有沒有10階有限射影平面？

蕭文強

1. 宴客問題

有本介紹趣味數學的經典之作，名叫「數學遊戲與小品」，是波爾（W.W. Rouse Ball）在1892年的著述。這本饒有趣味的書面世後，出了很多個版本，裏面陸續增添了一些別的名家手筆。第10章是以這樣一個問題開首的：

> 一位好客的女主人打算邀請她的七位朋友來家裏晚宴，每晚她只能招待三位賓客，但她希望任何兩位朋友都恰好在一次晚宴上見面，她應該怎樣安排呢？

請讀者先嘗試安排，不久你便會發現任何兩晚的賓客中必須有一位相同。換句話說，如果第一晚她邀請A、B、C，第二晚她邀請D、E、F，這樣下去肯定安排不成。一個安排方案是這樣子：

第一晚邀請A、B、C；
第二晚邀請A、D、E；
第三晚邀請A、F、G；
第四晚邀請B、D、F；
第五晚邀請B、E、G；
第六晚邀請C、D、G；
第七晚邀請C、E、F。

我們可以用一個圖表示這個方案（見圖1），圖中有七點，每點表示一位女主人的朋友；若干個點組成的集合叫做線，有七條線，每條線由三點組成，即是那些在同一晚給邀請的賓客。這個圖頗有名堂，可以說是組合數學上風頭最勁的圖形了！由於數學家范諾（G. Fano）

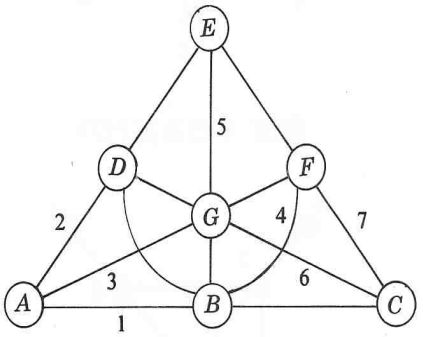

圖1

在1892年提出這個圖形，今天我們稱它作范諾構形（Fano configuration）。它的正式「學名」可是$PG(2,2)$，即是定義在二元域上的二維射影幾何，是一種有限射影平面。有限射影平面是這篇文章的主角，我們要探討的問題是有沒有某種有限射影平面？如果沿用宴客問題的語言，女主人打算邀請一百一十一位朋友來家裏晚宴，每晚只能招待十一位賓客，但又要求任何兩位朋友都恰好在一次晚宴上見面

，她應該怎樣安排呢？一個安排方案是個叫做10階有限射影平面的東西。1988年12月20日紐約時報（New York Times）刊載了一則新聞，報導加拿大康哥廸亞大學（Concordia University）林永康（Clement Lam）教授帶領一個研究小組，運用電腦驗算獲致充份證據認定不存在一個10階有限射影平面，也就是說，上述的問題是解決不來的。讀者會問：「數學家只曉得請客吃飯嗎？爲什麼對這個問題產生興趣？什麼叫做有限射影平面？它跟那些數學扯上關係？」請讀者稍安毋躁，聽我慢慢道來。

2. 射影幾何和有限射影平面

射影幾何的研究，始自法國數學家笛沙格（G. Desargues）在1639年的著作，但這些工作在當時並沒有得到重視，沒有引起什麼反響。直至再過幾乎兩個世紀後，另一位法國數學家彭賽列（J.V. Poncelet）深受老師蒙日（G. Monge）和卡諾（L.N.M. Carnot）的影響，在1822年發表了他的射影幾何學說，射影幾何才備受數學界重視，更成爲十九世紀的幾何重點研究。

那個時候的射影幾何建基於歐氏空間的幾何，讓我試以歐氏平面爲例作解釋，如果讀者對當中一些術語感到陌生的話，大可跳過這一段解釋續看下去。爲了不讓平行線享有與衆不同的特殊地位（不平行的直線延長必相交，平行的直線不論怎樣延長都不相交）。我們對平面補添一些「理想點」。對每一組平行線我們補添一點，不妨視作這些平行線的公共相交點；全部「理想點」組成一條「理想線」，於是原來的平面變成一個射影平面，裏面任何兩線相交於唯一個點，任何兩點決定唯一條線。如果採用座標幾何的慣用手法，我們應該怎樣描述這些補添的點和線呢？考慮通過原點的一條直線，在這條直線上取一點，設爲(x, y)，$\left(x/\frac{1}{2}, y/\frac{1}{2}\right)$是直線上距原點更遠的一點，$\left(x/\frac{1}{3}, y/\frac{1}{3}\right)$是直線上距原點又更遠的一點，……；這樣沿着直線一直走，便會越走越近那個「理想點」了。所以，「理想點」的座標有些像$(x/0, y/0)$，但用0除x和y，那怎成呢？一個轉彎抹角的說法是用$(x, y, 0)$表示那一點，把0寫在最後的位置，只在於表示意圖而非實施用0除x和y。爲求一致，我們索性把全部點都寫成(x, y, z)，不過大家需要先約好，當$z \neq 0$時，這個點其實是$(x/z, y/z)$；換句話說，所有(kx, ky, kz)，$k \neq 0$必須給視作相同的點。數學上有個叫做等價關係（Equivalence Relation）和等價類（Equivalence Class）的概念，正是爲了描述這種情況而設的。懂得等價關係的讀者便曉得剛才的敍述可以精確地寫作$(\boldsymbol{R}^3 \setminus \{0\})/\sim$，對三維實向量$\alpha$和$\beta$來說，$\alpha \sim \beta$（$\alpha$等價於$\beta$）表示有非零實數$k$使$\alpha = k\beta$。這樣得來的等價類集記作$PG(2, \boldsymbol{R})$，叫做一個二維實射影幾何，或稱作一個實射影平面。更一般地，$\boldsymbol{R}$可給換成一個任意域F（不懂得什麼是域的讀者可以把它看作是一個裏面能進行四則運算的集合），3可給換成$n+1$，得到的等價類集記作$PG(n, F)$，叫做域F上的n維射影幾何（n-dimensional projective geometry）。

二十世紀初，經過帕施（M. Pasch）、克萊茵（F. Klein）、維布倫（O. Veblen）、希爾伯特（D. Hilbert）諸人的努力，通過建立射影幾何的公理系統，射影幾何才擺脫對歐氏空間的倚賴而獲致它的獨立生存的權利。讓我只以射影平面（即是$n=2$）爲例作敍述，一個射影平面（Projective plane）是由兩個集和它們之間的一個關聯關係（incidence relation）構成：$\mathcal{P}$的元叫做點（point），

$\mathcal{L}$的元叫做線（line）；如果P是$\mathcal{P}$的元，ℓ是$\mathcal{L}$的元，$P\circ\ell$表示關聯，爲簡化以下的敍述，我們說P在ℓ上或ℓ在P上；$P\circ\ell$必須滿足下面四條公理，

〔$p1$〕 對$\mathcal{P}$中不相同的元P和Q，有且僅有一個$\mathcal{L}$中元ℓ使$P\circ\ell$和$Q\circ\ell$；

〔$p2$〕 對$\mathcal{L}$中不相同的元ℓ和m，有且僅有一個$\mathcal{P}$中元P使$P\circ\ell$和$P\circ m$；

〔$p3$〕 有四點，其中任何三點不在一線上；

〔$p4$〕 有四線，其中任何三線不在一點上。

固然，還有別的形式的公理系統是描述同一回事，但上面的公理系統有個「自對偶」的優點，從中推導出來的每一條定理，只要把命題中的點和線的地位互易，便又是另一條定理，可謂事半功倍！讀者只要回顧一下補添了「理想點」和「理想線」的平面，便自然看得出〔$p1$〕至〔$p4$〕這四條公理的幾何意義了。

當$\mathcal{P}$和$\mathcal{L}$都是有限集時，那個射影平面叫做有限射影平面，首先由德國數學家施陶特（K.G.C. Von Staudt）在1856年提出討論。范諾提出的構形，是最小的有限射影平面，有7點和7線。它其實是二元域$F=\{0,1\}$上的二維射影幾何，簡記作$PG(2,2)$。$\mathcal{P}$的7點是（見圖1）：

$〔0,0,1〕=C$、$〔0,1,0〕=A$、

$〔0,1,1〕=B$、$〔1,0,0〕=E$、

$〔1,0,1〕=F$、$〔1,1,0〕=D$、

$〔1,1,1〕=G$；

$\mathcal{L}$的7線是（見圖1）：

$<0,0,1>=ADE$、

$<0,1,0>=CEF$、

$<0,1,1>=BEG$、

$<1,0,0>=ABC$、

$<1,0,1>=AFG$、

$<1,1,0>=CDG$、

$<1,1,1>=BDF$；

而〔x,y,z〕。$<x;y;z'>$當且僅當$x'x+y'y+z'z=0$。這個射影平面的關聯關係可以利用下面的關聯表展示（見圖2），行是線，列是點。舉一個例，標以3那一行和標以F那一列相交的格子塗上黑色，表示點F在線3（即AFG）；標以6那一行和標以B那一列相交

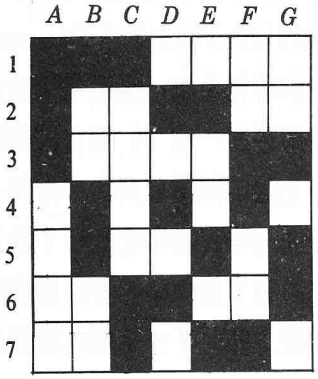

圖2

的格子塗上白色，表示點B不在線6（即CDG）。如果把黑色的格子換作1，白色的格子換作0，得到的矩陣叫做那一個射影平面的關聯矩陣（incidence matrix），在第3節裏將大派用場。注意，〔$p1$〕和〔$p2$〕等於說任何兩列（或兩行）有且僅有一個同等位置的格子是塗上黑色。對一般有限射影平面的關聯表，這個性質當然也是具備的，但眼下這一個關聯表還有一個單憑肉眼不易發覺的性質，就是適當地調換行和列後，關聯表的樣子很特別，每一行是上一行向右邊移一格得來（見圖3）。要解釋這個現象，需要借助有限域的知識，爲免篇幅過長，我不敍述了，這個漂亮的性質最先是由美國數學家辛格（J. Singer）在1938年發現的。讀者自然會提出疑問：「是不是任

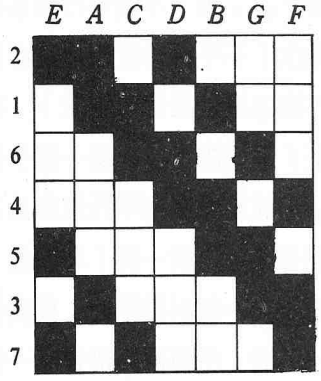

圖3

何一個有限射影平面的關聯表都具備這個漂亮的性質呢？」答案是否定的，但最小的反例已經是是一個 91 行 91 列的表，在本節結尾我們將要回到這一點。

讀者是否也注意到關聯表的每一行每一列都有同樣多塗了黑色的格子呢？對一般有限射影平面的關聯表，這仍然是對的。從公理〔$p1$〕至〔$p4$〕我們能推斷以下的結果。

定理 1：設N是大於 1 的整數，在有限射影平面內，下列各命題互相等價：

(1)有一線在$N+1$點上，

(2)有一點在$N+1$線上，

(3)任何線在$N+1$點上，

(4)任何點在$N+1$線上，

(5)共有N^2+N+1點，

(6)共有N^2+N+1線，

滿足這些（等價）條件的有限射影平面叫做N階射影平面（projective plane of order N）。

在過去一個世紀中，雖經衆多數學家的努力，我們仍然摸不透有限射影平面的存在與否這個問題。固然，對某些N我們肯定存在一個N階射影平面，例如當F是個q元域時，$PG(2,F)=PG(2,q)$是一個q階射影平面（熟悉有限域和向量空間的讀者可試證明任何線上有$q+1$點），由於q元域存在的充要條件是q爲質數冪，我們得到下面的結果。

定理 2：若N是個質數冪，則存在N階射影平面。

通過$PG(2,q)$構作得來的射影平面，叫做笛沙格平面，當質數冪N不大於 8 時，只有這一種射影平面，但當質數冪N大於 8 時，卻存在別的射影平面。特別地，當N是$9=3^2$時，很多年前數學家已經構作了幾個不是笛沙格平面的 9 階射影平面，它有 91 點和 91 線，由於並不是通過$PG(2,9)$構作得到，它的關聯表並不具備辛格發現的性質。兩年前林永康和他的研究小組更進一步證明了只有四種不同的 9 階射影平面。

3. 不存在那些階的射影平面？

讀者在上一節見過存在N階射影平面的數值N，自然要問：「有沒有那些N肯定不存在N階射影平面呢？」至今爲止，這方面的答案只有一個，就是美國數學家布魯克（R.H. Bruck）和賴瑟（J.H. Ryser）1949年發現的重要結果。

定理 3：（布魯克—賴瑟）：若N形如$4m+1$或$4m+2$且不能給寫作兩個平方數的和，則不存在N階射影平面。

我不在這兒證明這條重要定理，但卻通過解釋一個特殊情況展示證明的中心思想，當中必須假定讀者具備一些對稱矩陣和二次型（quadratic form）的基本知識，不熟悉這些知識的讀者跳過這段解釋也無妨。我希望說服讀者，爲什麼不存在 6 階射影平面。如果有一個 6 階射影平面，它的關聯矩陣A是個 43×43 矩陣，元是 0 或 1，射影平面的界定性質等於說$AA^T=6I+J$，這兒的A^T是A的轉置矩陣、I是單位矩陣、J是全部元爲 1 的矩陣。從直接計算可知AA^T的行列式是$49\times 6^{42}\neq 0$，所以A是非奇異矩陣。置$B=\begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$，$B$是個 44×44 非奇異矩陣，且$BB^T=\begin{bmatrix} 6I+J & 0 \\ 0 & 1 \end{bmatrix}$。再置$K=\begin{bmatrix} H & & 0 \\ & \ddots & \\ 0 & & H \end{bmatrix}$，對角線上共有 11 個 4×4 矩陣$H$，$H=\begin{bmatrix} 2 & 1 & 1 & 0 \\ 1 & -2 & 0 & -1 \\ 1 & 0 & -2 & 1 \\ 0 & 1 & -1 & -2 \end{bmatrix}$。

注意到$HH^T=6I$（這是因爲$6=2^2+1^2+1^2$

$+0^2$），便知道H是非奇異矩陣，所以K是個44×44非奇異矩陣，且$KK^T=6I$。因此，

有$(KB^{-1})\begin{bmatrix}6I+J & 0\\ 0 & 1\end{bmatrix}(KB^{-1})^T=6I$，

即是說下面的兩個有理數域上的二次型是相合（congruent）的：

$(x_1+\cdots\cdots+x_{43})^2+x_{44}^2+6(x_1^2+\cdots\cdots+x_{43}^2)$

和 $6(x_1^2+\cdots\cdots+x_{43}^2)+6x_{44}^2$。

把未定元再作適當的變換，更可以化爲下面兩個有理數域上的相合二次型：

$(x_1+\cdots\cdots+x_{43})^2+x_{44}^2$ 和 $6x_{44}^2$。

因此，存在有理數a、b、c滿足$a^2+b^2=6c^2$。通分母後，還可以設a、b、c是整數，由此可以推斷6能給寫作兩個平方數的和，但這是不可能的！

讓我們把從2開始的整數N分成三類，(Ⅰ)是質數冪、(Ⅱ)是布魯克-賴瑟定理排除的、(Ⅲ)是其餘：

(Ⅰ)	2	3	4	5		7	8	9	11		13			16	17		19		
(Ⅱ)					6							14							21
(Ⅲ)									10	12		15			18	20			

對(Ⅰ)我們知道存在N階射影平面，對(Ⅱ)我們知道不存在N階射影平面，對(Ⅲ)我們不肯定存在N階射影平面也不肯定不存在N階射影平面。不過數學家傾向相信只有兩種可能：一是當且僅當N在(Ⅰ)時，存在N階射影平面；另一是當且僅當N在(Ⅰ)或(Ⅲ)時，存在N階射影平面。爲了決定那一個可能較像樣，10階射影平面存在與否，起了關鍵作用。第1節結尾提到的發現，使數學家更加相信前一個猜想：N階射影平面存在的充要條件是N爲質數冪。

4. 有限射影平面與某些組合數學對象的關連

讓我們回到那個2階射影平面（或稱范諾構形）的關聯表（見圖3），把列順序改標作0、1、2、3、4、5、6。第一行塗上黑色的格子是0、1、3，把$D=\{0,1,3\}$看作是模7同餘類集合Z_7的子集，它有什麼性質呢？由於任何一行都是第一行向右移若干格得來，而且（除第一行自身不計）它跟第一行有且僅有一個同等位置的格子是塗上黑色，翻譯成Z_7內的語言就是說：對任何$t\neq 0$，$d_i-d_j=t$有唯一個有序偶(d_i,d_j)爲解，d_i和d_j是D中元。說得更淺白一點，D中全部不相同元的差（模7）正好是1、2、3、4、5、6。更一般地，如果$D=\{d_1,\cdots\cdots,d_k\}$是$Z_v$的子集，且對任何$t\neq 0$，$d_i-d_j=t$恰好有$\lambda$個有序偶$(d_i,d_j)$爲解，$d_i$和$d_j$是$D$中元，我們便說$D$是個$(v,k,\lambda)$-循環差集（cyclic difference set）。這兒的$N=k-\lambda$是個很有意思的參數，叫做循環差集的階。當$N=0$或1時，循環差集只能是顯而易見的幾種，即是空集ϕ、全集Z_v、單元集$\{d\}$、或者只欠單元的餘集$Z_v\setminus\{d\}$。當$N\geqslant 2$時，可以證明v只在$4N-1$和N^2+N+1中間取值。上界值和下界值都很有意思，很多時可以達致。對上界值N^2+N+1來說，由N階笛沙格射影平面$PG(2,N)$得到的$(N^2+N+1,N+1,1)$-循環差集即是一個例子。我們習慣把具有這些參數的循環差集叫做平面差集，奇怪的是迄今爲止我們仍未找到不是通過$PG(2,N)$得到的平面差集。對下界值$4N-1$來說，很多時可以構作$(4N-1,2N-1,N-1)$-循環差集，我們習慣把具有這些參數的循環差集叫做阿達馬差集，剛才的$(7,3,1)$-循環差集正好是一個例子。把這種差集的關聯表鑲嵌上一道全是黑色格子的曲尺邊，作爲第一行和第一列（見圖4），得到的陣列有個好性質，就是任何兩行（或兩列）都有恰好一半的位置同時白色或同是黑色的格子。在1868年英國數學家西勒維斯特（

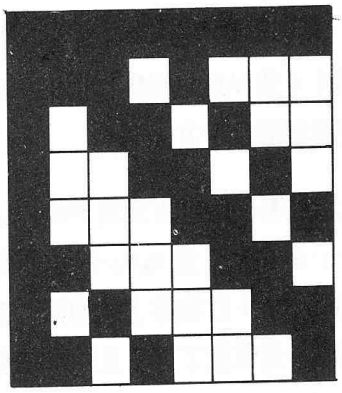

圖 4

J. J. Sylvester ）提出這樣的一個趣味數學問題，想不到過了二十五年後，法國數學家阿達馬（ J. Hadamard ）研究行列式的極大值時竟又碰上它！把黑色格子和白色格子分別換作 1 和－1 ，得到的矩陣滿足 $HH^T = H^T H = (4N)I$ ，這樣的矩陣叫做阿達馬矩陣，阿達馬差集的名稱便是這樣產生的。

讓我們又換一個角度看看范諾構形的關聯表，這次把它看成是放置 7 個元在 7 個區組的方案，要求每個區組都有 3 個元，每一對元都在一個僅只一個區組內出現。更一般地，我們可以試尋找在 v 元集 S 內挑選某些 k 元子集（叫做區組）的方案，要求每個 t 元子集都恰好在 λ 個區組內出現。這樣的一族 k 元子集𝒮叫做一個 (v, k, λ) - t 設計。范諾構形的關連表提供了一個 (7, 3, 1) - 2 設計。雖然 t 設計這個名字是到 1962 年才因數學家曉治（ D.R. Hughes ）的引進而流傳，但這種組合數學對象卻早在三十代年已受到注意，主要原因是它在統計學上的試驗設計非常有用。2 設計也叫做平衡不完全區組設計（ balanced incomplete block design ），簡稱BIBD，是英國統計學家葉斯（ F.Yates ）在 1936 年提出來研究的。當BIBD的參數 v 和 b 相同，它叫做 SBIBD ，頭一個字母表示對稱（symmetric ）。$\lambda=1$ 的SBIBD即是（ $k-1$ ）階射影平面。$\lambda=1$ 的BIBD 也叫做斯坦納系（ Steiner system ），因十九世紀瑞士數學家斯坦納（ J. Steiner ）的研究工作而得名，但其實最先提出這種問題的是一位英國牧師柯克曼（ T. J. Kirkman ）：「一位女教師每天帶領十五名女學生去散步，她要求學生們排成三人一行，又要求任何兩名學生在一週七天內恰好有一天排在同一行，她應該怎樣安排呢？」有關各種區組設計的研究和構作，至今猶蓬勃不已，除了由於它在試驗設計上的應用外，還因爲它跟編碼理論（ coding theory ）和散在單群（ sporadic group ）理論有密切關係。

5. 兩兩正交拉丁方完全組

看過第 2 節和第 4 節的敍述，讀者大抵明白數學家並非爲了請客吃飯才研究射影平面吧！在這一節我再介紹一種組合數學對象，並且通過它把 10 階射影平面存在問題化成另一個形式。無獨有偶，這種數學對象又是與數學遊戲有關。（也許這篇文章可以取題爲「戲無益乎？」！）瑞士數學家歐拉（ L. Euler ） 在 1779 年發表了一篇構作幻方（ magic square ）的文章，引進了今天我們叫做拉丁方的陣列。一個 N 階拉丁方（ latin square of order N ）是個 N 行 N 列的矩陣，裏面的元選自 N 個不同的符號（爲方便敍述不妨寫作 0、1、2、……、$N-1$ ），條件就是在每一行和每一列全部 N 個符號都要出現。例如 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$ 是個三階拉丁方，但 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix}$ 卻不是。設 A 和 B 是兩個 N 階拉丁方，考慮它們在相應位置的元構成的 N^2 對有序偶，如果兩兩不同，我們便說 A 和 B 是正交的拉丁方。例如 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$

和 $\begin{bmatrix}1&2&0\\0&1&2\\2&0&1\end{bmatrix}$ 是正交的拉丁方，但

$\begin{bmatrix}0&2&1\\2&1&0\\1&0&2\end{bmatrix}$ 和 $\begin{bmatrix}1&2&0\\2&0&1\\0&1&2\end{bmatrix}$ 卻不是，因爲第一行第一列和第二行第三列的有序偶都是（0，1）。歐拉在他的文章裏指出不存在一對正交的六階拉丁方，但他出諸遊戲口吻：「有六個軍團，從每個軍團選六名不同軍階的軍官。怎樣把這三十六名軍官排成六行六列，要求每一行和每一列都有六名不同軍階且隸屬不同軍團的代表？」接着他還說：「我毫不遲疑下這樣的結論，不存在一對正交的六階拉丁方，而且這個結論還能推廣至十階、十四階、……的情況，即是當階是二乘某個奇數的情況。」歐拉可沒有證明他的斷言，後人管叫這個斷言作歐拉猜想。1900年塔利兄弟（G. Tarry，H. Tarry）窮舉全部六階拉丁方驗算了猜想在六階情況果然成立。到了二十年代，由於拉丁方在試驗設計上的應用引起數學家的注意，歐拉猜想也就給提到議事日程來。美國數學家麥尼殊（H.F. MacNeish）在1922年甚至提出一個更強的猜想：設$N=p_1^{r_1}\cdots\cdots p_m^{r_m}$（$N\geqslant 2$）是$N$的質因子分解式，則頂多只能找到$t$個兩兩正交的$N$階拉丁方，$t$是$p_1^{r_1}-1$、……、$p_m^{r_m}-1$當中最小的數。不難證明當$N$是質數冪時（即$m=1$），這猜想是對的，因爲一般而言，頂多只有$N-1$個兩兩正交的$N$階拉丁方，讀者有興趣試證明嗎？後來數學家知道眞的可以找到這樣t個拉丁方，關鍵在於N是質數冪的情況，逐個$p_i^{r_i}$的情況解決了，便可以合成t個兩兩正交的N階拉丁方，詳情不贅。以「事後諸葛亮」的眼光看，質數冪的情況不難明白，但最先看到這種關係的洞察力，可叫人佩服，這份功勞歸於原籍印度的美國數學家玻色（R.C. Bose），他在1938年運用抽象代數中有限域的知識解答了這個問題。

定理4：若N是個質數冪，則有$N-1$個兩兩正交的N階拉丁方。

N是質數冪，便有N元域$F=\{a_0=0, a_1, \cdots\cdots, a_{N-1}\}$。置$a_h a_i+a_j$作第$k$個$N\times N$矩陣中第$i$行和第$j$列的元。直接驗算可知每個矩陣是個拉丁方，且兩兩正交，故定理4得證。

在1958年，美國數學家派克（E.T. Parker）找到至少四個兩兩正交的21階拉丁方，推翻了麥尼殊猜想（按照該猜想頂多只有兩個這樣的拉丁方），玻色和他的學生西里克漢特（S.S. Shrikhande）循着這個方向窮追猛打，數月後找到一對正交的22階拉丁方，推翻了歐拉猜想。同時，派克也找到一對正交的10階拉丁方，然後他們三位數學家聯手來攻，終於在翌年證明了一條叫人極感詫異的定理：除$N=2$和6以外，必有一對正交的N階拉丁方。這個發現竟上了當時（1959年4月24日）「紐約時報」的頭條新聞！

但是，一組個數最多的兩兩正交拉丁方，至今仍是懸而未決的問題。特別地，如果有$N-1$個兩兩正交的N階拉丁方，我們把它叫做一個完全組，定理4是說當N是質數冪時，存在一個兩兩正交N階拉丁方完全組。玻色在同一篇文章裏證明了另一條有趣的定理。

定理5：設$N\geqslant 3$，存在一個兩兩正交N階拉丁方完全組的充要條件是存在一個N階射影平面。

雖然我不在這兒證明這條定理，讓我以一個實例來印證，好使讀者看到它的內涵。取一個兩兩正交三階拉丁方完全組，由 $\begin{bmatrix}0&1&2\\1&2&0\\2&0&1\end{bmatrix}$ 和 $\begin{bmatrix}0&1&2\\2&0&1\\1&2&0\end{bmatrix}$ 組成。把相應位置的元構成有

A	0	0	0	0
B	0	1	1	1
C	0	2	2	2
D	1	0	1	2
E	1	1	2	0
F	1	2	0	1
G	2	0	2	1
H	2	1	0	2
I	2	2	1	0

圖 5

序偶寫在該位置標號的右邊，由此得到 9 點，如圖所示（見圖 5）。把這些點分成四組「平行線」，辦法如下：選第一個位是 0 的點構成第一條線、第一個位是 1 的點構成第二條線、第一個位是 2 的點構成第三條線，這三條線是第一組；類似地，按照第二個位分別是 0、1、2 又取三條線，是第二組；按照第三個位分別是 0、1、2 又取三條線，是第三組；按照第四個位分別是 0、1、2 又取三條線，是第四組（見圖 6）。現在，再添加四個「理想點」α、β、γ、δ，於是共有13點。在第一組的每條線多添 α、在第二組的每條線多添 β、在第三組的每條線多添 γ、在第四組的每條線多添 δ，連同由 α、β、γ、δ 組成的線共有13線。這 13 點和 13 線構成一個三階射影平面。

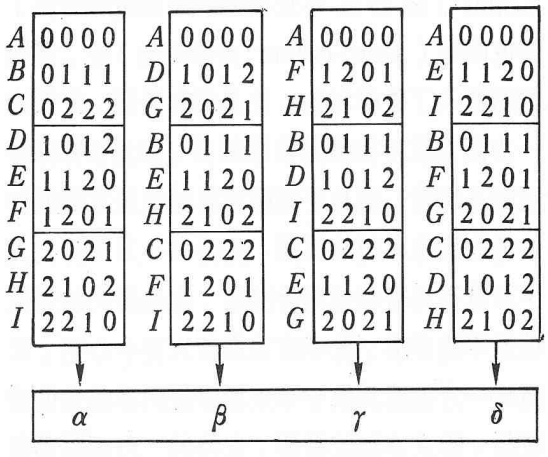

圖 6

反過來，如果有一個三階射影平面，適當地賦予座標後，可以把上述步驟倒轉過來構作一個兩兩正交三階拉丁方完全組。

從定理 5 可知 10 階射影平面存在問題化爲：有沒有 9 個兩兩正交的 10 階拉丁方？在六十年代派克曾經構作了一個 10 階拉丁方，估計有一百萬個 10 階拉丁方跟它正交，但可惜在這衆多拉丁方當中竟找不着一對互相正交的！至目前爲止，我們還不知道有沒有三個兩兩正交的10階拉丁方。

6. 不存在10階射影平面：電腦證明

閱讀了林永康教授惠寄來的多篇文章後，我看到他和他的小組的研究歷程，讓我在這一節作個很簡略的介紹。有興趣知道詳情的讀者可以參閱下面兩篇文章：

- C.W.H. Lam, L. Thiel, S. Swiercz, The non-existence of finite projective planes of order 10, preprint, 1989（將於*Canadian Journal of Mathematics* 1991年 4 月號上發表）
- C.W.H. Lam, The end of a finite projective plane of order 10, preprint, 1989.（將於*American Mathematical Monthly* 1991年4月號上發表）

要明白他們的工作，先要知道什麼是一個碼（code）。碼是通訊科學上爲了防範訊道受干擾引致的傳輸錯誤的設計，如果僅爲了看明白這一節，可以把一個碼看成是二元域上的 n 維空間裏的一個 k 維子空間，正確的術語是線性（n, k）碼（linear (n, k)-code）。它的向量叫做碼字，碼字裏 1 的個數叫做該碼字的重量（weight）。一個碼的檢錯和糾錯能力，視乎碼字的最小重量，所以一個碼的碼字重量分佈是很重要的研究目標，讓我們以 w_i

表示重量是 j 的碼字的個數。

如果存在一個 10 階射影平面，它的關聯矩陣的行可以看成是 111 個在二元域上的 111 維空間裏的向量，它們生成的子空間是個碼，記作 C。在 1970 年阿斯蒙斯（E.F. Assmus, Jr.）和馬森（H.F. Mattson, Jr.）提出研究這個碼以求了解 10 階射影平面，他們還證明了只用計算 w_{12}、w_{15}、w_{16} 便能完全確定 C 的碼字重量分佈。在 1973 年，麥威廉士（F.J. MacWilliams）、史隆尼（N.J.A. Sloane）和湯普森（J.G. Thompson）三人合力證明了 $w_{15}=0$。過了十年後，林永康和他的小組證明了 $w_{12}=0$。早在 1974 年卡特（J.L. Carter）在他的博士論文裏已經做了大部份關於 w_{16} 的計算，經湯普森的慫恿，林永康等乘勝追擊，在 1986 年完成剩下的計算，證明了 $w_{16}=0$。於是 C 的碼字重量分佈完全知道了，特別地 $w_{19}=24675$。換句話說，如果存在一個 10 階射影平面，由它生成的碼應該有 24675 個碼字的重量是 19。倒過來考慮，設 10 階射影平面裏的 19 點構成一個重量是 19 的碼字，數學家知道這些點和某些線的相交構形有某種性質，於是一個方法是試圖從這些「起點構形」出發，把它延伸爲一個 10 階射影平面的關聯矩陣，成功的話便找到一個 10 階射影平面，窮舉全部「起點構形」後也延伸不成功的話便證明了不存在 10 階射影平面了。

林永康等計算了共有 66 個「起點構形」要考慮，其中憑推理知道 21 個是不能延伸的，另外的 45 個卻只好借助電腦作驗算了。當中有 8 個涉及的計算量很大，使用他們的大學裏的電腦設備的話，估計要用上幾十年至一百年！幸好在這個時候，他們得到位於美國普林斯頓的國防分析研究所（Institute of Defense Analysis）的協助，允許他們利用那兒的 CRAY-1A 型超級電腦在工餘時間進行驗算。從 1986 年秋季開始計算，直至 1988 年 11 月中，經過超過 2000 小時的計算時間，答案終於出來了：不存在 10 階射影平面。宣稱這個重要發現時，林永康這樣說：「由於使用了電腦驗算，我們不應把這個結果視作在傳統意義下的「證明」，它只是一個實驗結果，也就不能避免產生實驗錯誤的可能。話雖如此說，以下我們要舉出理由說明存在仍然未給發現的 10 階射影平面的可能性是極低的。」這些理由分爲兩方面，其一是電腦程序的處理，其二是硬件設備的檢錯。在程序方面，他們使用不同的程序去計算以資比較，有時甚至用手算來驗證，同時又在程序中加了核算的步驟作保險。在硬件設備方面，超級電腦平均每 1,000 小時計算時間會出錯一次的，他們也的確曾經發現這種錯誤，後來補算了。或者可以這樣說，既然如果 10 階射影平面存在的話，它可以從那麼多碼字延伸而來（共有 24675 個重量是 19 的碼字），但至今仍然沒有 10 階射影平面給發現，這便是一個有力的證據，顯示它並不存在了。下一個待決定的情形是 12 階射影平面存在與否，但據林永康說，沿用同樣的手法使用目前的超級電腦去驗算，恐怕以人有生之年也辦不到了！

7. 後記

自從哈肯（W. Haken）和阿佩爾（K. Appel）在 1976 年宣稱他們借助電腦證明了四色問題（four-colour problem）後，電腦證明進入了數學討論，並且引起爭議。反對的一方認爲這不能算是數學證明，因爲很難保證電腦不出錯，而且更難確定出錯的是電腦操作的毛病還是人爲的紕漏；支持的一方則認爲人手計算不見得沒有機會出錯，有些證明的繁複程度不遑多讓，說不定電腦較人更小心呢。反對的一方也認爲數千年來數學證明都毋需借助電腦，將來亦無此需要；支持的一方卻認爲有些命題的證明可能除了驗算全部情況外別無他

法，以前它們不出現只因爲以前沒有電腦時人的計算能力未臻這個高度吧。

其實，如果我們不把證明的功能限於核實而更重視證明在說明闡釋方面的作用的話，電腦證明叫人最不愜意者倒不是上面提及的幾點，而是它頂多令人相信該命題成立，卻沒有令人明白爲何該命題成立。對於一個深信數學研究的主要目標乃追求理解的人來說，電腦證明只能起輔助作用卻不能帶來有如當年古希臘數學家阿基米德高喊Eureka 時的那份喜悅！

（最近林永康就這點寫了一篇文章，讀者可以參觀，聽聽證明者本人的意見：

C.W.H. Lam, How reliable is a computer-based proof ? The Mathematical Intelligencer, Vol. 12(1990), 8～12.）

——本文作者任教於香港大學——

（上接21頁）

"The k-domination and k-stability problems on sun-free chordal graphs," *Algebraic Discrete Methods*, 332–345, 1985.

[4] G. J. Chang(張鎮華)& G. L. Nemhauser, "Covering, packing and generalized perfection," *SIAM J. Algebraic Discrete Methods*, 109–132, 1985.

[5] M. Farber, " Characterizations of strongly chordal graphs," *Discrete Math.* 43, 173–189, 1983.

[6] A. J. Hoffman and A. W. J. Kolen and M. Sakarovitch, "Totally-balanced and greedy matrices," *SIAM J. Algebraic Disc. Math.* 6, 721–730, 1985.

[7] W.-L. Hsu, "Perfect graphs," Tech. Report, Academia Sinica, TR-88-16.

[8] A. Lubiw, Γ-*free Matrices*, M. S. Thesis, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 1982.