6.1. 以三角形來裝填所得到的最小殘留 L 如下：

n	1	2	3	4	5	6
L	ϕ	F	ϕ	T	C_4	F

其中 F 為 K_n 的一個 1-因子； T 為 K_n 的一個懸掛子圖，除了一點的度為 3 之外，其餘的度皆為 1； C_4 是具有 4 個邊的圈。

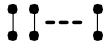
證明： (i) $n \equiv 1$ 或 $3 \pmod{6}$ ，由於史坦納三元系存在，因此沒有殘留的邊。(ii) $n \equiv 5 \pmod{6}$ ，由於殘留的邊所導出的子圖必須每個點都是偶數，所以最小的殘留是一個 2-因子；再加上當 $n=6k+5$ 時，

$$\binom{n}{4} - 4 = \frac{n(n-1)}{2} - 4 = \frac{n^2 - n - 8}{2} = \frac{(6k+5)^2 - (6k+5) - 8}{2} = \frac{36k^2 + 54k + 12}{2} =$$

$18k^2 + 27k + 6$ 為 3 的倍數，所以可能的話， C_4 為最小殘留。以下是以 C_4 為殘留的裝填方式。首先 K_5 可以利用兩個三角形裝填之後剩下一個

C_4 。接著 K_{6k} 可以分解成 5 個 1-因子及三角形 (?)，所以利用嵌入的概念，我們得到 K_{6k+5} 的裝填，使得殘留部份為 C_4 。(圖 6.1(a))

(iii) $n \equiv 0$ 或 $2 \pmod{6}$ ，這可以由一個 $STS(n+1)$ 去掉一點，而得到所需要的裝填。(我們注意到， K_n 中的每個點都有奇數點，而填塞一個三角形會用掉一點的二度，因此，每一點至少剩下一度， F 算是最小的殘留。)

(iv) $n \equiv 4 \pmod{6}$ ， F 不對的原因是 $K_n \setminus F$ 不是 3 的倍數：爲了再扣一邊才夠，殘留的部份就成爲 T ，又稱爲是三爪柱 (Tripole)， 。這個殘留可以由 $n=6k+5$ 具有 C_4 爲殘留的最大裝填中去掉一點 (殘留上)，而得到答案 (圖 6.1(b))。

我們也可以討論 λK_n 的填塞，由於證明的方式相近，在此省略。

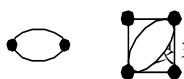
問題. λK_n 在填塞之後最小殘留的形式如何？

7. K_n 的覆蓋 (Covering)

對應於裝填的觀念，我們也可以用三角形來覆蓋 K_n ，不夠的部份需要加入一些補丁 (Padding)，如果補丁所用的邊數為最少，則此為最小覆蓋。

定理 7.1. 以三角形來覆蓋 K_n 所需要的最小補丁P如下：

n	1	2	3	4	5	6
P	ϕ	T	ϕ	T		F

證明：我們可以利用裝填的結果來完成覆蓋的工作。首先，在 n 為奇數時，只需考慮 $n \equiv 5 \pmod{6}$ ，由於 $C_4 +$ 容易分成兩個三角形，故得證。以下我們再考慮 n 為偶數的情況；由於證明方式類似，就以 $n \equiv 2 \pmod{6}$ 的情況加以證明。首先我們得到 K_{n-2} 的最大裝填，它的殘留為 $F = \{a_i b_i \mid i=1, 2, \dots, \frac{n-2}{2}\}$ ， $n-2 \equiv 0 \pmod{6}$ 。然後再加入兩個點 ∞_1, ∞_2 及連接 ∞_1, ∞_2 與 $\{a_i b_i \mid i=1, 2, \dots, \frac{n-2}{2}\}$ ，令補丁為 $F \cup \{a_i \infty_1, a_i \infty_2\}$ ，於是把加入的邊，殘留及補丁合起來分解成三角形。(如圖)

問題. λK_n 的覆蓋形式如何？

8. 史坦納三元系圖

依據三元系 $(\mathbf{X}, \mathbf{B})$ 我們可以定義出兩種圖，分別以 G 與 H 來表示。其中 $V(G) = \mathbf{B}$ ，而 G 中的兩點 B_1, B_2 相連的充要條件為 $B_1 \cap B_2 = \emptyset$ ；而 $V(H) = \mathbf{X}$ ， $E(H) = \mathbf{B}$ ，也就是說 H 為一超圖 (Hypergraph)，每個邊有三個點。所以一個設計也可以用類似的方式定義出兩種圖，於是研究設計的特性就可以藉由圖的刻劃來達成目的。

例如，判斷一個三元系是否為可分解，就等於是判斷它所對應的圖 G 是否可以找到一種均衡點著色，使得每個顏色都恰好出現 $\frac{|\mathbf{X}|}{3}$ 次，當然用了 $\frac{|\mathbf{X}|-1}{2}$ 個顏色，這也是最少的顏色數 (？)。有關 G 的點著色方面，任給一個史坦納三元系，證明它所對應的圖 G 一定滿足 $\chi(G) \leq |\mathbf{X}|$ 仍然是一個尚未解決的難題。以下是一個更強的猜測：

猜測. 除了 $|\mathbf{X}|=7$ 之外，任意史坦納三元系 $(\mathbf{X}, \mathbf{B})$ 所對應的圖 G 都滿足 $\chi(G) \leq 3|\mathbf{X}|/4$ 。

另外，求 G 中最大的獨立集 $\alpha(G)$ 也是一個多人研究過的問題。

問題. 試證 $\alpha(G) \geq \lfloor |\mathbf{X}|/4 \rfloor$ 。

就 H 而言，它是均勻圖，即每邊都具有三個點，圖的特性都可以討論，以下是一個例子。在組合設計上可以定義一種點著色：它用兩種顏色去塗點，沒有任何一般點著色的規定，但它希望能使任一個邊都有塗不同顏色的點，即邊上的三個點不可以用同一種顏色。我們不難證明在 H 來說是辦不到的，然而若是 H 對應於其他的設計，則是有可能。可以達成上述的設計又被稱為是二色設計，任一個顏色點所

成的集合也稱為是這個設計的攔截集 (Blocking Set)。

問題. 舉例說明二色設計。

史坦納三元系在組合設計的發展中扮演著開山始祖的角色，再加上它漂亮的結構，數學家從各種不同的角度從事研究，到目前為止已有上千篇的論文發表，是最受喜愛的研究對象，但由於篇幅的關係無法再多介紹，最後以幾個問題作為本章的結尾。

問題. 試證明滿足 $x^2=x$ ， $x \circ y=y \circ x$ 及 $x \circ (y \circ x)=y$ 的擬似群與一史坦納三元系等價。

(*)問題. 任給史坦納三元系，試求出它對應圖 G 的最長導出路徑 (Induced Path)。

問題. 試證對於所有 $v \equiv 1$ 或 $3 \pmod{6}$ 皆存在兩個史坦納三元系，它們只有一個共同的區組。

(*)問題. 令 $|X| \equiv 1$ 或 $3 \pmod{6}$ ，則 $\binom{X}{3}$ 可以分割成 $|X|-2$ 個史坦納三元系。

問題. 在 $\binom{X}{3}$ 中任選一組三元集 B' ，試問 B' 需要多大才一定會包含一個史坦納三元系？

第三章 一般的組合設計

只要有一個集合 X 以及 X 的一些部分集合所形成的集合族 B ，我們就有了設計 (X, B) ，這也是設計的定義。可是，由於沒有任何的規定，在應用上，尤其是實驗設計，容易造成偏差，而造成錯誤。在這一章中，我們將分別介紹幾種比較常見的組合設計，基本上都是所謂的平衡設計。有些設計在前一章已經介紹過了，在這一章中，我們將更仔細地把它們的性質作一闡述。

1. 配對平衡設計 (Pairwise Balanced Design, PBD)

定義 1.1. 在一個設計 (X, B) 中，如果任一個配對都出現在 λ 個 B 中的子集，則此設計為一配對平衡設計。如果 $|X| = v$ ， $K = \{|B| \mid B \in B\}$ ，我們一般以 (v, K, λ) -設計或 $B[v; K, \lambda]$ 來表示這一個 PBD。

以下是幾個容易證明的引理，所有的證明都省略。

引理 1.2. $K \subseteq B(K, \lambda) = \{v \mid B[v; K, \lambda] \text{ 存在}\}$ 。

引理 1.3. 假如 $K' \subseteq K$ ，則 $B(K', \lambda) \subseteq B(K, \lambda)$ 。

引理 1.4. 假如 $\lambda' \mid \lambda$ ，則 $B(K, \lambda') \subseteq B(K, \lambda)$ 。

引理 1.5. 對於任意的兩個正整數 m, n ， $B(K, \lambda) \cap B(K, \lambda') \subseteq B(K, m\lambda + n\lambda')$ 。

引理 1.6. 如果 $v \in B(K', \lambda')$ ，而且 $K' \subseteq B(K, \lambda)$ ，則 $v \in B(K, \lambda\lambda')$ 。

引理 1.6 是一個非常有用的性質，尤其是當 $\lambda'=1$ 而且 $K=\{k\}$ 的時候。

推理 1.7. 如果 $v \in B(K', 1)$ ，而且 $K' \subseteq B(k, \lambda) = B(\{k\}, \lambda)$ ，則 $v \in B(k, \lambda)$ 。

爲了更清楚地知道一個 PBD $(\mathbf{X}, \mathbf{B})$ 的性質，我們可以利用 $(\mathbf{X}, \mathbf{B})$ 來建構一個點-集圖 (Variety-Block Graph) $G_{\mathbf{X}, \mathbf{B}} = (\mathbf{X}, \mathbf{B})$ ，也就是 $G_{\mathbf{X}, \mathbf{B}}$ 爲一二分圖，其中的一個集合 $\mathbf{X} = \{x_1, x_2, \dots, x_v\}$ ，而另一集合爲 $\mathbf{B} = \{B_1, B_2, \dots, B_b\}$ ， x_i 與 B_j 相連的充要條件爲 $x_i \in B_j$ 。由 PBD 的性質，以下的引理並不難證明。

引理 1.8. 令 $(\mathbf{X}, \mathbf{B})$ 爲一 $B[v; K, \lambda]$ ，則在圖 $G_{\mathbf{X}, \mathbf{B}}$ 中，下列的性質皆成立，但 (v) 除外：

(i) $\forall B_j \in \mathbf{B}$ ， $\deg(B_j) \in K$ 。

(ii) 令 $K = \{k_1, k_2, \dots, k_t\}$ 且在 $\mathbf{B}$ 中具有度數 k_i 的點數爲 s_i ，則

$$\sum_{i=1}^t s_i \binom{k_i}{2} = \lambda \binom{|\mathbf{X}|}{2}。$$

(iii) 如果 $\lambda = 1$ ，則 $G_{\mathbf{X}, \mathbf{B}}$ 不含任何四個點的圈 (4-cycle, C_4)。

(iv) 如果 $K = \{k\}$ ，則對於所有的 $i = 1, 2, \dots, v$ ， $\deg(x_i) = \frac{\lambda(v-1)}{k-1}$ ，而且

$$b = \frac{\lambda v(v-1)}{k(k-1)}。$$

(*) (v) 當 $v \in K$ 時， $b \geq v$ 。

現在，我們可以把 $(\mathbf{X}, \mathbf{B})$ 中的平行族 (Parallel Class) 想成是 $G_{\mathbf{X}, \mathbf{B}}$ 中的一些點 $B_{i_1}, B_{i_2}, \dots, B_{i_l}$ ，它們的度數和為 v ，而且任兩點都沒有共同的鄰點 (Neighbor)，亦即 $N_G(B_{i_1}) \cap N_G(B_{i_2}) = \emptyset$ ，...，下列的猜測一般相信是非常困難的問題。

PBD 的部分平行族猜測 (P. Erdős)

在一個 PBD $B[v; K, 1] = (\mathbf{X}, \mathbf{B})$ 中， $\mathbf{B}$ 可以分割成 v 個集合，使得每一個集合都是部分平行族。

以實驗設計的觀點來看部分平行族，它代表著可以同時進行的實驗，於是平行族的個數就代表著實驗所需要的總時間之估計。當 $K = \{3\}$ ，我們就有了史坦納三元系的部分平行族猜測。

史坦納三元系的部分平行族猜測

任一個 $STS(v)$ 的區組集合皆可以分割成 v 個部分平行族。

上述的猜測在 $v \leq 15$ 時都已被核對出來，而且都是正確無誤。同時，除了 $v = 7$ 之外，所需要的平行族都很明顯地都小於 v ，因此，我們可以進一步猜測部分平行族的個數為 $\left\lceil \frac{3v}{4} \right\rceil$ ，其中 $v \neq 7$ 。

再來看看 $G_{\mathbf{X}, \mathbf{B}}$ 究竟會有多少個邊？首先，我們固定 $\lambda = 1$ ，則對於所有的 $m \leq n$ ，皆存在一個 PBD $(\mathbf{X}, \mathbf{B})$ 使得 $|\mathbf{X}| = m$ 及 $|\mathbf{B}| = n$ (？)。那麼，就給定的 (m, n) ，那一種具 n 個區組的 PBD $B[m; K, 1]$ 會對應到一個具有最多邊數的 $G_{\mathbf{X}, \mathbf{B}}$ 呢？例如， $(7, 7)$ 這個配對能對應到的 $G_{\mathbf{X}, \mathbf{B}}$ 最多有多少邊呢？

例： $(\mathbf{X}, \mathbf{B}_1) = \text{STS}(7)$ ， $(\mathbf{X}, \mathbf{B}_2)$ 中， $\mathbf{B}_2 = \{\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{1,6\}, \{1,7\}, \{2,3,4,5,6,7\}\}$ 。 $|E(G_{\mathbf{X}, \mathbf{B}_1})| = 21$ ， $|E(G_{\mathbf{X}, \mathbf{B}_2})| = 18$ 。

下面的定理告訴我們，上例中的 21 是最大的邊數，這更說明了區組的元素個數越平均將會製造出邊數較多的 $G_{\mathbf{X}, \mathbf{B}}$ 。

定理 1.9. (Fu and Bryant) 令 $(\mathbf{X}, \mathbf{B})$ 為一個 PBD，它的 $\lambda = 1$ ，

其中 $\mathbf{B} = \{B_1, B_2, \dots, B_n\}$ 。若是對所有的 $i=1, 2, \dots, n$ ， $|B_i| = \{k, k+1\}$ 且

$\binom{|\mathbf{X}|}{2} - \sum_{i=1}^n \binom{|B_i|}{2} < k$ ，則 $G_{\mathbf{X}, \mathbf{B}}$ 為所有用 $|\mathbf{X}|$ 個點及 $|\mathbf{B}|$ 個區組所能定義出

來的 $(v, K, 1)$ -設計之對應圖中，邊數最多的一個。

這個定理並沒有完全刻劃出如何找到最多邊的 $G_{\mathbf{X}, \mathbf{B}}$ ，後續的努力仍然是必要的。不過，有一額外的發現：因為 $G_{\mathbf{X}, \mathbf{B}}$ 中不含 C_4 ，於是，只要有一個二分圖，它不含任何 C_4 ，則可以用來定義一個部分 PBD (?)。

作業

1. 證明引理 1.6。
2. 證明引理 1.8 中的(i)~(iv)。
3. 令 $(m, n) = (9, 12)$ ，則所對應的 $G_{\mathbf{x}, \mathbf{B}}$ 可能會有多少邊？
4. 如果一個圖 G 本身不含 C_4 ，但是每加上任一邊就會含有 C_4 ，我們稱 G 為 C_4 -飽和 (Saturated)。試證任一 PBD 所對應的 $G_{\mathbf{x}, \mathbf{B}}$ 皆為 C_4 -飽和圖。

2. 可分組設計 (Group Divisible Design , GDD)

在第二章我們介紹過 GDD，在此再回憶一下。

定義 2.1. 令 X 為可分成 m 組，每組 n 個元素的集合，亦即 $X = \bigcup_{i=1}^m G_i$ ，

$|G_i| = n$ ， $i=1,2,\dots,m$ ； B 為一個由 k 元子集區組所形成的集合族，且滿足下列兩個條件：

- (i) 任兩個同組的元素會共同出現於 $\lambda_1 \geq 0$ 個區組中。
- (ii) 任兩個來自不同組的元素會共同出現於 $\lambda_2 \geq 1$ 個區組中。

在上面的定義中，同組的兩個元素稱為是第一結合類 (Associates)，不同組的兩個元素則為第二結合類。在傳統的 GDD 中，我們一般討論 $\lambda_1 = 0$ 的情況， $\lambda_1 \neq 0$ 而且 $\lambda_1 \neq \lambda_2$ 是比較近期才考慮的問題。在這一節中，我們假設 $\lambda_1 = 0$ 且 $\lambda_2 = \lambda$ 。為了方便起見，用 $GD[n,m;k,\lambda]$ 代表這樣的 GDD，於是當 $n=1$ 時，我們就等於是有一個 BIBD (平衡不完全區組設計)。同樣地，我們也可以用 $GD(k,\lambda)$ 來表示所有可能的 $v=mn$ 使得 $GD[n,m;k,\lambda]$ 存在。假設 m 或 n 已經固定，則用 $GD(-,m;k,\lambda)$ 或 $GD(n,-;k,\lambda)$ 來分別代表 $v=mn$ 所成的集合。

引理 2.2. 令 $\lambda' \mid \lambda$ ，則 $GD(n,-;k,\lambda') \subseteq GD(n,-;k,\lambda)$ 。

引理 2.3. $GD(n,-;k,\lambda) \subseteq B(\{k,n\},\lambda)$

引理 2.4. $GD(n,-;k,\lambda)+1 \subseteq B(\{k,n+1\},\lambda)$ 。

證明：加一點到 $GD(n,-;k,\lambda)$ 裡面。 ■

引理 2.5. $GD(k, -; k, \lambda) \subseteq B(k, \lambda)$ 。

引理 2.6. $GD(k-1, -; k, \lambda)+1 \subseteq B(k, \lambda)$ 。

引理 2.7. $GD(k-1, -; k, 1)+1 = B(k, 1)$ 。

證明：由引理 2.5，我們只需要在證明 $B(k, 1)$ 包含於另一集合。令 $v \in B(k, 1)$ ，而且 $(\mathbf{X}, \mathbf{B})$ 為一個 $B[v; k, 1]$ 。在 $\mathbf{X}$ 中任選一點 ∞ ，將 ∞ 去掉，也同時去掉包含 ∞ 的那些區組，於是剩下的就是一個 $GD[k-1, \frac{v-1}{k-1}; k, 1]$ 。所以 $v-1 \in GD(k-1, -; k, 1)$ 。 ■

引理 2.8. 令 $n \in B(k, \lambda)$ ，則 $GD(n, -; k, \lambda) \subseteq B(k, \lambda)$ 。

引理 2.9. 令 $n+1 \in B(k, \lambda)$ ，則 $GD(n, -; k, \lambda)+1 \subseteq B(k, \lambda)$ 。

引理 2.10. 令 $n+k \in B(k, 1)$ ，則 $GD(n, -; k, \lambda) \subseteq B(k, \lambda)$ 。

證明：加入 k 點到 GDD 上。 ■

引理 2.11. 令 $m \in B(K, \lambda)$ 且 $nK \subseteq GD(n, -; k, \lambda')$ ，則 $mn \in GD(n, m; k, \lambda\lambda')$ 。

引理 2.12. 令 $v \in B(k, \lambda)$ 且 $(k-1)K+1 \subseteq B(k, 1)$ ，則 $(k-1)v+1 \in B(k, \lambda)$ 。

證明：由引理 2.6，我們知道 $GD(k-1, -; k, 1)+1 = B(k, 1)$ ，因此 $GD(k-1, -; k, 1) = B(k, 1)-1$ ，所以由已知 $(k-1)K \subseteq GD(k-1, -; k, 1)$ ，於是由於 $v \in B(k, \lambda)$ ， $(k-1)v \in GD(k-1, -; k, \lambda)$ ，這個結果可以推得 $(k-1)v+1 \in B(k, \lambda)$ 。 ■

我們可以將定義 2.1 加以擴展成更一般形式的可分組設計，一般稱之為配對可分組設計。

定義 2.13. (Pairwise Group Divisible Design , PGDD) 一個三元序對 $(\mathbf{X}, \mathbf{G}, \mathbf{B})$ 稱為是 PGDD，記為 $\text{GD}[v; K, M; \lambda]$ ，如果它滿足下列五個條件：

- (i) $|\mathbf{X}| = v$ ；
- (ii) $\mathbf{X} = \bigcup_{i=1}^m G_i$ 且 $\{|G_i| \mid G_i \in \mathbf{G}\} \subseteq M$ ；
- (iii) $\{|B_i| \mid B_i \in \mathbf{B}\} \subseteq K$ ；
- (iv) $|G_i \cap B_j| \leq 1, \forall i, j, G_i \in \mathbf{G} \text{ 且 } B_j \in \mathbf{B}$ ；
- (v) 不在同組 (G_i 's) 的任兩個元素恰好一同出現在 λ 個 $\mathbf{B}$ 中的區組。

顯然，當 $M = \{n\}$ 及 $K = \{k\}$ 時一個 PGDD 基本上就是一個 GDD；所以 PGDD 可以把它想像成 PBD，它容許有不同大小的組 (Groups)，及不同的區組 (Blocks)。以下是一些基本性質：

在下列的引理中，我們用 $\text{GD}(K, M; \lambda)$ 代表所有使得 $\text{GD}[v; K, M; \lambda]$ 存在的 v 所成的集合。

引理 2.14. $M \subseteq \text{GD}(K, M; \lambda)$ 。

引理 2.15. 若 $M' \subseteq M$ 且 $K' \subseteq K$ ，則 $\text{GD}(K', M'; \lambda) \subseteq \text{GD}(K, M; \lambda)$ 。

引理 2.16. 若 $\lambda' \mid \lambda$ ，則 $\text{GD}(K, M; \lambda') \subseteq \text{GD}(K, M; \lambda)$ 。

引理 2.17. 若是 $v \in \text{GD}(K, M'; \lambda')$ 且 $M' \subseteq \text{GD}(K, M; \lambda)$ ，則 $v \in \text{GD}(K, M; \lambda\lambda')$ 。

引理 2.18. $\text{GD}(K, M; \lambda) \subseteq B(K \cup M, \lambda)$ 。

引理 2.19. $\text{GD}(K, M; \lambda) + 1 \subseteq B(K \cup (M+1), \lambda)$ 。

引理 2.20. 若是 $n \in \text{GD}(S, R; 1)$ ， $mR \subseteq B(k, \lambda)$ 以及 $mS \subseteq \text{GD}(m, -; k, \lambda)$ ，則 $mn \in B(k, \lambda)$ 。

證明： 令 $X = Z_m \times Z_n$ ，對於每一個 $i \in Z_m$ ，在集合 $\{i\} \times Z_n$ 上建構一個結構一樣的 $\text{GD}[n; S, R; 1]$ 。令這個 PGDD 的組分別為 $G_{i,1}, G_{i,2}, \dots, G_{i,t}$ ， $B_{i,l}$ 為這個 PGDD 在 $\{i\} \times Z_n$ 中的區組， $l=1,2,\dots$ 。現在，對每一個 $1 \leq j \leq t$ ，在集合 $\bigcup_{i=1}^m G_{i,j}$ 上建構一 $B[m|G_{i,j}|, k, \lambda]$ ，對每一個在 $\text{GD}[n; S, R; 1]$ 中的區組 $B_{i,l}$ 在 $\bigcup_{i=1}^m B_{i,l}$ 建構一個 GDD， $\text{GD}[m, |B_{i,l}|; k, \lambda]$ ，如此一來兩個設計的聯集即為所求的 $B[v; k, \lambda]$ ，其中 $v = mn$ 。 ■

同理，我們可以證明下面的結果。（作業）

引理 2.21. 若是 $n \in \text{GD}(S, R; 1)$ ， $mR+1 \subseteq B(k, \lambda)$ 且 $mS \subseteq \text{GD}(m, -; k, \lambda)$ ，則 $mn+1 \in B(k, \lambda)$ 。

作業

1. 試求 $\text{GD}[n, m; k, \lambda]$ 存在的必要條件。
2. 試證明上題的必要條件在 $m = 2$ 及 $k = 3$ 時不一定是充分條件。
3. 試證明引理 2.21。

3. 橫截設計 (Transversal Designs)

橫截設計是一種特殊的可分組設計，其中每一組與每一區組恰好有一共同點，也就是說組數恰為區組的大小。所以，區組與組的大小決定這個設計。我們用 $T[s, r; \lambda]$ 來代表一個具有區組大小為 s ，組的大小為 r 的橫截設計。由於組的大小一旦知道，加上區組的大小固定，橫截設計的形式自然決定，所以令 $T(s, \lambda)$ 代表所有使得 $T[s, r; \lambda]$ 存在的 r 所成的集合。下述的性質不難證明。

引理 3.1. 若 $s' \leq s$ ，則 $T(s, \lambda) \subseteq T(s', \lambda)$ 。

引理 3.2. 令 $\lambda' \mid \lambda$ ，則 $T(s, \lambda') \subseteq T(s, \lambda)$ 。

引理 3.3. 若 m 與 n 為正整數，則 $T(s, \lambda) \cap T(s, \lambda') \subseteq T(s, m\lambda + n\lambda')$ 。

引理 3.4. 若是 $r \in T(s, \lambda)$ 且 $r' \in T(s, \lambda')$ ，則 $rr' \in T(s, \lambda\lambda')$ 。

證明：作業。 ■

以下的結果可以由互相垂直的拉丁方陣求得。

定理 3.5. 令 q 為一質數的次方，即 $q = p^n$ ，則 $q \in T(q+1, 1)$ 。

證明：令 $A_1, A_2, \dots, A_{q-1}$ 為 $q-1$ 個彼此互相垂直的 q 階拉丁方陣。再令 $G_i = Z_q \times \{j\}$ ， $j=1, 2, \dots, q+1$ ， $B_{i,j} = \{(i, 1), (j, 2), (A_1(i, j), 3), \dots, (A_{q-1}(i, j), q+1)\}$ ，則 $\mathbf{B} = \{B_{i,j} \mid i \in Z_q, j=1, 2, \dots, q+1\}$ 為 $T[q+1, q; 1]$ 的區組。 ■

事實上，我們可以看出來當 $s \leq r$ 時，一個 $T[s, r; 1]$ 設計與 $s-2$ 個 $\text{MOLS}(r)$ 的存在性是互相對應的結果。接下來，我們再看一個比較特

殊的橫截設計。

定義 3.6. 一個橫截設計 $T[s, r; \lambda]$ ，如果它的區組能分割成 λr 個平行族，則此設計又稱為是可分解 (Resolvable) 的橫截設計，以 $RT[s, r; \lambda]$ 表示。

由於可分解的特性，我們可以證明下面的結果。

引理 3.7. $RT(s, 1) = T(s+1, 1)$ 。

證明：($\subseteq$) 對於每一個 $r \in RT(s, 1)$ ，我們可以分別加入一點 ∞_i 到第 i 個平行族，於是多了一組 $\{\infty_1, \infty_2, \dots, \infty_r\}$ ，而建構了一個 $T[s+1, r; 1]$ 。

($\supseteq$) 在 $T[s+1, r; 1]$ 去掉任一組即可獲得一個 $RT[s, r; 1]$ 。 ■

至於 $\lambda \neq 1$ ，引理 3.7 無法推出 $RT(s, \lambda) = T(s+1, \lambda)$ ，主要是因為在 $T[s+1, r; \lambda]$ 中去掉一組無法保證得出來的橫截設計必定是可分解的設計。

引理 3.8. $RT(s, \lambda) \subseteq T(s+1, \lambda)$ 。

定理 3.9. 若是 $r \in GD(K, M; \lambda)$ ， $M \subseteq T(s, \lambda)$ 且 $K \subseteq RT(s, 1)$ ，則 $r \in T(s, \lambda)$ 。

證明：首先建構一個配對 GDD，然後對應於組的大小 (M) 建構 $T(s, \lambda)$ ，而對應於區組的大小 (K) 建構一個 $RT(s, 1)$ 使它滿足垂直的區組恰為一個平行族，如圖 3.1。於是把對應於 M 中所求得的 $T(s, \lambda)$ ，以 λ 倍的 $RT(s, 1)$ (對應於 K) 的區組放在一起，然後去掉 $\lambda-1$ 組垂直的區組即為所求的橫截設計。 ■

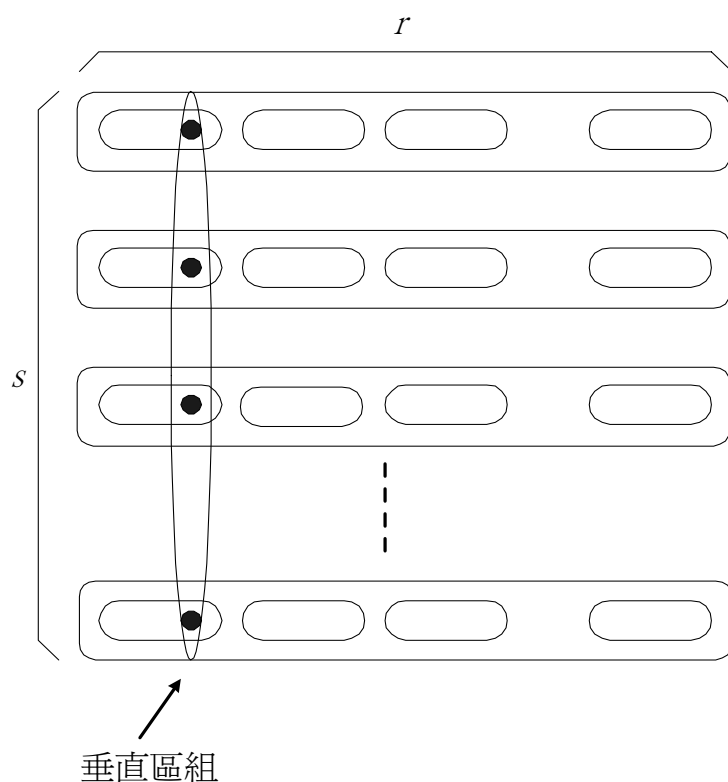


圖 3.1

上面定理在 $\lambda = 1$ 及 $M = \{1\}$ 的特殊情況下可以獲得相當好的結果。

定理 3.10. 若是 $r \in B(K, 1)$ ，而且 $K \subseteq RT(s, 1)$ ，則 $r \in T(s, 1)$ 。

推論 3.11. 若是 $r \in B(K, 1)$ ，而且 $K \subseteq T(s+1, 1)$ ，則 $r \in T(s, 1)$ 。

證明：引理 3.7。



這裡特別說明推論 3.11 的應用。例如，我們希望證明互相垂直的 n 階拉丁方陣存在，亦即證明 $n \in T(4, 1)$ ；利用 $\{4, 5\} \subseteq T(5, 1)$ ，只要 $n \in B(\{4, 5\}, 1)$ 即可，當然 K 可以選擇大一點的集合。

(*)問題：利用推論 3.11 推翻尤拉猜測。

作業

- (*) 1. 令 $K = \{4, 7, 10, 19\}$ ，則對於所有的 $k \geq 1$ ，證明 $3k+1 \in B(K, 1)$ 。
2. 先證明 $22 \in B(\{4, 7\}, 1)$ ，再利用推論 3.11 證明尤拉猜測是錯誤的。
- (**) 3. 利用推論 3.11 證明 $26 \in T(4, 1)$ 。

4. 刪點橫截設計 (Truncated Transversal Designs , TTD)

TTD 基本上是一種 PGDD，但是由於它可以經由一個 TD 刪去一些點之後而建構出來，因此特別有個名字。也因為它的應用不少，所以在這一節中我們特別介紹這種設計。

令 $(\mathbf{X}, \mathbf{G}, \mathbf{B})$ 為一個 $T[s+t, r; \lambda]$ ，其中 $\mathbf{G} = \{G_i \mid i = 1, 2, \dots, s+t\}$ 。現在，固定前面的 s 組， $G_1, G_2, \dots, G_s$ ，然後令 $H_{j-s} = G_j \setminus S_{j-s}$ ，其中 $S_{j-s} \subseteq G_j, j = s+1, \dots, s+t$ ，同時 $|H_{j-s}| = r_{j-s}$ 。為了方便起見，令 $r_1 \geq r_2 \geq \dots \geq r_t$ 。於是 $(\mathbf{X}', \mathbf{G}', \mathbf{B}')$ 為一 PGDD， $\mathbf{X}' = (\bigcup_{i=1}^s G_i) \cup (\bigcup_{l=1}^t H_l)$ ， $\mathbf{G}' = \{G_i, H_l \mid i=1, 2, \dots, s; l=1, 2, \dots, t\}$ 以及 $\mathbf{B}' = \{B \setminus (\bigcup_{j=1}^t S_{j-s}) \mid B \in \mathbf{B}\}$ 。同時這個 PGDD 的組，大小分別為 $r, r_1, r_2, \dots, r_t$ ，而區組的大小則可能為 $s+t, s+t-1, \dots, s$ 之一，所以這個 PGDD 可以記為 $GD[sr + \sum_{i=1}^t r_i; \{s, s+1, \dots, s+t\}, \{r, r_1, r_2, \dots, r_t\}; \lambda]$ ，以下的性質皆可以很容易地加以證明。

引理 4.1. 若是 $r \in T(s+t, 1)$ ， $r \geq r_1 \geq r_2 \geq \dots \geq r_t \geq 0$ 且 $\{s, s+1, \dots, s+t, r, r_1, \dots, r_t\} \subseteq B(K, \lambda)$ ，則 $rs + \sum_{i=1}^t r_i \in B(K, \lambda)$ 。

引理 4.2. 若是 $r \in T(s+t, 1)$ ， $r \geq r_1 \geq r_2 \geq \dots \geq r_t \geq 0$ ，且 $\{s, s+1, \dots, s+t, r+1, r_1+1, \dots, r_t+1\} \subseteq B(K, \lambda)$ ，則 $rs+1 + \sum_{i=1}^t r_i \in B(K, \lambda)$ 。

引理 4.3. 若是 $r \in T(s, 1)$ ，且 $\{s, r\} \subseteq B(K, \lambda)$ ，則 $rs \in B(K, \lambda)$ 。

引理 4.4. 若是 $r \in T(s, 1)$ ，且 $\{s, r+1\} \subseteq B(K, \lambda)$ ，則 $rs+1 \in B(K, \lambda)$ 。

引理 4.5. 若是 $r \in T(s,1)$ ，且 $r > 1$ ，則 $r \geq s-1$ 。

引理 4.6. 若是 $r \in T(s,1)$ ，且 $r \geq s$ ，則 $T[s,1;r]$ 中必定包含至少兩個互斥的區組。

有了以上的引理，我們就可以證明下面重要的結果。

定理 4.7. 令 $(Y \cup T', \mathbf{B}, \mathbf{G})$ 為一刪點橫截設計，其中 $\mathbf{G} = \{G_1, G_2, \dots, G_s, G_{s+1}, \dots, G_{s+t}\}$ ， $|G_i| = r$ ， $i = 1, 2, \dots, s$ ； $|G_{s+j}| = r_j \leq r$ ， $j = 1, 2, \dots, t$ ， $T' = \bigcup_{j=1}^t G_{s+j}$ ，以及 $\mathbf{B}$ 中的任一區組 B ， $|B \cap T'| \leq 2$ 。若是 $\{m, m+1, m+2, r_1, r_2, \dots, r_t\} \subseteq T(s,1)$ ，則 $mr + |T'| \in T(s,1)$ 。

證明：(概述) 令 $X = X_1 \cup X_2 \cup \dots \cup X_s$ ，其中每個 X_i 皆有 $mr + |T'|$ 個點。對應於已知的刪點橫截設計之區組 $\mathbf{B}$ ，及組（刪點），分別建構 $T[s, m+|B \cap T'|; 1]$ 及 $T[s, r_i; 1]$ 。當 $|B \cap T'| = 2$ 時， $T[s, m+2; 1]$ 必含有兩個互斥的區組，令此兩區組為垂直的區組，而且出現在刪點組的部分，如下圖，同理，於 $T[s, m+1; 1]$ 中，令垂直組為一區組；在全部的建構完成後，去掉這部分的區組即可求得所需要的橫截設計。 ■

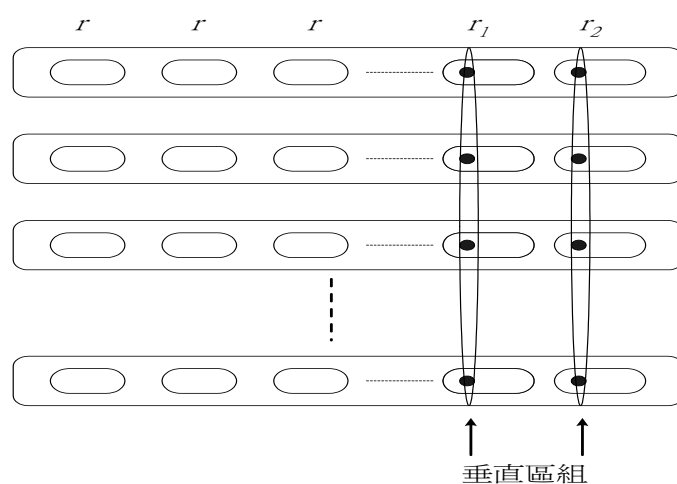


圖 4.1

有了定理 4.7，我們不難利用它來建構更多互相垂直的 n 階拉丁方陣，尤其是尤拉所猜測辦不到的 $n \equiv 2 \pmod{4}$ ，或者是多一點的互相垂直的拉丁方陣。例如： $r=7$ ， $s=5$ ， $t=2$ ， $(r_1=r_2=1)$ ， $m=7$ ，可以用來證明至少有 3 個互相垂直的 51 階拉丁方陣，而原來馬可尼希猜測只有兩個存在。

將上述定理以比較特別的形式表示出來就可以比較方便應用。

推論 4.8. 若是 $r \in T(s+2,1)$ ， $0 \leq r_2 \leq r_1 \leq r$ 且 $\{m, m+1, m+2, r_1, r_2\} \subseteq T(s,1)$ ，則 $mr+r_1+r_2 \in T(s,1)$ 。

推論 4.9. 若是 $r > \frac{(t-1)(t-2)}{2}$ ， $r \in T(s+t,1)$ 且 $\{m, m+1, m+2\} \subseteq T(s,1)$ ，則 $mr+t \in T(s,1)$ 。

證明：對應於定理 4.7 的刪點截集設計，我們希望能令 $r_1=r_2=\dots=r_t=1$ ，同時滿足任一區組與 T' 的交集最多兩點。由 $r > \frac{(t-1)(t-2)}{2}$ ，我們可以由 G_{s+1} 組選起，讓區組不會碰到兩組以上的點，於是推論得證。



在這裡再一次說明推論 4.8 的應用，當 $m=7$ ， $r=8$ ， $s=4$ 時，我們不難證明 $\{62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72\} \subseteq T(s,1)$ （？）。

作業

1. 證明對於所有的 $100 \leq n \leq 200$ ，皆存在 3 個互相垂直的 n 階拉丁方陣。
- (*)2. 證明對於所有的 n ， $n \neq 2, 6$ ，皆存在 2 個互相垂直的 n 階拉丁方陣。

5. BIBD with $k=4$

首先我們先討論當 $\lambda=1$ 的時候。由引理 2.21，我們考慮 $m=3$ ， $n \equiv 0$ 或 $1 \pmod{4}$ 即可，也就是對於所有 n ，要能建構一個 GDD， $GD[n; S, R; \lambda]$ 使得 $3R+1 \subseteq B(4,1)$ ，而且 $3S \subseteq GD(3, -; 4, 1)$ 。爲了便於建構 GDD，我們選擇 $S=\{4,5\}$ （區組的大小），在加上適當的 R ，就可以證明下面的定理。

定理 5.1. $B[v; 4, 1]$ 存在的充要條件爲 $v \equiv 1$ 或 $4 \pmod{12}$ 。

證明：（ $\Rightarrow$ ）由直接計算可得。

（ $\Leftarrow$ ）令 $v = 3n+1$ ，其中 $n \equiv 0$ 或 $1 \pmod{4}$ 。令 $R=\{1,4,5,8,9,12,13,28,29\}$ 及 $S=\{4,5\}$ 。首先我們證明 $GD[n; S, R; 1]$ 存在。由於對於所有 $n > 10$ ，皆存在至少三個 n 階拉丁方陣彼此互相垂直，所以對於所有的 $r > 10$ ， $T[5, r; 1]$ 存在。因此，當 $n \geq 52$ ，我們可以由 $T[5, r; 1]$ 中去掉一組元素中的 r 個使得此去掉後的刪點橫截設計元素總數爲 $4r+r_1$ ，其中 $0 \leq r_1 \leq r$ ， $r_1 \equiv 0$ 或 $1 \pmod{4}$ 。接著再利用小的 n 把每一組轉換成指定大小的組，亦即組的大小要是集合 R 中的元素，由引理 2.17，令 $\lambda = \lambda' = 1$ ，即可得到 $GD[n; S, R; 1]$ 。接下來再看小於 50 的 n ，這可以由小的 r 直接湊出來，例如 $16 \leq n \leq 20$ ，選 $r = 4$ 。其他的 n 不難找到對應的 r ，在此省略。再來，我們將利用引理 2.21，其中 $\lambda=1$ ，現在 $S=\{4,5\}$ ，而 $12, 15 \subseteq GD(3, -; 4, 1)$ ，取組數爲 4 或 5（？）。因此，只要 $3R+1 \subseteq B(4, 1)$ ，定理即得證。也就是要證明 $\{4, 13, 16, 25, 28, 37, 40, 85, 88\} \subseteq B(4, 1)$ 。由於每一個值都是直接建構，在此省略大部分的值，只以 40 及 85 爲例。由於 $13 \in B(4, 1)$ ，由引理 2.12， $40 \in B(4, 1)$ 。同理， $28 \in B(4, 1)$ 及 $13 \in B(4, 1)$ ，我們知道 $85 \in B(4, 1)$ 。 ■

由上述的討論，我們發現引理 2.20 是很重要的工具，而這個工具最需要的兩個條件為找到 R 使得 (1) $n \in \text{GD}(S, R; 1)$ 及 (2) $mR \subseteq B(k, \lambda)$ ，在討論 $k=4$ 的情況，一般都選定 $S=\{4,5\}$ ，所以 R 成為重點。

定理 5.2. $B[v; 4, 2]$ 存在的充要條件為 $v \equiv 1 \pmod{3}$ 。

證明：證明的概念與定理 4.1 相似。首先令 $v=3n+1$ ，此時 $m=3$ ，再來 $R_2=\{1, 2, \dots, 15, 26, 27\}$ 。接下來的工作是 (1) 證明 $\text{GD}[n; \{4, 5\}, R_2; 1]$ 存在，及 (2) 證明 $3R_2+1 \subseteq B(4, 2)$ 。其中 (1) 比較容易，它可由 $T[5, r; 1]$ 的存在加以證明，而另一件事就要建構小的 $B[v; 4, 2]$ 再完全全部的工作，當然，這是需要一些力氣，在此省略。(作業) ■

定理 5.3. $B[v; 4, 3]$ 存在的充要條件為 $v \equiv 0$ 或 $1 \pmod{4}$ 。

證明：由定理 1 的證明，我們推得 $v \in B(R, 1)$ ，於是只要證明 $R \subseteq B(4, 3)$ 即可。顯然 $\{1, 4, 13, 28\} \subseteq B(4, 1) \subseteq B(4, 3)$ ，所以剩下 5, 8, 9, 12 及 29。這些都可以直接建構(作業)，所以定理得證。 ■

定理 5.4. $B[v; 4, 6]$ 存在若且唯若 $v \geq 4$ 。

證明： $v=4$ 時顯然成立。當 $v=5$ 時可利用 $\{1, 2, 3, 4\}$ 及 $\{1, 2, 3, 5\}$ 做生成集 (Starters) 來求得 10 個區組，此時差集 $\{1, 2\}$ 中的元素各出現 6 次；當 $v=6$ 時，則生成集是 $\{1, 2, 3, 5\}$ ， $\{1, 2, 4, 6\}$ 及半個 $\{1, 2, 4, 5\}$ (?)。但一般的 v 有規則嗎? (作業)

定理 5.5. $B[v; 4, \lambda]$ 存在的充要條件為 $\lambda(v-1) \equiv 0 \pmod{3}$ 及 $\lambda v(v-1) \equiv 0 \pmod{12}$ 。

證明：綜合定理 5.1，5.2，5.3 及 5.4 即可得證。 ■

作業

1. 證明 $\{25, 28, 37, 88\} \subseteq B(4, 1)$ 。
2. 證明 $\{79, 82\} \subseteq B(4, 2)$ 。
3. 證明 $\{7, 8, 9, 10\} \subseteq B(4, 6)$ 。
4. 證明 $\{5, 8, 9, 12, 29\} \subseteq B(4, 3)$ 。

6. 利用 PBD 推翻尤拉猜測

在這一節中，我們主要是證明對於任一個不等於 2 或 6 的正整數 n ，都存在兩個互相垂直的 n 階拉丁方陣。當 $n=10$ ，在第一章已經提供了例子，以下的討論，將針對 $n \geq 14$ 加以說明。

引理 6.1. 令 $(\mathbf{X}, \mathbf{B})$ 為一個 PBD $B[n; K, 1]$ ，其中對於 K 中的任意一個元素 k 皆存在一個等冪 k 階拉丁方陣 L_k ，則由此 PBD 可以定義出一個等冪 n 階拉丁方陣 L ，定義如下：

(i) $L(x, x) = x, \forall x \in \mathbf{X}。$

(ii) $L(x, y) = L_k(x, y), x \neq y$ 且 x, y 同時落在一個 k 個元素的區組。

證明：(作業)。



定理 6.2. 令 $(\mathbf{X}, \mathbf{B})$ 為一個 PBD $B[n; K, 1]$ ，而且對於 K 中的每一個元素 k 皆存在兩個互相垂直的等冪 k 階拉丁方陣，則必存在兩個互相垂直的等冪 n 階拉丁方陣。

證明：由引理 6.1，首先針對一組的 k 階拉丁方陣建構一個等冪 n 階拉丁方陣 L_1 ，同理，由另一組建構一個 L_2 。現在，利用兩指定律即可證明 $L_1 \perp L_2$ 。



有了上述的定理，建構互相垂直的拉丁方陣就不再是那麼困難。例如當 $n=21$ ， $K=\{5\}$ 時，因為 $B[21; 5, 1]$ 存在，而且存在 3 個等冪 5 階拉丁方陣，如圖 6.1，於是存在 3 個互相垂直的等冪 21 階拉丁方陣，這樣的結果顯然已經證明馬克尼希的猜測是錯誤的，不過，我的目標是尤拉猜測。

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

圖 6.1

引理 6.3. 令 $K=\{4,7\}$ ，則 $B[22;K,1]$ 存在。

證明：令 $X=X_1 \cup \{\infty_1, \infty_2, \dots, \infty_7\}$ ，在 X_1 上建構一個 $KTS(15)$ ，然後將 ∞_i 加入於第 i 個平行族， $i=1,2,\dots,7$ ，而形成 5 個 4-子集，再將 ∞_i 放在一起形成一個 7-子集就可以建構出所要的 PBD。 ■

推理 6.4. 存在兩個互相垂直的等冪 22 階拉丁方陣。

證明：互相垂直的等冪 4 階與 7 階拉丁方陣皆存在，所以由定理 6.2，推論得證。(4 階的方陣，如圖 6.2)。 ■

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

0	3	1	2
2	1	3	0
3	0	2	1
1	2	0	3

圖 6.2

上述的推論顯然已經證明了尤拉猜測是錯誤的。值得在此說明的是，在 1959 年時 Bose 和 Shrikhande 並沒有用這簡潔的證明，他們用的 PBD 是 $B=[22;\{3,4,5\},1]$ ，但是因為互相垂直的等冪 3 階拉丁方陣並不存在，所以他們特別爲了這緣故做了一些修飾，在此不再贅述。

接下來看一般的狀況。

定理 6.5. 假如 $T[m,5;1]$ 及 $T[u,4;1]$ 存在， $u \leq m$ ，則 $T[3m+u,4;1]$ 存在。

證明： 令 $(P, G, \mathbf{B})$ 為一個 $T[m,5;1]$ ，其中 $G = \{G_1, G_2, \dots, G_5\}$ ， $U = \{x_1, x_2, \dots, x_u\} \subseteq G_5$ ，以及 $\pi_i = \{B \setminus \{x_i\} \mid x_i \in B \in \mathbf{B}\}$ 。再令 $P' = P \setminus G_5$ ， $G' = \{G_1, G_2, G_3, G_4\}$ 以及 $\mathbf{B}' = \{B \setminus G_5 \mid B \in \mathbf{B}\}$ ，則 $(P', G', \mathbf{B}')$ 為一個 $T[m,4;1]$ ，而且 $\pi_1, \pi_2, \dots, \pi_u$ 形成 $\mathbf{B}'$ 中的 u 個平行族。現在我們可以定義 $T[3m+u,4;1]$ 如下：

(i) $W = \{1, 2, 3\}$ ， $U^* = U \times \{1, 2, 3, 4\}$ ， $\tilde{P} = (W \times P') \cup (U \times \{1, 2, 3, 4\})$ 。

(ii) $\tilde{G} = \{(U \times \{i\}) \cup (W \times G_i) \mid i = 1, 2, 3, 4\}$ 。

(iii) 對於 π_i 中的每一個區組 $\{a, b, c, d\}$ ，令 $((\{x_i\} \times \{1, 2, 3, 4\})) \cup (W \times \{a, b, c, d\})$ ， $G^*, W(\{a, b, c, d\})$ 為一個截集設計 $T[4,4;1]$ ，其中 $G^* = \{(x_i, j)\} \cup (W \times \{x\}) \mid x \in \{a, b, c, d\} \cap G_j, j = 1, 2, 3, 4\}$ ，同時 $\{(x_i, 1), (x_i, 2), (x_i, 3), (x_i, 4)\} \in W(\{a, b, c, d\})$ 。令 $W(\{a, b, c, d\}) \setminus \{(x_i, 1), (x_i, 2), (x_i, 3), (x_i, 4)\}$ 為 $\tilde{\mathbf{B}}$ 的一部份。

(iv) 對於每個不在 $\pi_1 \cup \pi_2 \cup \dots \cup \pi_u$ 的區組 B ，令 $(W \times B, \{W \times \{x\} \mid x \in B\}, W(B))$ 為一個 $T[3,4;1]$ ，同時將這 9 個區組全部放在 $\tilde{\mathbf{B}}$ 中。

(v) 令 $(U \times \{1, 2, 3, 4\}, \{U \times \{i\} \mid i = 1, 2, 3, 4\}, \mathbf{B}^*)$ 為一個 $T[u,4;1]$ ，而且將 u^2 個區組放於 $\tilde{\mathbf{B}}$ 中。

如此一來， $(\tilde{P}, \tilde{G}, \tilde{\mathbf{B}})$ 為一個 $T[3m+u,4;1]$ 設計。

接下來就是核對的工作，在此省略細節。(作業) ■

定理 6.6. 對於所有不等於 2 或 6 的正整數 n ，皆存在兩個互相垂直的 n 階拉丁方陣。

證明：由第一章，除了 $n \geq 14$ 且 $n \equiv 2 \pmod{4}$ 的正整數之外，都已經可以找到互相垂直的 n 階拉丁方陣。現在 $n=14$ 可以直接建構出來，如圖 6.3，而剩下的 n 則可以參考下表，因此定理得證。 ■

n	m	u
$18k$	$6k-1$	3
$18k+2$	$6k-1$	5
$18k+4$	$6k+1$	1
$18k+6$	$6k+1$	3
$18k+8$	$6k+1$	5
$18k+10$	$6k+1$	7
$18k+12$	$6k+1$	9
$18k+14$	$6k+1$	11
$18k+16$	$6k+5$	1

12	7	0	6	4	2	11	9	13	5	3	1	10	8
1	11	10	4	5	6	13	8	9	0	7	12	2	3
2	1	11	0	7	12	3	4	5	6	13	8	9	10
10	9	8	1	2	3	4	5	6	13	0	7	12	11
7	0	12	3	1	10	8	6	4	2	11	9	13	5
3	2	1	13	8	9	10	11	0	7	12	4	5	6
5	4	3	10	11	1	2	0	7	12	6	13	8	9
13	6	5	2	3	4	0	7	12	8	9	10	11	1
9	8	13	5	6	0	7	12	10	11	1	2	3	4
11	10	9	8	0	7	12	1	2	3	4	5	6	13
0	12	7	11	9	13	5	3	1	10	8	6	4	2
4	3	2	7	12	5	6	13	8	9	10	11	1	0
6	5	4	12	13	8	9	10	11	1	2	3	0	7
8	13	6	9	10	11	1	2	3	4	5	0	7	12

12	13	4	10	7	0	1	9	6	3	11	8	5	2
9	8	10	5	6	7	4	13	12	11	1	2	3	0
5	0	6	7	8	9	10	11	1	2	3	4	13	12
6	5	7	1	2	3	0	4	13	12	8	9	10	11
4	12	13	6	3	11	8	5	2	10	7	0	1	9
1	11	2	9	10	4	13	12	3	0	5	6	7	8
0	3	5	2	4	13	12	6	7	8	9	10	11	1
7	6	8	4	13	12	9	10	11	1	2	3	0	5
10	9	11	13	12	1	2	3	0	5	6	7	8	4
2	1	3	12	0	5	6	7	8	9	10	11	4	13
13	4	12	3	11	8	5	2	10	7	0	1	9	6
8	7	9	11	1	2	3	0	5	6	4	13	12	10
11	10	1	0	5	6	7	8	9	4	13	12	2	3
3	2	0	8	9	10	11	1	4	13	12	5	6	7

圖 6.3 MOLS(14)

作業

1. 證明引理 6.1。
2. 核對定理 6.5 的正確性。

第四章 史坦納四元系

史坦納三元系 $\text{STS}(v)$ 存在的充要條件為 $v \equiv 1$ 或 $3 \pmod{6}$ ，同時也等價於一個完全圖 K_v 可以被分解成邊不重複出現的三角形。在擴展的方向，我們可以考慮分解的對象，由三角形 K_3 推展至 K_k ，即為區組大小為 k 的平衡不完全區組設計 BIBD，也可以由三角形 C_3 推展至 C_k ，即為圈長度皆為 k 的圈設計 (Cycle System)。當然，被分解的母圖亦可以由 K_v 改變為 λK_v 或是 $\lambda K_{m(n)}$ ，後者稱為是可分組設計 (GDD)。

另外，我們可以將完全圖推廣至均勻的超圖 (Uniform Hypergraph)，首先，我們先介紹超圖。

令 X 為一非空集合，則 (X, E) 稱為是定義於 X 的超圖，其中 $E \subseteq 2^X$ 。在 E 中的元素都有一樣大小時，此超圖也稱為是均勻的超圖。若是 $E = \binom{X}{t}$ (所有 t -子集所成的集合)，則 (X, E) 為一完全 t -均勻超圖，顯然 $|E| = \binom{|X|}{t}$ ，為了方便起見，我們用 $K_{|X|}^{(t)}$ 來表示這樣的圖，因此 $K_{|X|}^{(2)} = K_{|X|}$ 。現在，要考慮的分解是將 $\lambda K_{|X|}^{(t)}$ 分解成大小為 $k > t$ 的區組，使得任意的 t 個 X 中的元素皆出現在 λ 個區組中，這裡不難看出每個區組皆含有 $\binom{k}{t}$ 個 t -子集。這也是本章的主題。

1. t -設計

定義 1.1. 在一個 t -(v, k, λ)設計為一個序對 $(\mathbf{X}, \mathbf{B})$ ，其中 $|\mathbf{X}|=v$ ， $\mathbf{B}$ 中的區組大小皆為 k ，同時任意 $\mathbf{X}$ 中的 t 個元素皆包含於 λ 個 $\mathbf{B}$ 中的區組。

若 $t \geq 3$ 且 $\lambda = 1$ ，則不難看出，令 $x_0 \in \mathbf{X}$ ， $\mathbf{B}' = \{ B \setminus \{x_0\} \mid x_0 \in B, B \in \mathbf{B} \}$ ，則 $(\mathbf{X} \setminus \{x_0\}, \mathbf{B}')$ 為一個 $(t-1)$ -($v-1, k-1, 1$)設計。一般而言，以下的結果是可以想像得到的。

定理 1.2. 令 $(\mathbf{X}, \mathbf{B})$ 為一 t -($v, k, 1$)設計， $s < t$ ， $|S|=s$ ，且 $S \subseteq \mathbf{X}$ 。則 $(\mathbf{X} \setminus S, \mathbf{B}')$ 為一個 $(t-s)$ -($v-s, k-s, 1$)設計，其中 $\mathbf{B}' = \{ B \setminus S \mid B \in \mathbf{B} \}$ 。

證明：任意的 $t-s$ 個點與 S 合在一起會出現在唯一的一個區組，如果不去掉一些點，則 t 變小時， λ 會變大。 ■

定理 1.3. 令 $(\mathbf{X}, \mathbf{B})$ 為一 t -(v, k, λ)設計， $s < t$ ，則 $(\mathbf{X}, \mathbf{B})$ 亦為一個 s -(v, k, λ')設計，其中 $\lambda' = \lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$ 。

證明：令 S 為任一個具有 s 個點的集合，則再選 $t-s$ 個點與 S 組成一 個 t -集合的方法共有 $\lambda \binom{v-s}{t-s}$ ，然而，每個大小為 k 的區組可以提供 $\binom{k-s}{t-s}$ 個 $t-s$ 的子集合，所以 λ' 即可求得。

例如當 $v=10$ 時，一個 3 -($10, 4, 1$)設計可以是一個 2 -($10, 4, \lambda'$)設計，其中 $\lambda' = \frac{\binom{10-2}{3-2}}{\binom{4-2}{3-2}} = 4$ 。 ■

一般而言，當 $t \geq 3$ 時，要建構一個 t -設計並不容易，在下一節中，我們主要討論的對象是 $t=3$ 且 $k=4$ 的狀況。在這一節的最後，我們再

看一個問題：從定理 1.2，不難發現當 $t=3$ ， $k=4$ 及 $\lambda=1$ 時，只要去掉一點，即可得到一個 $t=2$ ， $k=3$ 及 $\lambda=1$ 的設計，這就是史坦納三元系。然而，反過來說，如果已知一個史坦納三元系，是否可以經由加一點，再加上一些四元子集合而獲得一個史坦納四元系呢？

定義 1.4. 如果一個史坦納三元系能經由一個史坦納四元系扣掉一點而建構出來，則此三元系又稱為是導出的史坦納三元系（Derived STS）。

問題. 是否每一個史坦納三元系都是一個導出的三元系？

到目前為止，除了一些具有特殊性質的史坦納三元系已經被證明是導出的三元系，一般而言，這是一個尚未解決的問題。在第三節中，我們會找到一類的導出三元系，讀者可以先試著去回答這問題（作業 2）。

作業

1. 試證任意的 $\text{STS}(7)$ ， $\text{STS}(9)$ 都是導出的史坦納三元系。
2. 試證當 $u=2v+1$ 時，而且一個 $\text{STS}(u)$ 包含有一個導出的子三元系 $\text{STS}(v)$ ，則此 $\text{STS}(u)$ 必定是一個導出的史坦納三元系。
3. 令 $(\mathbf{X}, \mathbf{B})$ 為一個 t -(v, k, λ) 設計，則我們可以定義一個圖 G 來對應於這個設計，其中 $V(G) = \mathbf{B}$ ， $E(G) = \{B_1 B_2 \mid B_1, B_2 \in \mathbf{B} \text{ 且 } B_1 \cap B_2 \neq \emptyset\}$ 。試討論圖 G 的性質：例如， G 是否有哈密爾頓圖？

2. 史坦納四元系的介紹

定義 2.1. 一個具有 v 個元素的史坦納四元系 $\text{SQS}(v)$ 為一個有序對 $(\mathbf{X}, \mathbf{B})$ ，其中 $|\mathbf{X}|=v$ ， $\mathbf{B}$ 為 $\mathbf{X}$ 中一些 4-子集所成的集合族，它滿足 $\mathbf{X}$ 中的任意 3 個元素必然會共同出現在 $\mathbf{B}$ 中的一個 4-子集中。

由定義，不難觀察出

引理 2.2. 一個 $\text{SQS}(v)$ 存在的必要條件為 $v \equiv 2$ 或 $4 \pmod{6}$ ，同時在 $\text{SQS}(v)$ 中有 $v(v-1)(v-2)/24$ 個區組。

引理 2.3. 令 $(\mathbf{X}, \mathbf{B})$ 為一個 $\text{SQS}(v)$ ，則對於 $\mathbf{X}$ 中的任一點 ∞ ， $(\mathbf{X} \setminus \{\infty\}, \mathbf{B}')$ 為一個 $\text{STS}(v-1)$ ，其中 $\mathbf{B}' = \{B \setminus \{\infty\} \mid B \in \mathbf{B} \text{ 且 } \infty \in B\}$ 。

在這裡順便說明兩類 $\text{SQS}(v)$ 。

定義 2.4. 一個 $\text{SQS}(v)$ 稱為是同調的史坦納四元系 (Homogeneous)，如果對於 $\mathbf{X}$ 中的任兩個元素 x_1, x_2 ，分別去掉 x_1, x_2 所得到的兩個史坦納三元系皆同構。

例如， $\text{SQS}(8)$ 就是這樣的一個例子。反過來，如果定義 2.4 中所提到的史坦納三元系兩兩皆不同構，則此 $\text{SQS}(v)$ 稱為是多變的史坦納四元系 (Heterogeneous)。這樣的例子就比較不容易找，但是它是存在的！

以下是一些 $\text{SQS}(v)$ 的例子。

例 1： $v=2^n$ ，令 $\mathbf{X}=(\mathbf{Z}_2)^n$ ， $\mathbf{B}=\{\{x,y,z,w\} \mid x,y,z,w \in (\mathbf{Z}_2)^n \text{ 且 } x+y+z+w=\vec{0}\}$

例 2： $v=10$ ，令 $\mathbf{X}=\mathbf{E}(\mathbf{K}_5)$ ， $\mathbf{B}=\{\{e_1, e_2, e_3, e_4\} \mid e_i \in \mathbf{E}(\mathbf{K}_5), i=1,2,3,4, \text{ 且 } <\{e_1, e_2, e_3, e_4\}> \text{ 導出圖 2.1 中的一個圖。}\}$

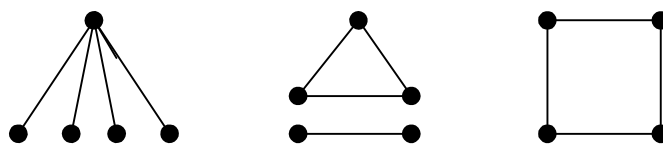


圖 2.1

例 3： $v=14$ ，令 $\mathbf{X}=\mathbf{Z}_7 \times \mathbf{Z}_2$ ， $\mathbf{B}_1=\{(0,0),(3,0),(0,1),(3,1)\}$ ，

$\mathbf{B}_2=\{(0,0),(3,0),(1,1),(5,1)\}$ ， $\mathbf{B}_3=\{(0,0),(3,0),(2,1),(6,1)\}$ ，

$\mathbf{B}_4=\{(0,0),(3,0),(2,0),(4,1)\}$ ， $\mathbf{B}_5=\{(0,0),(3,0),(4,0),(5,0)\}$ ，

$\pi_1((x,a))=(x+1,a)$ ， $\pi_2((x,a))=(2x,a)$ ， $\pi_3((x,a))=(-x,a+1)$ ，

這裡 $\pi_i: \mathbf{X} \rightarrow \mathbf{X}$ ， $i=1,2,3$ ，對於 $j=1,2,3,4,5$ ，令 $\mathbf{B}_j$ 為包含下列

區組的最小集合：(i) $\mathbf{B}_j \in \mathbf{B}_j$ ，(ii) 如果 $\mathbf{B} \in \mathbf{B}_j$ ，則 $\pi_i(\mathbf{B}) \in \mathbf{B}_j$ ，

$i=1,2,3$ 。於是 $(\mathbf{X}, \mathbf{B} = \bigcup_{j=1}^5 \mathbf{B}_j)$ 為所求的 $\text{SQS}(14)$ 。

例 3 提供了一種想法：先選定兩個集合，然後再選一些分別來自這兩個集合的元素來建構區組，這樣的構想當每一個集合的元素個數 $v \equiv 2$ 或 $4 \pmod{6}$ ，比較容易，而 $v \equiv 1$ 或 $5 \pmod{6}$ 時，則相當困難。

例 4：令 $(\mathbf{X}, \mathbf{B}_1)$ 為一個 $\text{SQS}(v)$ ，則 $(\mathbf{X} \times \mathbf{Z}_2, \mathbf{B})$ 為一個 $\text{SQS}(2v)$ ，

其中 $\mathbf{B}$ 的區組包含了下列的集合：

(i) 如果 $\{x,y,z,w\} \in \mathbf{B}_1$ ，則 $\{(x,0),(y,0),(z,0),(w,1)\}$ ， $\{(x,0),(y,0),(z,1),(w,0)\}$ ， $\{(x,0),(y,1),(z,0),(w,0)\}$ 及 $\{(x,1),(y,0),(z,0),(w,0)\} \in \mathbf{B}$ 。

(ii) 對於任意的 $x,y \in \mathbf{X}$ ， $\{(x,0),(y,0),(x,1),(y,1)\} \in \mathbf{B}$ 。

所以有了 $\text{SQS}(10)$ ， $\text{SQS}(14)$ 也就不難建構 $\text{SQS}(20)$ ， $\text{SQS}(28)$ 了。

定義 2.5. 一個 $\text{SQS}(v) (\mathbf{X}, \mathbf{B})$ 稱為是兩色(2-chromatic)史坦納四元系若且唯若 $\mathbf{X}$ 可以寫成兩個互斥子集 $\mathbf{X}_1$ 及 $\mathbf{X}_2$ 的聯集，使得對於任意的 $B \in \mathbf{B}$ ， $B \cap X_i \neq \emptyset$ ， $i=1,2$ 。

於是，我們不難發現例 3，例 4 所建構出來的 SQS 均為兩色史坦納四元系。對於任意的 $v \equiv 2$ 或 $4 \pmod{6}$ 是否皆存在兩色 $\text{SQS}(v)$ ，目前仍是一個尚未解決的問題。

問題：

*(1) 是否每一個 $\text{SQS}(v)$ 皆為兩色的 $\text{SQS}(v)$ ？

*(2) 對於任意的 $v \equiv 2$ 或 $4 \pmod{6}$ ，是否皆可建構出一個兩色的 $\text{SQS}(v)$ ？

作業

1. 試驗證本節所舉的例子皆為史坦納四元系。
- (*)2. 試模仿例 3，建構一個兩色SQS(22)。
- (*)3. 試建構一個SQS(16)，使得在這個SQS(16)中包含一個子集合族，它們形成一個BIBD， $k=4$ 及 $\lambda=1$ 。(這樣的(4,2)-設計也稱為是懸掛設計(Spanning Design))

3. 兩倍式建構法 (Doubling Construction)

在上一節例 4 所建構的 $\text{SQS}(2v)$ 雖然來自一個 $\text{SQS}(v)$ ，然而在建構出 $\text{SQS}(2v)$ 之後，原來的 $\text{SQS}(v)$ 已經不復存在。在這一節中，我們介紹另一種可以保持原 $\text{SQS}(v)$ 的建構法。用組合數學的術語也可以說是將小的 $\text{SQS}(v)$ 嵌入於大的 $\text{SQS}(2v)$ 中。

引理 3.1. 令 (X, B) 為一個 $\text{SQS}(v)$ ，若它嵌入於一個 (X', B') 的 $\text{SQS}(u)$ 中，則 $u \geq 2v$ 。

證明：如圖 3.1 所示，首先固定 ∞, ∞' ，它們分別為 X 及 $X' \setminus X$ 的元素。再考慮 3-子集 $\{\infty, \infty', x\}$ ，其中 $x \in X \setminus \{\infty\}$ ，則此 3-子集必定包含於 B' 中的一個區組 B ；由於 (X, B) 為一個 $\text{SQS}(v)$ ，則此區組 B 不能包含 3 個 X 中的元素及一個 $X' \setminus X$ 的元素，所以 $B = \{\infty, \infty', x, \pi(x)\}$ ， $\pi(x) \in X' \setminus X$ ，顯然 π 為一個由 $X \setminus \{\infty\}$ 對應至 $(X' \setminus (X \cup \{\infty'\}))$ 的 1-1 函數，所以 $2|X| \leq |X'|$ 。 ■

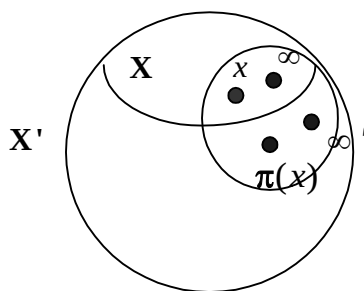


圖 3.1

由於以下的建構需要利用到一個圖的 1-分解(1-factorization)，在此先介紹這種分解的存在性。

一個圖的 1-因子 (1-factor) 即為該圖的完全配對 (Perfect Matching)，所以對於有奇數個點的圖是沒有必要討論它的存在性。而具有偶數個點的圖，完全配對的存在性可以利用一個簡單的演算法來判斷出來 (？)。然而，一個正則圖是否可以分解成 1-因子就沒有那麼容易判斷了。以下是一個著色的猜測。

1-分解猜測 (1-factorization Conjecture)

令 G 為具有 $2m$ 個點的 k -正則圖。則當 $k \geq m$ 時， G 可以 1-分解。

這個猜測已經獲得一些部份的結果，但是尚未完全解決，而它的極端狀況 $k=2m-1$ 則是家喻戶曉的知名結果。以下我們除了一般所熟悉的證明方法之外，另外提供一個可以參考的概念。

引理 3.2. K_{2m} 具有 1-分解。

證明：(證明 1) 令 $V(K_{2m}) = Z_{2m}$ ， $F_1 = \{\{0,1\}, \{2,2m-1\}, \{3,2m-2\}, \dots, \{m,m+1\}\}$ ，如圖 3.2 所示，則 $F_2, F_3, \dots, F_{2m-1}$ 可以由旋轉的方式求得。

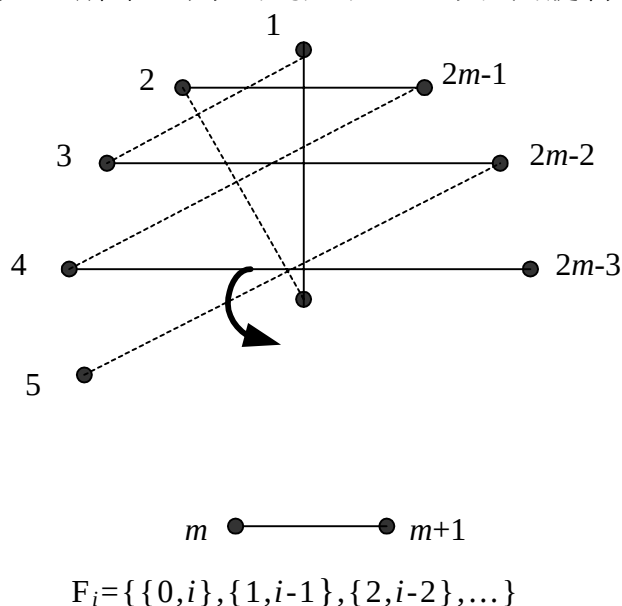


圖 3.2

(證明 2)

(i) $m \equiv 1$ 或 $2 \pmod{3}$

令 $v=2m-1$ ，則 $v \equiv 1$ 或 $3 \pmod{6}$ ，因此 $\text{STS}(v)$ 存在，令此 $\text{STS}(v)$ 為 (S, t) ，其中 $S = \{1, 2, \dots, 2m-1\}$ ，則 K_{2m} 的 1-分解 $\{F_1, F_2, \dots, F_{2m-1}\}$ 可以求得，其中 $F_i = \{\{0, i\}, \{x, y\} \mid \{i, x, y\} \in t\}$ 。

(ii) $m \equiv 0 \pmod{3}$

令 $v=2m-1$ ，則 $v \equiv 5 \pmod{6}$ 。因此 $B(K, 1)$ 存在， $K = \{3, 5\}$ 。同時在這個 PBD 中只有一個區組它具有 5 個元素，令它們為 x_1, x_2, x_3, x_4, x_5 ，則同理可以求得 $\{F_1, F_2, \dots, F_{2m-1}\}$ ，其中對於 $1 \leq i \leq 5$ ，

$$F_1 = \{\{0, x_1\}, \{x_2, x_5\}, \{x_3, x_4\}, \{y, z\} \mid \{x_1, y, z\} \in \mathbf{B}\}$$

$$F_2 = \{\{0, x_2\}, \{x_1, x_3\}, \{x_4, x_5\}, \{y, z\} \mid \{x_2, y, z\} \in \mathbf{B}\}$$

$\vdots$

$$F_5 = \{\{0, x_5\}, \{x_1, x_4\}, \{x_2, x_3\}, \{y, z\} \mid \{x_5, y, z\} \in \mathbf{B}\}$$

其他與 (i) 的 1-因子求法相同。 ■

證明 2 顯然是要仰賴設計的存在性，然而，它也說出了它們之間的關聯性。

定理 3.3. (兩倍式建構法) 令 $(\mathbf{X}, \mathbf{B})$ 為一個 $\text{SQS}(v)$ ，則必存在一個 $\text{SQS}(2v)$ ，它包含兩個互斥的 $\text{SQS}(v)$ 。

證明： 令 $\mathbf{X} = Z_v$ ， $\tilde{\mathbf{X}} = v + Z_v$ ， $\mathbf{F} = \{F_1, F_2, \dots, F_{v-1}\}$ 與 $\tilde{\mathbf{F}} = \{\tilde{F}_1, \tilde{F}_2, \dots, \tilde{F}_{v-1}\}$ 分別為 K_v 及 $\tilde{K}_v$ 的 1-分解，其中 $V(K_v) = Z_v$ ， $V(\tilde{K}_v) = v + Z_v$ 。則 $(\mathbf{X}', \mathbf{B}')$ 為所求的 $\text{SQS}(2v)$ (?) (作業)，其中 $\mathbf{X}' = \mathbf{X} \cup \tilde{\mathbf{X}}$ ， $\mathbf{B}'$ 的區組為：

(i) $\mathbf{B}$ 中的區組，

(ii) 若 $B \in \mathbf{B}$ ，則 $v+B \in \mathbf{B}'$ ，以及

(iii) 對於所有的 $i=1,2,\dots,v-1$ ，若 $\{x,y\} \in F_i$ ， $\{x',y'\} \in \tilde{F}_i$ ，則 $\{x,y, x',y'\} \in \mathbf{B}'$ 。

上述定理的建構方式可以再略作改變：在第(iii)類的區組，我們不一定要選 F_i 及 $\tilde{F}_i$ 的邊來形成區組，取而代之的是 F_i 及 $\tilde{F}_{\alpha(i)}$ 的搭配，這裡的 α 是 $\{1,2,\dots,v-1\}$ 的一個排列即可。於是，利用上述的方法所建構出來的 $\text{SQS}(2v)$ 就會有很多不同的四元系。如果再加上 1-分解本身也有很多不同的選擇，可想而知，不同的 $\text{SQS}(2v)$ 之個數在 v 大一點的時候，已是一個天文數字了。但究竟有多少呢？

定義 3.4. (同構的SQS) 兩個 $\text{SQS}(v)$ ， $(\mathbf{X}_1, \mathbf{B}_1)$ 及 $(\mathbf{X}_2, \mathbf{B}_2)$ ，稱為同構的 $\text{SQS}(v)$ 若且唯若存在一個 1-1 且映成的函數 $\alpha: \mathbf{X}_1 \rightarrow \mathbf{X}_2$ 使得對於任意的 $\{x,y,z,w\} \in \mathbf{B}_1$ 等價於 $\{\alpha(x), \alpha(y), \alpha(z), \alpha(w)\} \in \mathbf{B}_2$ 。

截至目前，研究這方面的成果並不多；令 $N(v)$ 代表彼此不同構之 $\text{SQS}(v)$ 的個數，則在 $v \leq 10$ 時， $N(v)=1$ ， $N(14)=4$ ，其它的就不清楚了。對了，有一個上界很值得一提，它是由 Doyen 及 Vandensavel 所證明的。(log x 以 10 為底)

定理 3.5. $\log N(v) \leq \frac{v^3}{24} \log v [1 + o(1)]$ 。

在下界的部份，Lenz 證明了下面這個出色的結果。

定理 3.6. $\log N(v) > \frac{v^3}{24}$ 。

不同構的 SQS 已經有那麼多了，不一樣的 SQS 就不必再提了。儘管如此，要建構一個 $\text{SQS}(v)$ ， $v \equiv 2$ 或 $10 \pmod{12}$ ，仍然是非常困難，我們把這工作留至下一節。在這裡附帶說明導出三元系的存在問題。由於有了兩倍式建構四元系的方法，第一節作業 2 所提的結果就可以順利地證明出來。

定理 3.7. 一個 $\text{STS}(2v+1)(\mathbf{X}', \mathbf{B}')$ ，如果它包含了一個導出的子三元系 $\text{STS}(v)(\mathbf{X}'', \mathbf{B}'')$ ，則它本身是一個導出的三元系。

證明： 令 $\mathbf{X} = \mathbf{X}' \cup \{\infty\}$ ，而且 $(\mathbf{X}'' \cup \{\infty\}, \tilde{\mathbf{B}})$ 為一 $\text{SQS}(v+1)$ ，它可以去掉 ∞ 之後得到 $(\mathbf{X}'', \mathbf{B}'')$ 。由於 $(\mathbf{X}', \mathbf{B}')$ 是一個 $\text{STS}(2v+1)$ ，所以分別去掉 $\mathbf{X}''$ 中的點可以獲得以 $\mathbf{X}' \setminus \mathbf{X}''$ 為點集合所定義完全圖的 1-分解。令此 1-分解為 $\{\tilde{\mathbf{F}}_1, \tilde{\mathbf{F}}_2, \dots, \tilde{\mathbf{F}}_v\}$ 。然後令 $\{\mathbf{F}_1, \mathbf{F}_2, \dots, \mathbf{F}_v\}$ 為定義於 $\mathbf{X}'' \cup \{\infty\}$ 的完全圖之 1-分解。現在，利用兩倍式的建構法即可獲得一個 $\text{SQS}(2v+2)$ ，它的區組除了來自兩個 1-分解之外，還包括了 $\tilde{\mathbf{B}}$ 及 $v + \tilde{\mathbf{B}} = \{\{v+x, v+y, v+z, v+w\} \mid \{x, y, z, w\} \in \tilde{\mathbf{B}}\}$ 。顯然，這時候從 $\text{SQS}(2v+2)$ 中去掉 ∞ 之後而得的 $\text{STS}(2v+1)$ ，即為已知的史坦納三元系。

作業

1. 驗證定理 3.3 所建構的設計的確是一個 $\text{SQS}(2v)$ 。
- ^(*)2. 建構兩個不同構的 $\text{SQS}(16)$ ？
3. 由定理 3.3 所建構出來的 $\text{SQS}(2v)$ 是否為兩色的 $\text{SQS}(2v)$ ，說明理由？

4. SQS(v)存在的充分條件

爲了證明 $\text{SQS}(v)$ 對於所有的 $v \equiv 2$ 或 $4 \pmod{6}$ 皆存在，利用直接建構 $\text{SQS}(6k+2)$ ， $\text{SQS}(6k+4)$ 或遞迴建構 $v \rightarrow 2v$ ， $v \rightarrow 2v+6$ 是最早被想到的幾種建構方式，前兩者自然可以回答存在性的問題，而且也非常漂亮，就像證明所有的 $u \equiv 1$ 或 $3 \pmod{6}$ ， $\text{STS}(u)$ 存在的方式一樣；然而，這兩種想像中的漂亮方法，無一成功，至少到目前爲止尚未看到答案。另外兩個遞迴建構的方式也來自簡單的觀察，當然 $\text{STS}(u)$ 也有類似的建構方法，即 $u \rightarrow 2u+1$ 及 $u \rightarrow 2u+7$ ；但不同的是， $v \rightarrow 2v$ 得來並不困難，可是 $v \rightarrow 2v+6$ 到目前爲止卻是方法全無，所以無庸置疑的這個建構方式是最被人期待的一個。

問題：證明一個 $\text{SQS}(v)$ 可以嵌入於一個 $\text{SQS}(2v+6)$ 中。

雖然上述幾個比較直接的方法沒有獲得答案，但在 1960 年左右，Hanani 用了比較多的建構，將它們組合起來而證明了下面的定理。

定理 4.1. $\text{SQS}(v)$ 存在的充要條件爲 $v \equiv 2$ 或 $4 \pmod{6}$ 。

證明：(摘要) 首先，他提出 6 個遞迴建構：(A) $v \rightarrow 2v$ ，(B) $v \rightarrow 3v-2$ ，(C) 對 $v \equiv 2 \pmod{12}$ ， $v \rightarrow 3v-8$ ，(D) 對 $v \equiv 10 \pmod{12}$ 時， $v \rightarrow 3v-4$ ，(E) $v \rightarrow 4v-6$ 及 (F) $v \rightarrow 12v-10$ 。然後，再加上 $\text{SQS}(14)$ 及 $\text{SQS}(38)$ 這兩個自己的大一點之 $\text{SQS}(v)$ ，他證明了這個定理。 ■

由於這個結果整體而言並不漂亮，後來 Hanani 又再另證了一次，也用到比較深入的概念，尤其更引進了 3-GDD 的概念，亦即將 GDD 推展至討論任意 3 點出現的狀況，但是取代 (E) 及 (F) 是另外兩個相去不遠的建構，其中一個是 $v \rightarrow 6v-10$ 。

既然，兩倍式的建構 $v \rightarrow 2v+6$ 辦不到，三倍式的建構是否就足以建構出所有的 $\text{SQS}(v)$ 呢？這個答案不久由 Hartman 獲得了肯定的答案，他證明了以下的結果。

定理 4.2. 如果一個 $\text{SQS}(v)$ 包含了一個 $\text{SQS}(u)$ ， $v > u$ ，則必定存在一個 $\text{SQS}(3v-2u)$ ，它包含了 $\text{SQS}(v)$ 為它的一個子四元系。

我們不難看出（作業），定理 3.3 及 4.2 證明了定理 4.1。然而要了解 Hartman 的證明絕非易事。幸運的是，定理 4.2 在 Stern 及 Lenz 的引理協助下，簡化了許多，以下所介紹的方法就是經過簡化之後的結果。至於 Stern 和 Lenz 的引理請參考第二章。

證明：（Lenz 的證明方法）

（摘要）令 $V = \{1, 2, \dots, v\}$ ， $V' = \{v-u+1, v-u+2, \dots, v\}$ ，同時 (V, B) 及 (V', B') 分別為 $\text{SQS}(v)$ 及 $\text{SQS}(u)$ 。令 $V'' = \{\infty_1, \infty_2, \dots, \infty_u\} \cup (\{1, 2, \dots, v-u\} \times \{1, 2, 3\})$ ，則 $|V''| = 3v-2u$ 。為了方便說明，令 $g = v-u$ ，且對於 $i=1, 2, 3$ ，定義 (a, i) ， $1 \leq a \leq g$ ，

$$\varphi_i(a) = \begin{cases} \infty_{a-g}, & g+1 \leq a \leq v \end{cases}$$
 所以，對於 $1 \leq a \leq g$ ，一個 a 將對應 3 個元素 $(a, 1)$ ， $(a, 2)$ 及 $(a, 3)$ ，而當 $a > g$ 時， $\varphi_1(a) = \varphi_2(a) = \varphi_3(a) = \infty_{a-g}$ 。現在，我們先定義 5 類的區組，最後再證明前 4 類在 $v \not\equiv u \pmod{6}$ 的情況下合起來是一個 $\text{SQS}(3v-2u)$ ，而在 $v \equiv u \pmod{6}$ 的情況下，則需要綜合全部 5 類所定義出來的區組。

(i) $Q_1 = \{\{\varphi_i(x), \varphi_i(y), \varphi_i(z), \varphi_i(w) \mid \{x, y, z, w\} \in B, 1 \leq i \leq 3\}\}$ 。

(ii) $Q_2(a, l) = \{\{\infty_l, (x, 1), (y, 2), (z, 3) \mid x+y+z \equiv a \pmod{g}\}\}$ ，其中 $0 \leq a \leq g-1, 1 \leq l \leq u$ 。

(iii) 對於 $1 \leq d < g$, $d \neq g/2$ 以及 $\{a_1, a_2, a_3\}$ (multi-set) $\subseteq \{0, 1, \dots, g-1\}$,

$$Q_3(a_1, a_2, a_3; d) = \{ \{(x, i), (x+d, i), (y, i+1), (z, i+2)\} \mid 1 \leq i \leq 3, x+y+z \equiv a_i \pmod{g} \} \text{ (第一座標 mod } g, \text{ 第二座標 mod } 3)。$$

(iv) 對於 $g/2 \in D \subseteq \{1, 2, \dots, g/2\}$, 令 $G(D, g)$ 的 1-分解為 $\{F_1, F_2, \dots, F_t\}$

$$Q_4(D) = \{ \{(x, i), (y, i), (z, j), (w, j)\} \mid 1 \leq i < j \leq 3, \{x, y\} \in F_k, \{z, w\} \in F_k, 1 \leq k \leq t \}。$$

(v) 在這一類中, $g \equiv 0 \pmod{6}$, 對於所有的 $1 \leq a \leq g$ 及不等於 $g/2$ 的 $1 \leq d < g$, 在 $a \not\equiv 0 \pmod{3}$ 及 $a \equiv d \pmod{3}$ 的情況下, 令 $Q_5'(a, d) = \{ \{(x, i), (x+d, i), (y, i+1), (z, i+2)\} \mid 1 \leq i \leq 3, y \equiv z \pmod{3}, x+y+z \equiv a \pmod{g} \}$, $Q_5''(a, d) = \{ \{(x, i), (x+d, i), (y, j), (y+d, j)\} \mid 1 \leq i \leq 3, x \equiv y \pmod{3} \}$, 以及 $Q_5(a, d) = Q_5'(a, d) \cup Q_5''(a, d)。$

由於核對的工作比較複雜, 在此省略。 ■

接下來**證明定理 4.1.**(利用定理 3.3 及 4.2), 即對於所有的 $w \equiv 2$ 或 $4 \pmod{6}$, $SQS(w)$ 存在。

- (1) 當 $w < 16$, $SQS(w)$ 存在(例子)。
- (2) 當 $16 \leq w \leq 38$, $SQS(w)$ 存在, 而且都包含一個子四元系 $SQS(8)$, (可以直接建構, 在此略去)。
- (3) 當 $w \equiv 4$ 或 $8 \pmod{12}$ 時, 利用 $v \rightarrow 2v$ 建構法, 同時可以保證它包含一個子四元系 $SQS(8)$ 。
- (4) 當 $w \equiv 10$ 或 $22 \pmod{36}$ 時, 利用 $v \rightarrow 3v-2$ ($u=1$), 它也包含一個 $SQS(8)$ (?)。($v \equiv 4$ 或 $8 \pmod{12}$)。
- (5) 當 $w \equiv 14, 26$ 或 $34 \pmod{36}$, 則 $w \geq 50$, 分別利用 $u=8, 2$ 或

4 及 $3v-2u$ 來建構 $SQS(w)$ ，此時 $v \equiv 22 \pmod{36}$ (14,26) 或是 $v \equiv 26 \pmod{36}$ (34)。

(6) 當 $w \equiv 2 \pmod{36}$ 時， $w \geq 74$ ，此時 $v \equiv u = 2$ 即可。

由於(1)~(6)涵蓋所有可能的情況，定理得證。 ■

爲了對此定理有更進一步的了解，以下是幾個例子：

例 1. $w=58$ ，令 $v=20$ ， $u=1$ 。($SQS(1)$ 可以看成是存在的四元系)。

例 2. $w=230$ ，令 $v=82$ ， $u=8$ 。

例 3. $w=110$ ，令 $v=38$ ， $u=2$ 。

作業

1. 試驗證利用 Hanani 的 6 種建構法及較小的 $\text{SQS}(v)$ ， $v \leq 38$ ，定理 4.1 即可被證明。
2. 試驗證定理 4.2 中所有的區組數是正確的。
- (***)3. 直接建構法 $6k+2$ ， $6k+4$ 是否存在？
- (***)4. $v \rightarrow 2v+6$ 可以辦到嗎？

第五章 圈系

前面已經提到過，在選擇分解對象時， K_3 可以看成 C_3 ，於是，就一般而言，是否可以將一個圖分解成一樣大小的 C_k 呢？如果可以的話，充要條件是什麼呢？

定義 0.1. 圈系 (Cycle System)

如果 λK_n 可以分解成 C_k 所成的集合，記為 $C_k \mid \lambda K_n$ ，則我們稱一個 k -圈系，或 (n, k, λ) -圈系存在。

引理 0.2. 一個 (n, k, λ) -圈系存在的必要條件為 (i) $\lambda(n-1)$ 是偶數，及(ii) $\lambda n(n-1)$ 為 $2k$ 的倍數。

證明：第一個條件來自每個點被一個圈通過時每次用掉兩度；而第二個條件是總邊數必須是 k 的倍數。 ■

和一般設計的問題一樣，我們關心的是引理 0.2 的必要條件是否也是充分條件？在這一章中，我們將試著去回答這個問題，當然， $k=3$ 的情況在第二章中已詳細說明，所以我們從 $k=4$ 開始。

1. 4-圈系

4-圈系又稱為是四邊形系 (Quadrangle System)，是一個簡單卻結果漂亮的系統。首先，我們需要一些簡單的引理。

引理 1.1. $C_4 \mid K_{2n_1, 2n_2}$ ， n_1, n_2 為自然數。

引理 1.2. $C_4 \mid K_9$ 。

證明：令 $(0,1,5,2)$ 為一圈，則 $\{i + (0,1,5,2) \mid i \in \mathbb{Z}_9\}$ 為所求的分解。 ■

引理 1.3. $C_4 \mid 2K_{2n_1, n_2}$ ， $n_1, n_2 (>1)$ 為自然數。

引理 1.4. $(n, 4, \lambda)$ -圈系存在的必要條件為

- (i) $\lambda \equiv 1$ 或 $3 \pmod{4}$ 時， $n \equiv 1 \pmod{8}$ ，
- (ii) $\lambda \equiv 2 \pmod{4}$ 時， $n \equiv 0, 1, 4, 5 \pmod{8}$ ，以及
- (iii) $\lambda \equiv 0 \pmod{4}$ 時， n 為任意大於 3 的正整數。

定理 1.5. $(n, 4, \lambda)$ -圈系存在的充要條件為 (i) $2 \mid \lambda(n-1)$ 及

(ii) $k \mid \lambda \binom{n}{2}$ 。

證明：我們僅證明 $(n, 4, 1)$ -圈系的存在性，可以保證 $(n+8, 4, 1)$ -圈系的存在性，也就是所謂的 $n+8$ 建構法，剩下的部分留為作業。由於 $C_4 \mid K_{8, n-1}$ (引理 1.1)，利用圖 1.1，即可獲得所需要的 $(n+8, 4, 1)$ -圈系。

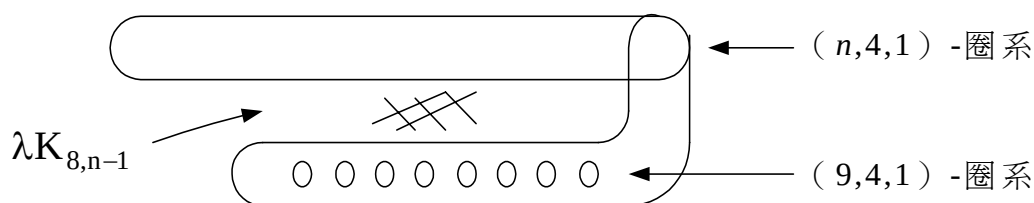


圖 1.1

接下來是一些小的 4-圈系。

(1) $n=4$ ， $\lambda=2$ ， $\{(0,1,3,2), (0,3,1,2), (0,1,2,3)\}$ 。

(2) $n=5$, $\lambda=2$, $\{(0,1,3,2)+i \mid i \in \mathbb{Z}_5\}$ 。

(3) $n=6$, $\lambda=4$, (作業) 。

(4) $n=7$, $\lambda=4$, (作業) 。

(5) $n=8$, $\lambda=2$, 由(1)及引理 1.1 即可求得。 ■

從上面的建構方式，不難看出要把一個 4-圈系嵌入於另一個較大的 4-圈系並不困難，而且不需要比兩倍大。

推論 1.6. 一個 $(n,4,1)$ -圈系可以嵌入於一個 $(m,4,1)$ -圈系，若且唯若 $m > n$ 。

推論 1.7. 一個 $(n,4,2)$ -圈系可以嵌入於一個 $(m,4,2)$ -圈系，若且唯若 $m > n+1$ 。

證明：因為 $n, m \equiv 0, 1, 4, 5 \pmod{8}$ ，所以 $m \geq n+3$ ，亦即 $m-n \geq 3$ 。利用相似於 $n \rightarrow n+8$ 的概念，可以證明當 n 或 m 為奇數的情況，而當 m, n 皆為偶數時，則利用圖 1.2 加以證明。 ■

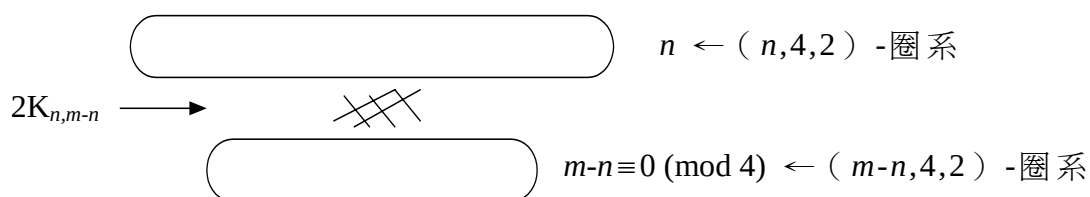


圖 1.2

對於所有的 n , $n \not\equiv 1 \pmod{8}$ ，我們討論 K_n 中究竟最多可以拿出幾個 C_4 ，如同第二章的概念，這稱之為最大裝填 (Maximum Packing)。於是，剩下的也就最少 (Minimum Leave)。對應的情況下，討論加入最少的邊 (Minimum Padding) 使得加完之後的新圖可以分割成 C_4 的

集合，這是最小覆蓋（Minimum Covering）。

定理 1.8. 在 λK_n 的裝填中，最小的殘留如下表所示：

$\begin{smallmatrix} n \\ \lambda \end{smallmatrix}$	0	1	2	3	4	5	6	7
1	F	ϕ	F	C_3	F	E_6	F	C_5
2	ϕ	ϕ	E_6	E_6	ϕ	ϕ	E_6	E_6
3	F	ϕ	F_2	C_5	F	E_6	F_2	C_3
4	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ

$$\lambda \pmod{4}, n \pmod{8}, n \geq 4$$

F：1-因子。 F_2 ：奇圖，具有 $n/2+2$ 個邊。 E_6 ：偶圖，具有 2 邊或 6 邊。

圖 1.3

證明：整體而言，證明雖瑣碎但並不難，以下用 $n \equiv 5 \pmod{8}$ ， $\lambda=1$ 爲例子，說明證明技巧。首先，當 $n=5$ 時，可以直接從 K_5 中選一個 C_4 ，剩下的爲 E_6 。現在考慮 $n>5$ ，如圖 1.4 如示， $n-5 \equiv 0 \pmod{8}$ 。

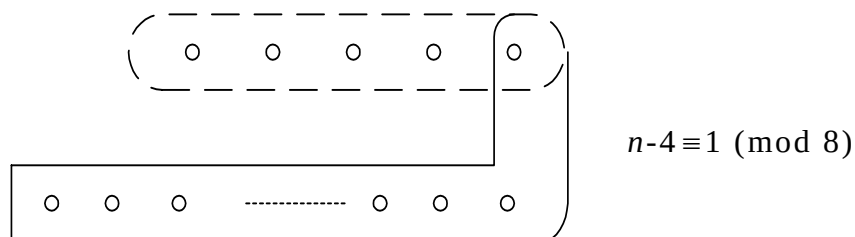


圖 1.4

因爲 $n-4 \equiv 1 \pmod{8}$ ，所以存在一個 $n-4$ 個點的 4-圈系，利用 $K_{4,n-5}$ 的分割再拿出 A 中的一個 C_4 即剩下 E_6 ，它是一個領結狀的圖，由兩個有一

交點的三角形所形成。如果規定 E_6 為 C_6 或兩個互斥的三角形，我們也可以利用圖 1.5 求得。(在 $K_{4,n-5}$ 的分割中選一個特定的 C_4 ，再回去 K_5 中剩下的 E_6 ，再重新分割即可。)

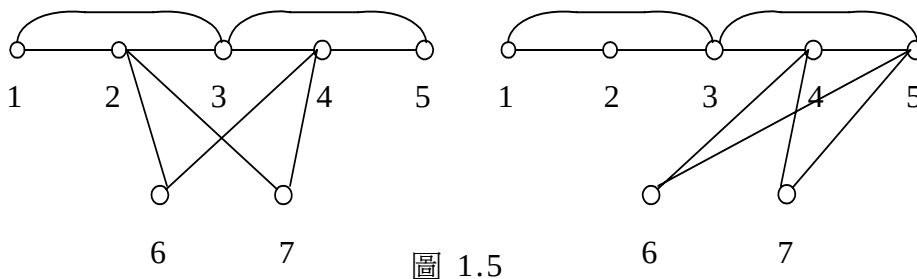


圖 1.5



至於覆蓋的討論，則可以利用定理 1.7 所得到的殘留 (Leave) 而得到答案，例如當殘留為 C_3 時，則補進去的 (Padding) 為 C_5 (如圖 1.6)，殘留為 E_6 時補進去的為 D ()，至於殘留為 F 時，補進去的不是 F 就是 F_2 。(?)

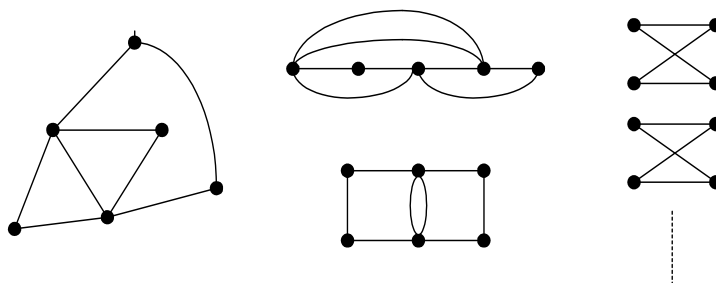


圖 1.6

最後，考慮 $\lambda K_{m(n)}$ 的分割，由於證明較複雜，在此只敘述它的內容。

定理 1.9. 在 $\lambda K_{m(n)}$ 的裝填中，最小的殘留如下：(n 為偶數時，殘留是 ϕ 。)

$\begin{matrix} m \\ \lambda \end{matrix}$	0	1	2	3	4	5	6	7
1	F	ϕ	$F(n \equiv 1(\bmod 4))$ $F_2(n \equiv 3(\bmod 4))$	C_3	F	E_6	$F(n \equiv 1(\bmod 4))$ $F_2(n \equiv 3(\bmod 4))$	C_5
2	ϕ	ϕ	E_6	E_6	ϕ	ϕ	E_6	E_6
3	F	ϕ	$F_2(n \equiv 1(\bmod 4))$ $F(n \equiv 3(\bmod 4))$	C_5	F	E_6	$F_2(n \equiv 1(\bmod 4))$ $F(n \equiv 3(\bmod 4))$	C_3
4	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ

n 為奇數， $\lambda \pmod{4}$ ， $m \pmod{8}$

圖 1.7

作業

1. 試求在 λK_n 的覆蓋之最小的補丁。
2. 證明當 n 為奇數， $m \equiv 1 \pmod{8}$ 時，對於所有的 λ ， $C_4 \mid \lambda K_{m(n)}$ 。
3. 證明定理 1.5。
4. 證明定理 1.8 中， $\lambda=1$ 的所有情況。

2. 5-圈系 (Pentagon System)

在這一節，我們討論 $C_5 \mid K_n$ 的充要條件。首先，看一個 $n=11$ 的例子。令 $V(K_{11})=Z_{11}$ ， $P=\{(1+i,3+i,9+i,5+i,4+i) \mid i \in Z_{11}\}$ ；另外 $n=5$ 則很容易看出來。

定理 2.1.[A. Rosa,1966] $C_5 \mid K_n$ 的充要條件為 $n \equiv 1$ 或 $5 \pmod{10}$ 。

證明：必要條件的部份可以由點的度數及 K_n 的邊數看出來，而充分條件的部份可以由以下的兩個直接建構法獲得證明。

(1) $10k+5$ 的建構法

對於 $1 \leq i \leq 5$ ，令 L_i 為任意的 $2k+1$ 階等冪對稱拉丁方陣。現在令 $S=Z_{2k+1} \times Z_5$ ，而 P 為下列兩類型 5-圈 (C_5) 的集合：

(i) $\forall x \in Z_{2k+1}$ ， $((x,0),(x,1),(x,2),(x,3),(x,4))$ 及 $((x,0),(x,2),(x,4),(x,1),(x,3))$ 為 P 中的 5-圈。

(ii) $\forall x \neq y \in Z_{2k+1}$ ， $((x,i),(y,i),(x,i+1),(L_4(x,y),i+3),(y,i+1)) \in P$ ，其中 $i \in Z_5$ ，第二分量取 5 的同餘。

(2) $10k+1$ 的建構法

對於 $1 \leq i \leq 5$ ，令 L_i 為任意的 $2k$ 階具有 2^k 形式洞的對稱拉丁方陣。現在，令 $S=\{\infty\} \cup (Z_{2k+1} \times Z_5)$ ，而 P 為下列兩類型 5-圈的集合：

(i) 當 $\{x,y\}$ 為 L_i 的一個洞時，在 $S=\{(x,i),(y,i) \mid i \in Z_5\} \cup \{\infty\}$ 上定義一個 5-圈系，可參考上面的例子。

(ii) 當 $\{x,y\}$ 不是洞的時候，5-圈的定義方式與 $10k+5$ 建構法的(ii)

一樣。

就這樣，上述的兩個直接建構法可以建構出所有的 5-圈系。詳細的核對在此省略。

接下來，我們探討 5-圈系的嵌入問題。

定義 2.2. 我們稱 (V, P) 為具有大小為 m 的洞之 5-圈系，如果 $K_{|V|} - K_m$ 可以被分割成 5-圈所成的集合，亦即 $C_5 \mid K_{|V|} - K_m$ 。

引理 2.3. 令 $|V|=n$ ，則 $C_5 \mid K_n - K_m$ 的必要條件為 (i) $5 \mid \binom{n}{2} - \binom{m}{2}$ ，(ii) n 是奇數而且 m 也是奇數，及 (iii) $\binom{n-m}{2} \geq \frac{1}{4}mn$ 。

證明：(i)及(ii)為明顯的必要條件，而(iii)則來自 5-圈的特性，所有連接洞裡與洞外點的邊都必須被用完，然而，這些來自二分圖型式的邊無法形成奇數圈，因此至少要有一邊來自洞外兩點連接的邊，於是有了(iii)這個不等式。 ■

定理 2.4. $C_5 \mid K_n - K_m$ 的充要條件為 (i) $5 \mid \binom{n}{2} - \binom{m}{2}$ ，(ii) n, m 為奇數及 (iii) $\binom{n-m}{2} \geq \frac{1}{4}mn$ 。

這個結果數年前由 Bryant 及 Rodger 兩人合力證明出來，請參考 JCD(2)，253-271，他們的結果甚至可以解決當 m 為奇數的情況。

推論 2.5. 一個 $5CS(m)$ 可以嵌入於一個 $5CS(n)$ 的充要條件為

$$\binom{n-m}{2} \geq \frac{1}{4}mn。$$

證明：定理 2.4 中的前面兩個條件皆因 $n, m \equiv 1$ 或 $5 \pmod{10}$ 而成立。

3. Alspach 的問題

由於圈在圖的分割中扮演很重要的角色，如何把一個圖分割成圈族一直是熱門話題。如果我們不限制圈的大小，最出名的結果當然是尤拉圖的分割。

定理 3.1. (尤拉) 一個連通圖 G 是尤拉圖和下面兩個敘述等價：

- (i) G 的每一點度數都是偶數。
- (ii) $E(G)$ 可以分割成沒有共用邊的圈所成的集合。

而最出名的猜測是：對於任意邊的連通圖 G ， $2G$ 可以分割成圈所成的集合。

這個猜測就是雙覆蓋猜測 (Cycle Double Cover Conjecture, CDCC)，截至目前為止仍然尚未解決。

上述所提到的兩個敘述，一個已經證實，一個尚未解決，而未解決的 CDCC 則是非常困難的問題。以下，我們考慮一個不一樣的問題；在這裡，圈的長度扮演著重要的角色。同時，因為要分割成圈的集合，所以被分割的圖自然每個點都是偶點，而連通性就沒有那麼重要了。不過，為了描述的方便，連通圖仍然是第一個被考量的對象。

Alspach問題

(i) 當 n 為奇數時，若 $3 \leq m_1 \leq m_2 \leq \dots \leq m_t \leq n$ ，而且 $\sum_{i=1}^t m_i = \binom{n}{2}$ ，則 K_n 可以分割成 t 個圈 $C^{(1)}, C^{(2)}, \dots, C^{(t)}$ 使得 $C^{(i)}$ 恰有 m_i 個邊， $i=1, 2, \dots, t$ 。

(ii) 當 n 為偶數時，若 $3 \leq m_1 \leq m_2 \leq \dots \leq m_t \leq n$ ，而且 $\sum_{i=1}^t m_i = \frac{n(n-2)}{2}$ ，則 $K_n - F$

(1-factor) 可以分割成 t 個圈 $C^{(1)}, C^{(2)}, \dots, C^{(t)}$ 使得 $C^{(i)}$ 恰有 m_i 個邊， $i=1, 2, \dots, t$ 。

顯然，當 $m_1=m_2=\dots=m_t=m$ 時，我們得到了 m -圈系，或者是最大的 m -圈系它具有最少的殘留 (Minimum Leave)。而當 m 為 n 時，這就是所謂的哈密爾頓圈分割。

這個問題一般相信也是有非常高的難度，但是，對於特殊的 m_i ，則已經有了不少的成果。例如當 $m_i=3$ 或 4 時，只要 $3s+4t=\binom{n}{2}$ (n 為奇數) 或是 $3s+4t=\binom{n}{2}-\frac{n}{2}$ (n 為偶數)， K_n (或 K_n -F) 就可以被分割成 s 個三角形及 t 個四邊形。(作業) 目前已經知道的結果有：

$\{m_1, m_2, \dots, m_t\} = \{3, 4, 6\}$, $\{m_1, m_2, \dots, m_t\} = \{3, 5\}$, $\{m_1, m_2, \dots, m_t\} = \{4, 5\}$,

$\{3 \leq m_1 < m_2 < \dots < m_t \leq n\}$ 以及 $\{m_1, m_2, \dots, m_t\} = \{n-1, n\}$ 。而對應於完全圖的的分割，完全二分圖 $K_{m,n}$ 也可以做同樣的考量。目前最好的結果則是分割成 $\{4, 6, 8\}$ 的形式。

至於完全多分圖 (Complete Multipartite Graph) 的分割就沒有那麼容易了，以下的問題便可以說明它的難度，更何況 Alspach 的引伸問題。

問題 對於那些 n_1, n_2, n_3 ， $C_5 \mid K_{n_1, n_2, n_3}$ ？

作業

1. 證明在 $n \leq 8$ 時，問題 1 的敘述是正確的。
2. 證明在 $n \leq 7$ 時，問題 2 的敘述是正確的。
3. 證明 $K_9 - C_9$ 不可能分割成三角形的集合。

4. 具有指定殘留的圈系

對於圈系的了解，除了最大的裝填之外，我們也可以研究具有適當殘留的裝填。以下的結果是顯而易見的，證明省略。

引理 4.1. 令 H 為 G 的一個子圖，如果 $C_m \mid G-H$ ，則 $V(G-H)$ 中的每一個點均為偶點，而且 $|E(G)| - |E(H)|$ 為 m 的倍數。

推論 4.2. 令 H 為 K_{2n+1} 的一個子圖，而且 H 中的每個點均為偶點，則 $C_3 \mid K_{2n+1}-H$ 的必要條件為 $\binom{2n+1}{2} - |E(H)|$ 是 3 的倍數。

於是，我們想知道究竟有那些 H ，它滿足了上述的條件，而且 $K_{2n+1}-H$ 的確可以分割成三角形所成的集合。例如， K_9-C_9 中的 C_9 可以是上述的 H 嗎？也就是說 $C_3 \mid K_9-C_9$ 對嗎？這個相關的問題，經過一番努力已有了很好的結果。

定理 4.3. (Rosa & Colburn) 令 H 為 K_{2n+1} 2-正則子圖，除了 $n=4$ 及 $H \cong C_9$ 之外，只要 $\binom{2n+1}{2} - |E(H)|$ 為 3 的倍數，則 $C_3 \mid K_{2n+1}-H$ 。

這個定理原始證明很長，且非常不容易，以下是一個簡化的概念，究竟能否完成仍待努力。

例. 在 K_{13} 中，令 $H=3C_4$ 。首先把 13 個點分成三部分，如下圖所示。把不在 H 中的點 ∞ 連到各部份去掉 C_4 之後的邊，得到一些 C_3 。現在 $K_{13}-H-C_3$'s 為 $K_{4,4,4}$ ，它可以利用 4 階拉丁方陣分割成 C_3 。

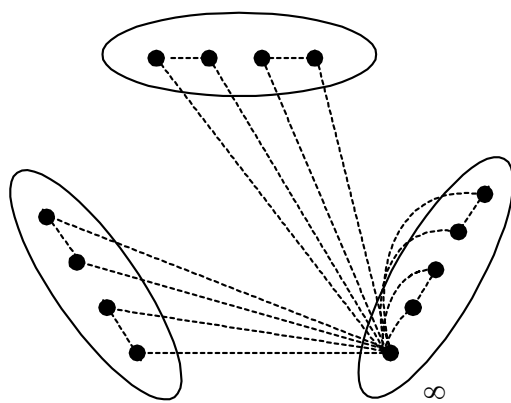


圖 4.1

所以，基本上我們可以將 $2n+1$ 分成三部份，最後應用 $\left\lfloor \frac{2n+1}{3} \right\rfloor$ 階拉丁方陣或部份拉丁方陣來協助分割，當然遞迴建構也要派上用場。

另外，在 K_{2n} 中也可以扣掉子圖 H ，使得 $C_3 \mid K_{2n}-H$ 。不過，由於 K_{2n} 中的點都是奇點，所以 H 中的點也要都是奇點才可以。以下的問題目前仍未解決，不過一般相信它應該是對的。

問題 1. 令 H 為 K_{2n} 的懸掛森林，而且 H 中的每個點均為奇點，則 $C_3 \mid K_{2n}-H$ 的充要條件為 $\binom{2n}{2} - |E(H)|$ 是 3 的倍數。

現在，把上述的問題改成 C_4 的分割，因為 C_4 可以由二分圖分割出來，所以困難度稍微低一些；於是，下面的兩個定理都已經被證明好。

定理 4.4. (Fu & Rodger, GC) 令 H 為 K_{2n+1} 的 2-正則子圖，則 $C_4 \mid K_{2n+1}-H$ 的充要條件為 $\binom{2n+1}{2} - |E(H)|$ 是 4 的倍數。

定理 4.5. (Fu & Rodger, JGT) 令 H 為 K_{2n} 的懸掛森林，同時 H 中的每一個點均為奇點，則 $C_4 \mid K_{2n}-H$ 的充要條件為 $\binom{2n}{2} - |E(H)|$ 是 4 的倍數。

類似的概念也被拿來研究 C_6 的分割，這個對應的結果不日即可完成；然而，相信一般 C_m 的分割就沒有那麼容易了；不過當 m 是偶數時，可能會較容易些。

問題 2. 對於上述的問題考慮定理 4.4 的 C_5 -分割。

5. 可分組圈系 (GDD Cycle System)

對應於區組設計的GDD，我們可以把區組所對應的 K_k 換成 C_k ，於是GDD k -圈系就產生了，一般以 k CGDD表示之。以圖分割的概念來加以詮釋比較容易，基本上，我們研究如何把 $K_{m(n)}$ 分割成圈的集合，也就是探討對於何種 m, n ， $C_k \mid K_{m(n)}$ 。

為了使研究更一般化，以下所探討的分割主體為 $(\lambda_1, \lambda_2)K_{m(n)}$ ，也就是一個 m 分圖，每一個部份均有 n 點；同時來自不同部份的兩點連 λ_2 邊，而來自同一部份的點則連 λ_1 邊。於是 $C_k \mid (\lambda_1, \lambda_2)K_{m(n)}$ 的必要條件如下：

引理 5.1. 若是 $C_k \mid (\lambda_1, \lambda_2)K_{m(n)}$ ，則

(i) $2 \mid \lambda_1(n-1) + \lambda_2 n(m-1)$ ，及

(ii) $k \mid \lambda_1 \binom{n}{2} m + \lambda_2 n^2 \binom{m}{2}$ 。

然而，(i)及(ii)是否為 $C_k \mid (\lambda_1, \lambda_2)K_{m(n)}$ 的充分條件就不是容易回答的問題了。為了便於解釋，我們以 $k=4$ 為例做說明。因為要證明上述的兩個條件是充分條件，我們需要證明，對於所有滿足(i)與(ii)的 λ_1, λ_2 ， m 與 n ， $C_4 \mid (\lambda_1, \lambda_2)K_{m(n)}$ ，所以先將滿足的條件列表，然後，再逐一建構滿足該條件的設計。(參考圖 5.1)可是，這些設計都只能對 $n \geq 4$ 有用，如果 $n < 4$ ，情況就有所不同。因為，在這個時候，第一結合類的邊將無法自己形成 C_4 ，而需仰賴第二結合類的邊，這時候關係就變得非常複雜；以下我們就以兩個例子來說明這類設計的建構概念；當然，這個類型的結果已經有了完整的答案。

定理 5.2. (Fu & Rodger) $C_4 \mid (\lambda_1, \lambda_2)K_{m(n)}$ 的充要條件為

(i) $2 \mid \lambda_1(n-1) + \lambda_2 n(m-1)$,

(ii) $k \mid \lambda_1 \binom{n}{2} m + \lambda_2 n^2 \binom{m}{2}$,

(iii) 當 $n=2$ 時， $\lambda_1 \leq 2(m-1)\lambda_2$ ，以及

(iv) 當 $n=3$ 時， $\lambda_1 \leq \frac{3(m-1)\lambda_2}{2} - \frac{\delta(m-1)}{9}$ ，這裡當 λ_2 是偶數時 $\delta=0$ ，而當 λ_2 是奇數時 $\delta=1$ 。

$\lambda_2 \backslash \lambda_1$	0	1	2	3	4
0 或 4	(any;any)	(even;any) (odd;1)	(even;any) (odd;0,1,4,5)	(even;any) (odd;1)	(any;any)
1	(1;any)	$n \cdot m \equiv 1 \pmod{8}$	(1;0,1,4,5) (3,7;even) (5;0,3,4,7)	(1;1) , (5;5) (3;7) , (7;3)	(1;any) (3,7;4,0) (5;even)
2	(0,1,4,5;any)	(0,4;any) (1,5;1) (2,6;even) (3,7;5)	$n \cdot m \equiv 0,1,4,5 \pmod{8}$	(0,4;any) (1,5;1) (2,6;even) (3,7;5)	(0,1,4,5;any) (2,3,6,7;even)
3	(1;any)	(1;1) , (5;5) (3;7) , (7;3)	(1;0,1,4,5) (3,7;even) (5;0,3,4,7)	$n \cdot m \equiv 1 \pmod{8}$	(1;any) (3,7;4,0) (5;even)

圖 5.1 $(n;m) \pmod{8}$ ， $\lambda_1, \lambda_2 \in \{0,1,2,3,4\}$

例 1. $C_4 \mid (1,2)K_{13(9)}$ 。

就圖中的每個部份而言，由定理 1.2 知道 $C_4 \mid K_9$ ，而就 GDD 來看，由引理 2.2 知道 $(0,2)K_{13(9)}$ 可以分割成 C_4 ，所以把兩個建構放在一起， $C_4 \mid (1,2)K_{13(9)}$ 。

例 2. $C_4 \mid (5,7)K_{15(11)}$ 。

由於 $C_4 \mid (4,4)K_{15(11)}$ ，所以只要判斷是否 $C_4 \mid (1,3)K_{15(11)}$ 即可。這時候我們需要 K_{165} 的裝填，也需要 $(0,2)K_{15(11)}$ 的裝填；同理，由定理 1.8 及引理 2.2，我們可以把兩者合起來求出 $(1,3)K_{15(11)}$ 的分割。（作業）

對應 C_4 ， C_3 也有類似型態的結果，建構的過程也是相當複雜，經過 Savarte，Rodger 與 Fu 的努力，以下的結果寫成兩部份，分別將在 Ars Combinatoria 及 JCT(A) 中刊登出來。

定理 5.3. $C_3 \mid (\lambda_1, \lambda_2)K_{m(n)}$ 的充要條件為

(i) $2 \mid (n-1)\lambda_1 + n(m-1)\lambda_2$ ，

(ii) $3 \mid mn(n-1)\lambda_1 + m(m-1)n^2\lambda_2$ ，

(iii) 若 $m=2$ 時，則 $\lambda_1 \geq \frac{n}{2(n-1)}\lambda_2$ ，以及

(iv) 若 $n=2$ 時，則 $\lambda_1 \leq (m-1)\lambda_2$ 。

作業

1. 試證 $C_4 \mid (1,3)K_{15(11)}$ 。
2. 試求 $C_k \mid (\lambda_1, \lambda_2)K_{m(n)}$ 的必要條件。

6. 圈系的嵌入問題

在第二章，我們已經知道史坦納三元系的嵌入是可以辦到的，而且可以討論部份三元系的嵌入問題。顯然，後者要困難許多；到目前為止，最好的結果如下：

定理 6.1. (Hilton 等人) 一個具有 v 個元素的部份史坦納三元系一定可以嵌入於一個具有 u 個元素的史坦納三元系，其中 $u \geq 4v+1$ 。

補充說明：一個部份史坦納三元系是指一個有序對 (V, p) ， V 為點集，而 p 則為一些三個元素的子集所形成的集合族，它滿足 V 中的任兩個元素最多只出現在一個 p 中的三元集。

在圈系中，我們也可以討論同樣的問題，只不過偶圈系的嵌入相對地比較容易，這主要是因為 Sotteau 的定理。

定理 6.2. (Sotteau) 令 n_1, n_2 為不小於 k 的正偶數同時滿足

$k \mid n_1 n_2$ ，則 $C_{2k} \mid K_{n_1, n_2}$ 。

在證明定理 1.5 時，實際上已經用了上述的定理，只不過是因為 C_4 比較容易直接建構，所以不用它；以下就以 6-圈系為例作說明。

引理 6.3. $C_6 \mid K_n$ 的充要條件為 $n \equiv 1$ 或 $9 \pmod{12}$ ， $n \geq 9$ 。

引理 6.4. 如果 $C_6 \mid K_n$ ，則 $C_6 \mid K_{n+12}$ 。

證明：利用圖 6.1，由於 $n_1 = n-1 \equiv 0$ 或 $8 \pmod{12}$ ，所以 $C_6 \mid K_{n_1, 12}$ 。再加上 $C_6 \mid K_{13}$ ，定理得證。

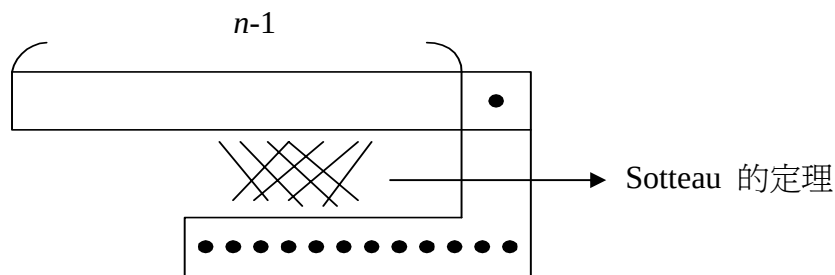


圖 6.1 $n \rightarrow n+12$ 建構法

引理 6.5. 當 $n \equiv 1 \pmod{12}$ 時， $C_6 \mid K_{n+8}$ 。

證明： 將 n_2 改成 8 即可。

引理 6.6. 當 $n \equiv 9 \pmod{12}$ 時， $C_6 \mid K_{n+4}$ 。

證明： 令 $n_1 = n-3$ ，則 $K_{n+4} - K_n - K_{n-3,4} = O_3 \vee K_4$ (圖 6.2)，再直接將 $O_3 \vee K_4$ 分割成 3 個 C_6 即可： $(a, 1, b, 2, 3, 4)$ ， $(a, 2, c, 4, 1, 3)$ 及 $(1, c, 3, b, 4, 2)$ 。

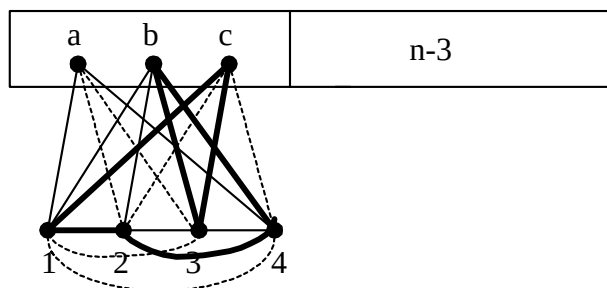


圖 6.2. $n \rightarrow n+4$ 建構法

補充說明： 引理 6.3 實際上可以利用 $C_6 \mid K_9$ ， $C_6 \mid K_{13}$ (作業) 以及三個引理 6.4，6.5，6.6 加以證明。

有了上述引理，以下的嵌入定理也就不難理解了。

定理 6.7. 任一 6-圈系都可以嵌入於一個比它大的 6-圈系中。

證明： (作業)。

相對於部份三元系，部份圈系的嵌入也是比較困難的工作，甚至是部份 4-圈系，到目前都沒有完全解決哩！

作業

1. 試分割 K_9 及 K_{13} 成 C_6 所成的集合。
2. 證明定理 6.7。
3. 證明引理 6.3。

第六章 組合設計的應用

在這一章中我們不再討論如何利用組合設計來建構實驗設計，或是應用到解決組合數學上的問題；我們將在編碼理論(Coding Theory)及暗碼理論(Cryptography)這兩方面作簡單的介紹，並說明如何利用組合設計來建構錯誤更正碼(Error-Correcting Code)及暗碼系統。

1. 錯誤更正碼

編碼理論是研究如何設計所要傳遞的訊息，使得訊息能夠快速、正確地傳送給對方；這裏的訊息一般以數位的方式傳遞，例如：太空船把拍到的照片傳回基地或人造衛星的使用都需要好的傳遞方式。它的主要原因來自傳遞時所經過的管道(Channel)是一種會受干擾的管道，傳遞的訊息在受到干擾時可能會造成錯誤，如果沒有適當的防患，後果可能不堪設想。另外，利用正確數位化的訊息傳遞，也可以用來製造各種CD片，使得原音或原影像能更準確地呈現出來。

定義 1.1. (q -ary Code, q 元碼) 令 F_q 為一有限體，任一個 F_q^n 的子集合稱為是長度為 n 的 q 元碼。當 $q=2$ 時，一般稱之為二元碼(Binary Code)。一個碼中的元素稱為是碼字(Codeword)。

二元碼是一般比較常見的數碼(Code)，因為它可以配合電腦，所使用的字串為 0 與 1 的組合，在以下介紹的前段，我們先介紹二元碼，最後再介紹一種特殊的 q 元碼。

定義 1.2. (漢明距離, Hamming Distance, 簡稱距離) 令

$\vec{x} = (x_1, x_2, \dots, x_n) = x_1x_2\dots x_n, \vec{y} = (y_1, y_2, \dots, y_n) = y_1y_2\dots y_n$ 為 F_q^n 中的兩個向量

(碼字), 則 $\vec{x}$ 與 $\vec{y}$ 的漢明距離定義為 $d(\vec{x}, \vec{y}) = |\{i \mid x_i \neq y_i, i = 1, 2, \dots, n\}|$ 。

例 1. $d(12012, 21020) = 4$ 。

我們不難看出定義 1.2 的距離本身就是一個度量 (Metric), 亦即滿足下列三個條件:

(1) $d(\vec{x}, \vec{y}) = 0$ 若且唯若 $\vec{x} = \vec{y}$ 。

(2) $d(\vec{x}, \vec{y}) = d(\vec{y}, \vec{x})$ 。

(3) $d(\vec{x}, \vec{z}) + d(\vec{z}, \vec{y}) \geq d(\vec{x}, \vec{y})$ (三角不等式)。

由於數碼 (Code) 是有限個元素所成的集合, 因此我們可以計算兩兩之間距離而得到該數碼的距離。

定義 1.3. (Code distance) 令 C 為一數碼, 則 $d(C)$ 定義為 $\min\{d(\vec{x}, \vec{y}) \mid \vec{x} \neq \vec{y} \text{ 且 } \vec{x}, \vec{y} \in C\}$ 。

定義 1.4. (線性碼, Linear Code) 如果 $(C, +, \cdot)$ 為 $(F_q^n, +, \cdot)$ 的一個子向量空間, 則稱 C 是線性碼。

定理 1.5. 令 $wt(\vec{x})$ 代表 $\vec{x}$ 中不等於 0 的分量數, C 為一個線性碼。則

$$d(C) = \min\{wt(\vec{x}) \mid \vec{x} \in C \setminus \{\vec{0}\}\}.$$

證明: $\min\{d(\vec{x}, \vec{y}) \mid \vec{x} \neq \vec{y}\} = \min\{wt(\vec{x} - \vec{y}) \mid \vec{x} \neq \vec{y}\} = \min\{wt(\vec{z}) \mid \vec{z} \in C \setminus \{\vec{0}\}\}.$

■

由於訊息在傳遞中可能因為受到干擾（Noise）而產生錯誤，例如，打字可能打錯，太空傳遞碰到氣層，閃電，聲音傳達時遇到雜音等。所以，計算可能傳錯的機率就很重要。以下，我們僅考慮二元碼，而且是對稱的二元碼，亦即傳送 0 與 1 時，出錯的機率相等。

引理 1.6. 令 0 與 1 傳錯的機率為 p ，則一個長度為 n 的字傳錯其中 m 個字母（0 或 1）的機率為 $p^m \cdot (1-p)^{n-m}$ 。

顯然，我們得假設每個字母傳送的對錯都是獨立發生才會得到上述的結論。

定理 1.7. 令 $p < \frac{1}{2}$, $0 \leq m_1 < m_2 \leq n$, 則傳錯 m_1 個字母的機率比傳錯 m_2 個字母的機率高。

最大可能法則（Maximum Likelihood Decoding, MLD）

機率大的事件發生的可能性比機率小的事件大。

基於上述的法則，在選擇比較可能發生的答案時，就不會產生疑義。（也許事實上有例外）

例 2. $C=\{000,111\}$ ，已知 C 中的一個碼字被傳送出去，而收到的是 101，試問：傳送的是那一個碼字？由引理 1.7， $000 \rightarrow 101$ 錯了二個字母，而 $111 \rightarrow 101$ 錯了一個字母，所以利用 MLD，傳送的是 111。

值得補充說明的是，當 $111 \rightarrow 001$ 時，利用 MLD 會得到傳送的碼字為 000，顯然是錯了！但是，這樣的事件是無法避免的，原因是錯太多個字母，理論上也說"不太可能"。

定義 1.8. (t -偵錯碼, t -error-detecting Code) 如果一個數碼可以在傳送時, 錯誤不超過 t 個字母的情況下, 都能看出來有錯誤發生, 則這個數碼稱為是 t -偵錯碼。

例 2 為 2-偵錯碼。以下的性質, 證明省略。

定理 1.9. 如果 $d(C) = t+1$, 則 C 為 t -偵錯碼。

定義 1.10. (t -糾錯碼, t -error-correcting Code) 如果一個數碼可以在傳送時, 錯誤不超過 t 個字母的情況下, 正確地指出傳錯的碼字, 則這個數碼稱為是 t -糾錯碼。

定理 1.11. 當 $d(C) \geq 2t+1$ 時, C 為 t -糾錯碼。

證明: 令 $\vec{x}$ 為傳送的碼字, 而 $\vec{y}$ 為收到的字; 由假設 $d(\vec{x}, \vec{y}) \leq t$ 。我們證明 $\vec{x}$ 為唯一與 $\vec{y}$ 距離不大於 t 的碼字即可。令 $\vec{z} \neq \vec{x}$ 而且 $\vec{z} \in C$, 如果 $d(\vec{z}, \vec{y}) \leq t$, 則 $d(\vec{x}, \vec{z}) \leq d(\vec{x}, \vec{y}) + d(\vec{y}, \vec{z}) = 2t$, 與假設 $d(C) \geq 2t+1$ 矛盾, 所以定理得證。 ■

由前面定理 1.10 及 1.11. 我們可以看出來, 只要 $d(C)$ 大, 那麼可以偵察或糾正的錯誤也比較多; 然而, 一般來說, $d(C)$ 比較大可能達成的方式之一是碼字的長度, 例如重覆 00 與 01 t 次, 即可使得製造出來的字, 距離為 t ; 這個時候由於碼字的長度大, 傳送也就比較費時, 當然, 也就更容易造成錯誤; 另外, 傳遞的訊息不可能只有一兩個而已, 例如要傳遞照片, 則每一小格 (解析之後) 的明暗度可以是 1~64, 因此要分別用 64 個不同的碼字來代表明暗度, 否則一旦錯誤, 又無法糾正, 後果將不堪設想。所以, 一個數碼的好壞決定於 (n, M, d) , n 為長度, M 為訊息數, 而 d 則為最小距離。如果研究的對象僅限於

線性碼，則 M 可以用該碼的維數來表示，一般以 k 表示。也就是說，在 q 元碼中， $M = q^k$ ，於是，線性碼的好壞決定於 $[n, k, d]$ 。

定義 1.12. $A_q(n, d) = \max\{M \mid \text{存在一個 } (n, M, d)\text{-}q\text{ 元碼}\}$ 。

定義 1.13. $A_q[n, d] = \max\{q^k \mid \text{存在一個 } [n, k, d]\text{-}q\text{ 元碼}\}$ 。

研究上述兩個量是編碼論中最重要的問題，在下一節中，我們會利用組合設計來說明如何找到好的下界。

2. 設計與數碼 (Design and Code)

一般使用的數碼都是線性碼，也因此碼字的長度是固定的，這樣的數碼，我們稱之為區組碼 (Block Code)。現在，假設一個區組設計 (n, k, λ) -設計存在，令此設計為 (V, B) ，其中 $|V| = n$ 。於是，對於 B 中的任一個區組 B ，我們定義一個 $(0, 1)$ -向量 $(x_1, x_2, \dots, x_n)$ 使得 $x_i = 0$ 若且唯若 $i \in B$ 。於是 (V, B) 就對應出一個二元碼；反過來看，一個數碼也對應出一個設計，只是無法確定是它是否為一個平衡設計。

定理 2.1. 令 C 為由一個 (n, k, λ) -設計所對應出來的數碼，則

(i) C 中的每一個碼字 $\vec{x}$ 它的加權 $wt(\vec{x}) = k$ 。

(ii) 當 $\lambda = 1$ 時， $d(C) \geq 2(k-1)$ 。

(iii) $|C| = \lambda n(n-1)/k(k-1)$ 。

證明： (i) 及 (iii) 可以直接看出來，而 (ii) 則是因為兩個區組至多只有一個元素相同。 ■

在上述定理中，如果 $\lambda = 2$ ，則會因為區組可能重複而造成 $d(C) = 0$ ，所以不是我們喜歡討論的情況。

例 3. $A_2(7, 3) = 16$ ，一個 STS(7) 對應出 $n=7$ ， $M=7$ ， $d=4$ 的數碼：
 $\{1101000, 0110100, 0011010, 0001101, 1000110, 0100011, 1010001\}$ ，再加上
 $\{0010111, 1001011, 1100101, 1110010, 0111001, 1011100, 0101110\}$ 及
 $\{0000000, 1111111\}$ ，則 $A_2(7, 3) \geq 16$ 。

現在，利用 (*) $A_2(7, 3) \leq \frac{2^7}{1 + \binom{7}{1}} = 16$ ，所以 $A_2(7, 3) = 16$ 。

$$(註) \quad A_2(n, 2t+1) \leq \frac{2^n}{\left(1 + \binom{n}{1} + \dots + \binom{n}{t}\right)} \quad (\text{Sphere-Packing Bound}).$$

由例 3，不難看出漂亮的組合設計的確有機會可以協助建構出非常好的數碼，反之亦然，在此不多做描述，讀者可參考編碼理論的書籍，自然可以獲得更多的資料。

接下來再看如何利用拉丁方陣的建構數碼。

例 4. 考慮互相垂直的兩個 3 階拉丁方陣：

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \quad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

於是，它們所形成的正交表（Orthogonal Array）如下：

$$\begin{array}{ccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \end{array}$$

由於任兩行之間至多只有一個位置會相同，所以把行看成向量（由上而下），就可得到一個 $n=4$ ， $M=9$ ， $d=3$ 的數碼，此時 $q=3$ 。所以 $A_3(4,3) \geq 9$ 。同理，因為 $A_q(4,3) \leq \frac{q^4}{(4q-3)}$ ，所以 $A_3(4,3) \leq 9$ ，於是 $A_3(4,3) = 9$ 。

$$(註) \quad A_q(4,3) \leq \frac{q^4}{\left(1 + \binom{q-1}{1} \binom{4}{1}\right)},$$

$$A_q(n, 2t+1) \leq \frac{q^n}{\left(1 + \binom{q-1}{1} \binom{n}{1} + \binom{q-1}{2} \binom{n}{2} + \dots + \binom{q-1}{t} \binom{n}{t}\right)}.$$

有了上面的例子，以下的定理就不難理解。

定理 2.2. 當 q 為質數次方時，一定存在一個 $(q+1, q^2, q)$ - q 元碼。

證明：當 q 為質數次方時，由定理 4.7，必存在 $q-1$ 個彼此互相垂直的 q 階拉丁方陣；這對應於一個 $(q+1) \times q^2$ 的正交表，所以所求的數碼就可以得到。 ■

定理 2.3. $A_q(q+1, q) = q^2$ 。

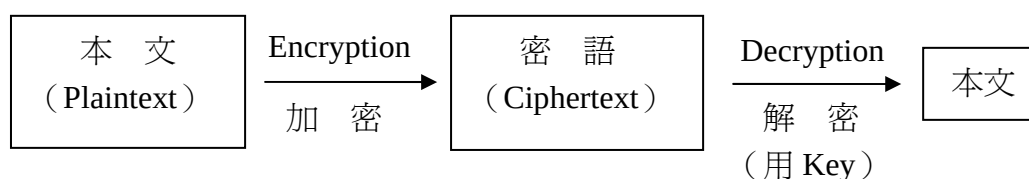
證明：由定理 2.2， $A_q(q+1, q) \geq q^2$ 。另一方面，由於距離 $\geq q$ ，所以任兩個碼字至多有一個分量相等；現在，看最後兩個分量的組合，如果碼字的個數多於 q^2 ，由鴿籠原理，則至少有兩個碼字最後的兩個分量都一樣，這與 q 為最小距離矛盾，所以 $A_q(q+1, q) \leq q^2$ ，定理得證。 ■

由於這一節的目標是要介紹組合設計與編碼理論的關係，所以只能以”點到為止”的方式說明，有興趣者不妨多找些參考資料閱讀，在下一節，我們將介紹設計與暗碼理論之間的關係。

3. 暗碼學 (Cryptology)

暗碼學是在學習如何設計暗碼系統 (Cipher System) 及破解暗碼系統 (Cryptanalysis)。設計的工作一般也稱為暗碼理論 (Cryptography)。在這一節裏面，我們簡要地介紹一些基本概念，然後在下一節探討它與組合設計的關連性。

所謂的暗碼，是將原來要傳遞的訊息 (本文)，經由一個轉換的動作變成不容易猜測出來的另一種訊息 (密語)，然後再傳遞出去；在設計這種轉換 (Encryption) 的同時，就要設計所謂的”正解”(Key)，只要有正解，就能順利地將收到的密語 (Ciphertext) 轉成本文 (Decryption)。所以，一般的暗碼系統可以用下面的簡表說明：



例 1. 令 $A, B, C, \dots, X, Y, Z, .$, 分別用 $0, 1, 2, \dots, 27$ 來表示；則任一個 $\mathbf{Z}_{28}$ 上面的排列都可以用來作為正解，這個正解的反元素同時把原來要傳遞的本文轉換成密語。例如： $(0\ 1)(2\ 3)\cdots(26\ 27)$ 可以把本文 I LOVE YOU. 轉換成 J.KPUF.ZPV_。這個例子的 Key 與轉換的排列恰好一樣。

例 2. 把要傳的訊息分成字母一樣多的很多組，例如每組 5 個，然後再利用 $x_1x_2x_3x_4x_5 =_{def} x_1 \times 28^4 + x_2 \times 28^3 + x_3 \times 28^2 + x_4 \times 28 + x_5$ ，然後再利用數的對應傳出去。例如：**RSA Scheme**。

令 $n=pq$ ，其中 p, q 均為質數且保密 (Key)，再令 $(e_B, \phi(n))=1$ ，其中 e_B 可以公開， $\phi(n)$ 則保密；現在甲要傳 M 給乙，只需要傳 M^{e_B} ，

而當乙收到時，他先利用 $e_B d_B \equiv 1 \pmod{\varphi(n)}$ 求出 d_B ，接著算出 $(M^{e_B})^{d_B} \equiv M \pmod{n}$ ，就可以知道傳遞的本文是什麼。

（註）這個系統的困難是知道 n ，但是無法很快地知道 p 與 q ，否則 $\varphi(n)$ 即被求得， d_B 這個 Key 也就不保。另外，這個暗碼並非傳遞的人就一定知道正解（如例 1），所以是目前最被廣泛使用的一種系統，一般而言， p, q 均為給 100 位數的質數。這系統的最大的缺點當然是需要龐大的計算！

4. 拉丁方陣與暗碼學

利用拉丁方陣來建構暗碼系統是近代的產物，其中互相垂直的拉丁方陣扮演著最重要角色，而它的形成方式如下：

Step 1. 找一個 n 使得互相垂直的 n 階拉丁方陣有很多個。

Step 2. 將要傳遞的訊息寫成有序對 (i, j) ，其中 i, j 皆取除以 n 的同餘。

Step 3. 找兩個互相垂直的 n 階拉丁方陣 $L=[l_{i,j}]$ 與 $M=[m_{i,j}]$ 作為解 (Key)。

Step 4. (Encryption) 將 (i, j) 轉成暗語 $(l_{i,j}, m_{i,j})$ ，然後傳出去。

Step 5. (Decryption) 收到暗語後，對照 L 與 M 即可轉成正確的本文。

顯然上述的密語系統是建立在 $L \perp M$ 的特性以及要找出 L 與 M 的困難度非常高的基礎上，所以它是一套相當好的系統。值得一提的是 L 與 M 的傳遞也是最重要的工作，由臨界集的概念，我們也可以傳遞 L 與 M 的臨界集就可以了，這時候在傳遞的工作方面就可以省下約 $3/4$ 的時間 (?)。

臨界集尚有其他重要的功能，而這方面的貢獻也是近代不可或缺的產物：組合解的密語系統 (Sharing Scheme)。

在很多時候，尤其是重要的工作，常常需要很謹慎的處理一件事，譬如，美國準備發射核子武器的攻擊，這時除了參謀總長，國防部長之外，也許還有其它的重要將領，甚至於總統要同時”同意”這項工作。於是，在同意的訊息全部到達之後，攻擊行動才算確定；否則，只要有人反對，就會因此而無法啟動。另外，銀行的金庫也會有兩人

同行才能開啓的設定，這也是一種組合解的系統，下面就介紹如何用拉丁方陣來協助完成這類系統的建構。

組合解系統的建構（利用臨界集）

Step 1. 找一個 n ，使得某一個 n 階拉丁方陣 $L=[l_{i,j}]$ 它具有很多最小的臨界集 A （元素個數最少）。

Step 2. 找到 t 個 L 的部份拉丁方陣 $P_1, P_2, \dots, P_t$ 使得它們都是可以填完的拉丁方陣，且填完的方法不止一個（很多種），另外 $A \subseteq \bigcup_{i=1}^t P_i$ ，而且少了任一個 P_i 都無法包含 A 。

Step 3. 將 $P_1, P_2, \dots, P_t$ 分送給 t 個人當解，於是系統完成設計。

以下是一個非常簡單的例子：

$$A = \begin{array}{|c|c|c|} \hline & & \\ \hline 2 & & \\ \hline & 1 & \\ \hline \end{array} \quad L = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \quad P_1 = \begin{array}{|c|c|c|} \hline & 2 & \\ \hline 2 & & \\ \hline & & \\ \hline \end{array} \quad P_2 = \begin{array}{|c|c|c|} \hline 1 & & \\ \hline & & \\ \hline & 1 & \\ \hline \end{array}$$

上述系統的 P_i 並不需要有非常多完成拉丁方陣的方法，例如 10 種，則成功的機率是 $1/10$ ，但是，想像要和其他人共同形成解，如果是錯的，則立刻暴露出造假的身份，所以安全性較高；同時，也要注意不可以有比 t 個人少的解合起來就能求出正解，否則我們就只能稱它是 t' -組合解系統，其中 $t' < t$ 。

另外，組合解系統也不排除某人可以擁有正解，他可能就是總經理或是老闆哩！（職員們要完成工作利用組合解系統）有了拉丁方陣之後就可以得到解，例如前面所述，我們需要兩個互相垂直的拉丁方陣。