從離散數學到數學文化

1．非常感激第十七屆組合數學暨新苗研討會的主辦者，特別是傅恒霖教授和陳秋媛教授，邀請我來參加這趟盛會。四十年前我也是新苗，如今是老樹矣！更高興者，這趟盛會同時慶祝李國偉教授六十歲生辰，讓我有機會當面向國偉兄表達我對他的欽佩和敬意。

國偉兄對離散數學、數學史、數學普及工作、文化推廣工作，貢獻良多。於我而言，過去將近二十年，在這幾方面他都給我不少幫助、指點和鼓勵。從大學至研究院至從事數學工作，國偉兄走過的路，我跟他有一點相似。在那個年代，到美國唸書的中國留學生，畢業後留在彼邦發展的十居其九，我們卻各自回到自己的家鄉，國偉兄回了台灣，我回了香港，直到現在，三十多年過去了。當然，套用現正在北京舉行的奧林匹克運動會的格言，國偉兄是比我“Citius, Altius, Fortius（更快，更高，更強）”！

閒話休提，言歸正傳。

2．離散數學引人入勝的特色有三點：其一者，具體方面它可謂伸手能及，但抽象方面它任由想像翱翔；其二者，應用方面它涵蓋極廣，事例眾多；其三者，它的各項課題貌似不同，卻互相密切關連，至其底蘊，往往歸結爲古老的數論和幾何。

先來看一個例子，是以下的問題：在正六邊形的端點上放一枚紅珠、一枚黃珠、四枚綠珠，共有多少個真正不同的構形？所謂真正不同，就是不能憑旋轉或反轉由一個變成另一個。即使完全不懂數學的人，只要他有耐性和有條理，畫一下便知道只有三種構形，即是紅珠和黃珠相鄰、或者相隔一個位、或者相隔兩個位。要是問題換作是把二枚紅珠、一枚黃珠、三枚綠珠放在六個端點上，利用類似的步驟也不難找到只有六種構形，雖然要多費一點時間去臚列全部情況。這類問題十分具體，答案亦觸手可及，說一不二，斬釘截鐵。起初，我們不一定懂得爲何答案是如此，也不懂得如何預測更一般情況的答案，但至少對較簡單的具體情況我們有一種捉摸得到的感覺，不像有些數學問題，從開首已經踏入了抽象境界，於初學者而言，近乎“虛無飄渺”！

話得說回來，不要以爲問題只涉及有限情形便不複雜，就像這個問題，相信讀者不希望每次都要臚列全部可能的情況才求到答案。運用數學知識，這類問題有極漂亮的算法，是群論及組合數學的一個優美結合，由數學家波利亞 (George Pólya, 1887-1985) 在一九三七年提出來（其實另一位數學家列爾菲爾 (John Howard Redfield, 1879-1944) 在一九二七年已經獨立地提出了這種想法）。讀者毋需理會箇中詳情，也可以從下面的數式感受到其間涉及不少數學理論。（有興趣的讀者，不妨參看一本普及讀物：蕭文強，《波利亞計數定理》，湖南教育出版社，1991

年。）波利亞引進一個對稱群的圈指標這個概念，不同的問題與不同的對稱群有關。在上面的問題，用到的是正六邊形的對稱群，正式術語叫做十二階二面體群，通常記作 D_6。這個群的圈指標計算出來是

$Z(D_6)=\frac{1}{12}\left[X_1^6+4X_2^3+2X_3^2+3X_1^2X_2^2+2X_6\right]$。如果我們把 X_1、X_2、⋯、X_6 分別換成 $r+y+g$、$r^2+y^2+g^2$、⋯、$r^6+y^6+g^6$，$Z(D_6)$ 便給換成一條公式 $I(r,y,g)=r^6+r^5y+r^5g+3r^4y^2+3r^4yg+\cdots+6r^2yg^3+\cdots+3ryg^4+\cdots+yg^5+g^6$。看上去是否有些眼花繚亂呢？但奇妙的事情，是那些系數竟然就是我們要找的答案！譬如 $3ryg^4$ 表示有三個真正不同的構形，有一枚紅珠 (r)、一枚黃珠 (y)、四枚綠珠 (g)；$6r^2yg^3$ 表示有六個真正不同的構形，有二枚紅珠、一枚黃珠、三枚綠珠。

波利亞設計這種算法，心中有其應用，就是計算有機化學裏某些化合物的同分異構體的數目。譬如烷烴系列 C_NH_{2N+2} 的 CH_4、C_2H_6、C_3H_8 各有一個同分異構體，但 C_4H_{10} 卻有兩個，C_5H_{12} 有三個，等等（見圖 1）。

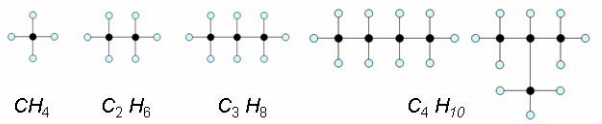

圖 1

波利亞巧妙地運用他的計數理論，結合母函數理論成功地解決了這個問題。這個例子，是否反映了這一節開首提到離散數學引人入勝的三個特色呢？

我覺得這就有點像一堆群島，我們見到海面上星羅棋布的島嶼，島與島之間沒有相連，但其實在海底裏卻是一片相連的大陸（見圖 2）。我便有如一個潛泳員，在當中探幽尋微，欣賞那無限風光！

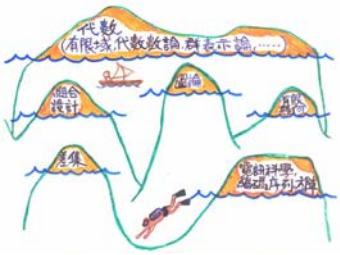

圖 2

以前我寫了幾篇文章，介紹一些曾經吸引了我的課題：

M.K. Siu, From binary sequences to combinatorial designs, *J. Math. Res Exposition*, 9 (1989), 605-621.

M.K. Siu, The combinatorics of binary arrays, J. *Stat. Planning & Inference*, 62 (1997), 103-113.

M.K. Siu, Combinatorics and algebra: A medley of problems? A medley of techniques? *Contemporary Mathematics*, 264 (2000), 287-305.

漸漸我體會到前人智慧，幾千年前他們已經指出難解的問題往往歸結到古老的學問——幾何及數論。柏拉圖 (Plato, 427B.C.-347B.C.) 說「神老是幾何化。（God ever geometrizes.）」伽利略 (Galileo Galilei, 1564-1642) 說：「大自然的奧秘都寫在這部偉大的書本上，…這部書用數學語言寫的，它用的字是三角形、圓形及別的幾何圖形，…([Natural] Philosophy is written in this grand book…written in the language of mathematics, and its characters are triangles, circles, and other geometric figures,…)」畢達哥拉斯 (Pythagoras, c. 560B.C.- 480B.C.) 說：「萬物皆數。（All is number.）」雅可比 (Carl Gustav Jacob Jacobi, 1804-1851) 說：「神老是算術化。（God ever arithmetizes.）」拉格朗日 （Joseph Louis Lagrange, 1736-1813） 說得更全面：「有一位古代學者說過，算術及幾何乃是數學的一對翅膀。（An ancient writer said that arithmetic and geometry are the wings of mathematics.）」他提到的學者可能是波義耳 (Robert Boyle, 1627-1691) ，只比他早活一個世紀。波義耳曾經說過：「算術及幾何，天文學家藉著這對翅膀翱翔天際，與天比高。（Arithmetic and geometry, these wings on which the astronomer soars as high as heaven.）」

3. 接著這兩節，我打算敘述一些個人從事離散數學工作的片斷故事，技術內容無疑較其他各節是濃厚一點，但讀者不理會箇中細節只作略讀亦無妨，反正我也沒可能仔細詳述的。不過，完全跳去這部份，讀者便失卻機會觀賞離散數學引人入勝的第三點，而正正好是這一點體會，引起我對數學文化的關注和興趣。

我在美國哥倫比亞大學研究院攻讀數學，跟隨巴斯教授（Hyman Bass）研讀代數 K-理論，在當時那是一門新興的研究領域，進展蓬勃，新發現接踵而來，叫我學得既吃力也興奮。一九七五年夏，我受母校之聘，回到香港大學任教，頓然發現要繼續貼近代數 K-理論研究頗有些困難。那個年代的香港，於科研而言乃邊陲之疆，資訊不流通，參加國際學術會議的交流機會也缺乏，和二十多年後相比，完全是另一番面貌。既然不容易貼近本行的研究，但我仍然鍾情於數學，尤其是代數，便想到在別的方向另謀發展。

未返母校前三年，我在美國佛州的邁亞密大學工作，當時曾經旁聽了一位同事伯遜教授（Alton Thomas Butson）開設的組合數學課，用的課本是霍爾（Marshall Hall, Jr., 1910-1990）的《組合論》（*Combinatorial Theory*, 1967），令我很感興趣。同時伯遜也給我介紹了齊勒爾（Neal Zierler）關於線性遞歸序列的論文〔N. Zierler, Linear recurring sequences, *J. Soc. Ind. Appl. Math.*, 7(1959), 31-48〕，引起了我不少聯想。如今回頭看，我被這些課題吸引過去，是否因爲當中的代數內容有以致之呢？剛回到香港大學的第一年，我被派任教一門應用數學課「排隊論」，其中有一節課提到模擬計算中運用的隨機數，它們的生成與線性遞歸序列有點關係，喚

起了我兩三年前對組合數學產生的興趣，便一頭跳進去了。當時剛好有位勤奮好學的年青人唐寶找我當他的碩士生導師，我們兩人從細讀齊勒爾的論文開始工作。

國偉兄專長於圖論，讓我就以一個圖論問題作引子。問題是關於一串 0 和 1 組成的二元序列，我們嘗試逐 n 個連續項察看。例如序列是（01010101…）而 $n=3$，則有 010、101、010、101、…，兩次後模式即重複。換了序列是（00111010011101001101 1…）而 $n=3$，則有 001、011、111、110、101、010、100、001、011…，七次後模式才重複，而且除卻 000 以外，全部二元 n 重數組都出現一次。如果在適當位置添加一個 0，把序列變成是（0001110100011101000110 1…），更能得到全部八個二元 n 重數組 000、001、011、111、110、101、010、100 了。把問題化爲圖論敘述形式，是考慮一種特殊的有向圖，叫做德布魯因-古德(de Bruijn-Good)圖 G_n，頂點是全部二元 n 重數組，共有 2^n 個；兩個頂點 a 和 b 有一條邊相連，方向是從 a 到 b，當且僅當 a 的後面 $n-1$ 個元構成的數組恰好是 b 的前面 $n-1$ 個元構成的數組。取一個具體例子 G_3 看看好了（見圖 3），

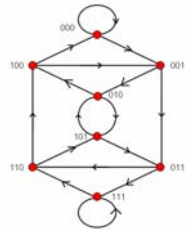

圖 3

它包含有很多個圈分解，即是取全部頂點和部份邊，某些點和某些邊構成一個圈，每個圈各自當然是連通的子圖，但圈與圈卻是不相干的。在電子工程通訊科學中，這種圈分解可以由一種叫做移位寄存器的設備生成，例如下圖（見圖 4）

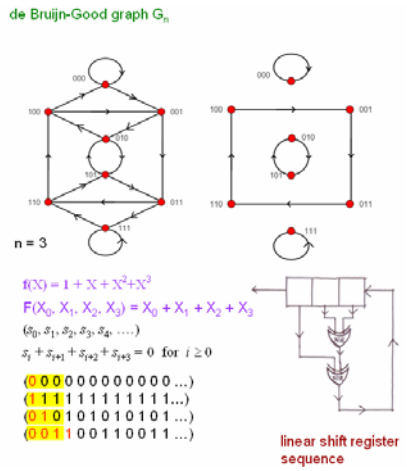

圖 4

所示的圈分解相當於四條序列〔只列出一個周期〕：（0），（1），（01），（0011）。數學上有個簡捷的表達方式，是寫成一條遞歸關係式

$$s_i + s_{i+1} + s_{i+2} + s_{i+3} = 0 \text{ ， } i \geq 0 \text{ 。}$$

若置初始狀態爲 $s_0 = 0$ ， $s_1 = 0$ ， $s_2 = 0$ ，便由此得 $s_3 = 0$（用二元算術運算），$s_4 = 0$ ， $s_5 = 0$ ，等等，即是序列（0）。若置初始狀態爲 $s_0 = 0$ ， $s_1 = 1$ ， $s_2 = 0$ ，便由此得 $s_3 = 1$ ， $s_4 = 0$ ， $s_5 = 1$ ， $s_6 = 0$ ，等等，即是序列（01）。餘類推便得出那四條序列，亦即是那個圈分解。

再多看一個例子（見圖 5），這次只有三條序列：（0），（001），（0111）。

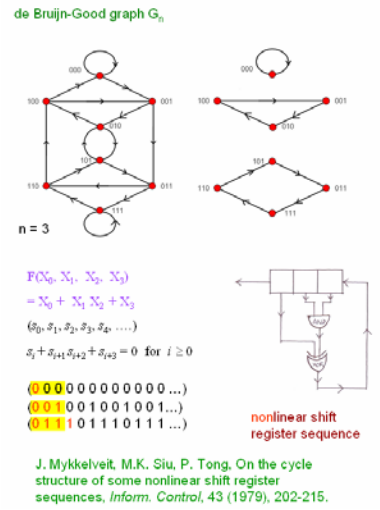

圖 5

相應的遞歸關係式是

$$s_i + s_{i+1}s_{i+2} + s_{i+3} = 0 \text{ ， } i \geq 0 \text{ 。}$$

從數學上看，雖然兩個例子的基本思想是一樣，它們有一點性質極不相同，第一個涉及的關係式是“線性”的，而第二個涉及的關係式是“非線性的”。如果利用多項式去表示（讀者不必擔心箇中技術細節，獲取一種感覺便成），第一個例子可以寫成 $F(X_0, X_1, X_2, X_3) = X_0 + X_1 + X_2 + X_3$ ，是個一次多項式，而第二個例子可以寫成 $F(X_0, X_1, X_2, X_3) = X_0 + X_1X_2 + X_3$ ，不是一個一次多項式。

更有趣的例子是當圈分解（i）只有一個圈，或者（ii）只有兩個圈而其一是（00…0）。看看下圖的例子（見圖 6），

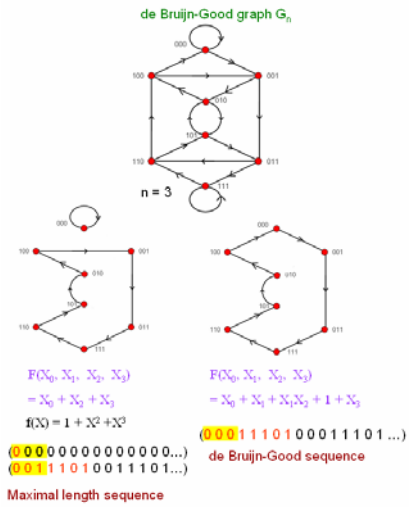

圖 6

相應於（i）的序列是（00011101），多項式是 $F(X_0, X_1, X_2, X_3) = X_0 + X_1 + X_1X_2 + 1 + X_3$；相應於（ii）的序列是（0）和（0011101），多項式是 $F(X_0, X_1, X_2, X_3) = X_0 + X_2 + X_3$。這兩個例子都在開首提過，它們的部份二元 n 重數組兩兩不同，而且全部出現（第二個例子只欠一個全零 n 重數組）。

一個自然產生的問題，是怎樣由一條給定的多項式推算它對應的德布魯因-古德圖 G_n 的圈分解。若 $F(X_0, X_1, \cdots, X_n)$ 是一次多項式，已經有一套完備的理論，鉅細無遺地描述有多少個圈，每個圈有多長。三十年前我便對這個問題產生興趣，做過一丁點工夫〔J. Mykkelveit, M.K. Siu, P. Tong, On the cycle structure of some nonlinear shift register sequences, *Inform. Control*, 43(1979), 202-215〕，但像隔靴搔癢，距離目標十分遙遠。據我所知，至今大家對這個問題還是知的不多。

讓我們把（0011101）這條序列再仔細審視一下，把序列向右平移 t 個位，數一數相疊的項有多少個相同，有多少個不相同（序列是按周期重複自身的），把這兩個數相減，得到的答案叫做該序列的實自相關函數在 t-平移的取值，記作 $RP(t)$。數一數相疊的項有多少個是 1，得到的答案叫做該序列的二元自相關函數在 t-平移的取值，記作 $BP(t)$。在這個特例，RP 和 BP 具備獨特性質，若 t 不是 0 或不是序列周期 v 的倍數時， $RP(t)$ 取相同值 -1，而 $BP(t)$ 取相同值 2；顯然，當 t 是 0 或 v 的倍數時， $RP(t)$ 取值 7，而 $BP(t)$ 取值 4（見圖 7）。我們說，序列（0011101）的（實或二元）自相關函數是二水平的。

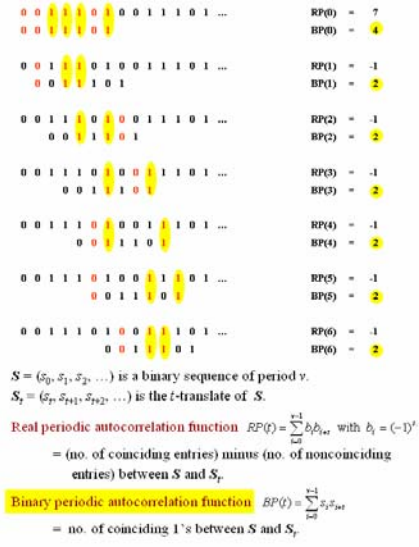

圖 7

這個獨特性質反映了 0 和 1（與及它們的組合）在序列中的分佈情況，也在某方面反映了序列的隨機性，於此不贅。由於這些序列具備某些隨機性質，但卻是由特定的方法（肯定不是隨機方法！）生成，故稱爲僞隨機序列，在應用方面很重要。

在第二節開首我說過離散數學的各項課題貌似不同卻互相密切關連，就讓我們再換一個角度看同一個問題吧。仍然是考慮周期 v 是 7 的二元序列（0011101），注意它的非零項（即是 1）出現在位置 2、3、4、6（第一項標作 0，第二項標作 1，餘類推）。置集 D = {2,3,4,6}，它有個獨特性質，即是各相異項相減（模 7）得到的十二個數，正好是 1、2、3、4、5、6，每個出現兩次。在組合數學上，這是一種備受關注的研究對象，叫做循環差集，是這樣定義的：$D=\{d_1,\cdots,d_k\}$ 是 v 階循環群 $\mathbb{Z}/v\mathbb{Z}$ 的一個子集，如果對任意 $t\neq 0$，$d_i-d_j=t$ 恰好有 λ 對解 (d_i,d_j)，便把 D 稱作一個 (v,k,λ)-(循環)差集。把定義弄清楚後，不難證明以下的定理：

> 設 $\mathbf{S}=(s_0,s_1,\cdots,s_{v-1})$ 是周期爲 v 的二元序列，它有 k 項是 1 而且它的自相關函數是二水平的。在 v 階循環群 $\mathbb{Z}/v\mathbb{Z}$ 中取子集 D，其中 i 是在 D 當且僅當 $s_i=1$。則 D 是一個 (v,k,λ)-差集。
>
> 反之，設 D 是一個 (v,k,λ)-差集，置二元序列 $\mathbf{S}=(s_0,s_1,\cdots,s_{v-1})$，其中 $s_i=1$ 當且僅當 i 是在 D。則 $\mathbf{S}$ 的自相關函數是二水平的，且對所有 $t\neq 0$，$BP(t)=\lambda$。

不難看到，在序列中把 0 和 1 互換，無傷大雅！所以從（0011101）中也可以考慮 $D=\{0,1,5\}$（即是零項出現的位置），它是一個 $(7,3,1)$-差集，各相異項相減(模 7)得到的六個數兩兩不同，正好就是全部非零數(模 7)。這又帶引我們再看另一個研究對象，較適宜以幾何語言描述。設有七個點，記作 0、1、2、3、4、5、6；取

$D=\{0,1,5\}$，叫做一條線。把各點加一，得另一條線$\{1,2,6\}$；再把各點加一，又得另一條線$\{2,3,0\}$，餘此類推得到七條線，即是

$\{0,1,5\},\{1,2,6\},\{2,3,0\},\{3,4,1\},\{4,5,2\},\{5,6,3\},\{6,0,4\}$。

任何兩個點必在唯一條線上，任何兩條線必有唯一個公共點。這是有限射影平面最簡單的一個例子，叫做法諾七點構形（Fano's seven-point configuration），不妨稱爲組合數學（特別是組合設計）工作者的"招牌"！（見圖 8）

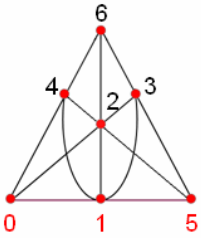

圖 8

有限射影平面是一種頗精密的構形，它的點數 N 和線數 N 不單相同，而且都是形如 n^2+n+1，n 便叫做該射影平面的階。利用抽象代數有限域的知識，我們能構作某些有限射影平面，它們的階正好是有限域的階。由於有限域的階必爲質數的冪，這些射影平面的階都是質數的冪。數學家也找到一些射影平面，不能這樣從有限域構作而成，但奇怪地，所有找到的有限射影平面，它們的階都是質數的冪。於是，有一個主要猜想，說有限射影平面的階必爲質數的冪。這個猜想已經提出來半個世紀有多，至今懸而未決，看似甚難解答。

4．我在離散數學方面的嘗試，都是無功而退者居多，那麼多失敗的事例，講演再長幾個小時也不夠，不如只再講一個，它與好萊塢（Hollywood）一位名演員有關，題材輕鬆，貼切這個慶祝國偉兄生辰的場合！這位演員在二十世紀的三十年代四十年代非常著名，就是艷光四射的喜地拉瑪（Hedy Lamarr, 1913-2000）。此乃其藝名，她原籍奧地利，真名是奇士拿（Hedwig Eva Maria Kiesler），曾結婚六次，第一任丈夫曼特（Friedrich Mandl, 1900-1977）是奧地利軍事工業家，爲了不想太太在演藝界工作，經常帶她參與工業界的技術會議。拉瑪本人頗富數學才華，從中她學到不少。在第二次大戰期間，她和一位美國作曲家安泰（George Antheil, 1900-1950）合作，發明了一種能夠躲避敵方干擾，由無線電通訊控制的魚雷發射裝置，在一九四二年八月取得專利權（當時登記專利權她用的名字是 Hedy Kiesler Markey，後者是她的第二任丈夫的姓名）（見圖 9）。

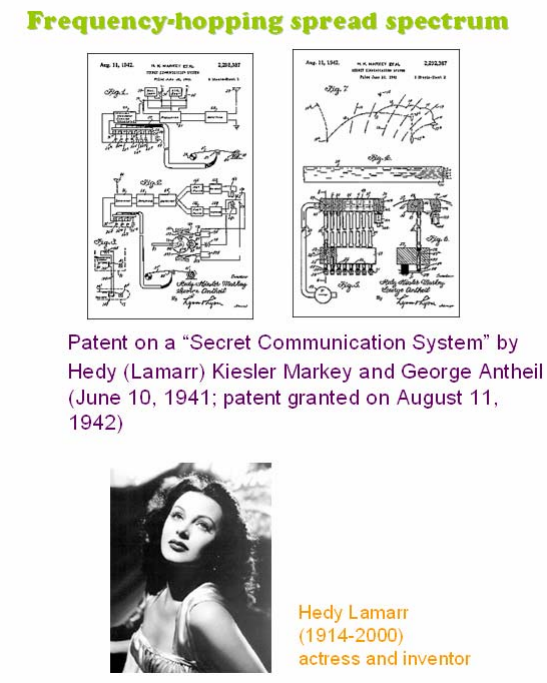

圖 9

拉瑪和安泰的發明並沒有受到軍方重視，結果在二次大戰中從來沒有使用過，但這項發明開了一項技術先河，就是展布頻譜（spread spectrum）的跳頻（frequency-hopping）技術，在今天的人造衛星、手提電話、互聯網上是不可或缺的技術發明。由於這個緣故，在一九九七年拉瑪以八十二歲高齡獲頒電子前沿基金會（Electronic Frontier Foundation）的獎項！

粗略簡單地說，我要考慮的問題的通訊工程背景是這樣的。有若干名用者各自與一個公共資料庫連結，互相交換資訊，每人有其通訊頻道，而且每人按時更改頻道。設有五名用者和五條頻道，標作 0、1、2、3、4，譬如說用者 1 的頻道按次是（3224132241…），用者 2 的頻道按次是（4330243302…），用者 3 的頻道按次是（0441304413…），用者 4 的頻道按次是（1002410024…），用者 5 的頻道按次是（2113021130…）。用者與用者之間在某個時刻所用的頻道可能相同也可能不相同，希望做到的是不相同者居多，否則便互相干擾了。要比較的不單單是兩名用者定了位的頻道，而是他們的頻道及其移位，譬如說（32241）和（43302）、（22413）和（43302）、（24132）和（43302）、（41322）和（43302）、（13224）和（43302）；又或者（32241）和（21130）、（22413）和（21130）、（24132）和（21130）、（41322）和（21130）、（13224）和（21130）；等等。

不如換另一個圖像表示形式，把一個 5×5 方陣的某些格塗色（或者打上叉形符號）以表示用者的頻道（見圖 10）。

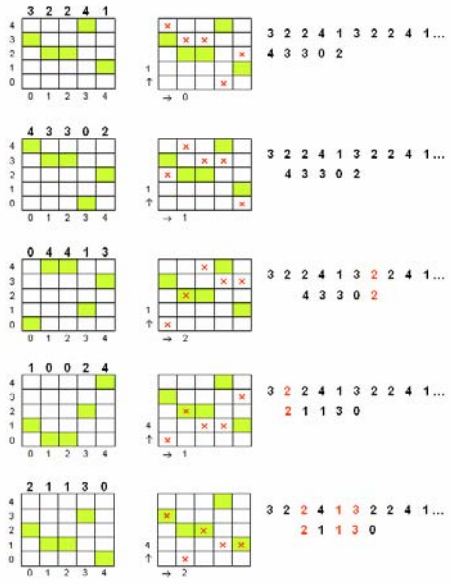

圖 10

讀者一定會留意到，上面例子五位用者的頻道並非胡亂寫下來的，只要知道某位用者的頻道，把各項加一（模 5）便得到下一位用者的頻道，在圖像表示中即是把塗了色的模樣向上移一行（超越了最頂一行便變成最底一行）。這樣做至少保證了任意兩位用者的頻道沒有干擾，例如（32241）和（43302）沒有干擾。但要比較向右移位的塗了色的模樣，卻無此保證了。例如（24132）和（43302）有一處干擾，而（24132）和（21130）有兩處干擾（見圖 10）。

這樣用圖像表示看問題，不難明白無可能完全沒有干擾（爲什麼？），能夠做到最好的是每次比較兩個用者的頻道或其移位時，頂多只有一處干擾，我們要求做到這種理想情況。自然地，我們定義以下一種叫做理想方陣的研究對象。一個 $N \times N$ 二元方陣 A 的每列有且只有一個 1（1 表示塗了色的格，0 表示沒有塗色的格）。A 的 (u,v)-平移是把 A 向上移 u 位，向右移 v 位，如果 A 和它的任何 (u,v)-平移（即是 $(u,v) \neq (0,0)$ (模 N)）相疊的項頂多只有一個 1，便把 A 叫做一個 N 階理想方陣。[P.V. Kumar, On the existence of square dot-matrix patterns having a specific three-valued periodic correlation function, *IEEE Trans. Inform. Theory*, IT-34 (1988), 271-277.] 再化妝一下，一個 N 階理想方陣可以寫成一個叫做平面函數的研究對象，即是一個從 $\mathbb{Z}/N\mathbb{Z}$ 到 $\mathbb{Z}/N\mathbb{Z}$ 的影射 f，無論 v 取任何非零值， f_v 都是全射，這兒的 f_v 也是從 $\mathbb{Z}/N\mathbb{Z}$ 到 $\mathbb{Z}/N\mathbb{Z}$ 的影射，定義爲 $f_v(j) = f(j-v) - f(j)$。

其實，f 就是用以刻畫方陣首行的非零項位置。由（32241）得來的五階方陣並不是理想方陣，由 $\mathbb{Z}/5\mathbb{Z}$ 到 $\mathbb{Z}/5\mathbb{Z}$ 的對應函數 f：

$$f(0) = 3, f(1) = 2, f(s) = 2, f(3) = 4, f(4) = 1 \text{ ，}$$

並不是平面函數（見圖 11）。

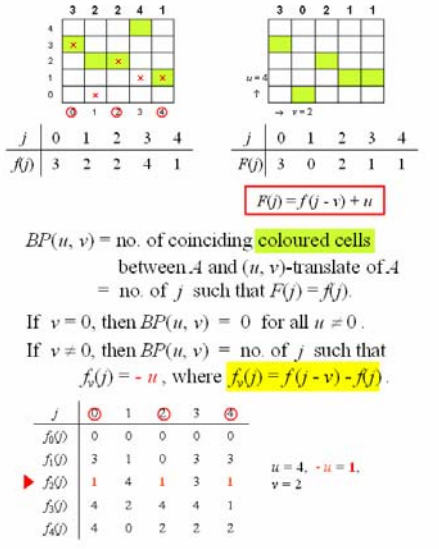

圖 11

由（31344）得來的五階方陣是一個理想方陣，它對應的函數 f 是一個平面函數（見圖 12）。

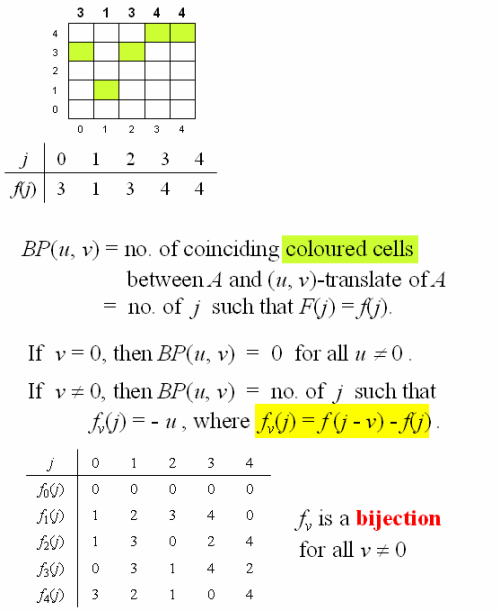

圖 12

事實上，那個對應的函數 f 是個二次多項式，就是 $f(j) = 2j^2 + j + 3$（模 5）。明顯地，如果 N 是個奇質數，對任意 $a \neq 0$ 和任意 b, c， $f(j) = aj^2 + bj + c$ 給出一個平面函數，也就給出一個 N 階理想方陣，也就提供了一套 N 個用者的頻道設計。

不難證明，沒有偶數階的理想方陣。在一九八九年我和馮振業、馬少麟證明了如果存在一個 N 階理想方陣，則 N 必定沒有重複的質因子〔C.I. Fung, M.K. Siu, S.L. Ma, On arrays with small off-phase binary autocorrelation, *Ars Combinatoria*, 29A (1990), 189-192.〕。順帶提一句，馬少麟是我的第一位博士研究生，從一九八五年的畢業論文開始，他在組合設計方面做出了很多極好的成果，我沒能解答的問題差不多都由他完成了。包括他在內的一群研究生與我一同研讀數學，在過去三十年來一直是我在數學研究工作上的支柱，我從他們得到的遠比我能教給他們的爲多，除了學術意念交流以外，更重要者是他們予我動力，使我保持研習熱情。

一個驚喜是理想方陣（或平面函數）與有限射影平面有密切關連，這或許解釋了爲何有平面函數這個名字。從一個 N 階理想方陣我們能構作一個 N 階射影平面，與其詳敘述箇中細節，不如就利用一個具體的三階理想方陣——相應於（122）——構作一個三階射影平面（見圖 13），這個具體例子已經說明了一般的構作方法。

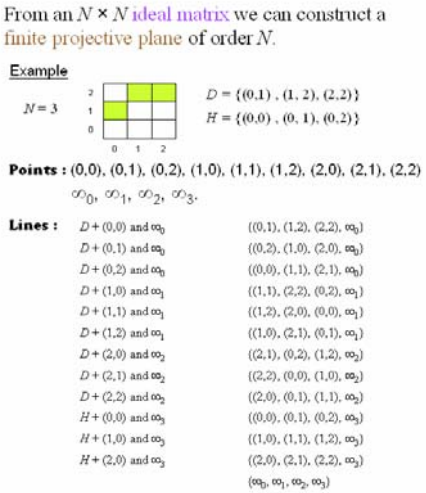

圖 13

由於有個著名的猜想說有限射影平面的階是質數的冪，我們便猜想理想方陣的階也是質數的冪。前面提及我們已經證明了理想方陣的階沒有重複的質因子，因此我們猜想理想方陣的階必定是個質數，而且相應的平面函數必定是個二次多項式。當時我們不曉得原來日本數學家平峰豐（Yutaka Hiramine）已經證明了後面那部份〔Y. Hiramine, A conjecture on affine planes of prime order, *J. Comb. Theory*, A-52 (1989), 44-50.〕，他也證明了理想方陣的階不能形如 $3p$，p 是個質數〔Y. Hiramine, Planar functions and related group algebras, *J. Algebra*, 152 (1992), 135-145.〕，馬少麟再進一步證明了理想方陣的階不能形如 pq，p 和 q 是質數〔S.L. Ma, Planar functions, relative difference sets, and character theory, *J. Algebra*, 185 (1996), 342-356.〕。由論文的題目可以窺視理想方陣（平面函數）與抽象代數的密切關連。以我所知，這方面最新近的結果是七年前布洛克烏斯、容吉尼科、施密特的定理：如果 G 是一個 n 階射影平面的 n^2 階可換直射群，則 n 是個質數的冪〔A. Blockhuis, D. Jungnickel, B. Schmidt, Proof of the Prime Power Conjecture for projective planes of order n with

abelian collineation groups of order n^2, *Proc. Amer. Math, Soc*., 130 (5) (2001), 1473-1476.〕。由理想方陣（或平面函數）構作出來的射影平面有特定性質的直射群，從上述定理可以推論理想方陣的階必爲質數，解答了我們將近二十年前提出來的問題。

5．像我一樣，國偉兄也是被離散數學吸引過去而“半途出家”，他原本師承熊菲爾（Joseph Schoenfield）專攻數理邏輯。熊菲爾師承懷爾特（Raymond Wilder，1896-1982），相信國偉兄受到懷爾特的影響也不少。說來真巧，我也是從懷爾特的著作學到很多東西，他的觀點對我日後的學術生涯有頗強的影響。

最先碰上懷爾特是在大學二年級讀了他的《數學基礎導論》（*Introduction to the Foundations of Mathematics*, 1952; 2nd ed. 1965），但深受影響卻是過了十年後讀到他的另一本著作《數學概念的演化初論》（*Evolution of Mathematical Concepts：An Elementary Study*, 1968），再過幾年後，又讀到其續篇《數學文化體系》（*Mathematics as a Cultural System*, 1981）。請注意書名中用了「文化」（culture）這個辭，懷爾特採用人類學的角度去探討數學是怎樣的一門活動和學問。

固然，早於二十世紀四十年代，著名數學史家斯特羅伊克（Dirk Jan Struik, 1894-2000）已經明確指出數學與社會及文化的密切關係。他在《簡明數學史》（*A Concise History of Mathematics*, 1948）的導言裏開宗明義提及「每個時代的數學興衰與一般文化及社會氛圍有關係（references to the general cultural and sociological atmosphere in which the mathematics of a period matured---or was stifled）」。何謂文化呢？英國科學家、文學家斯諾（Charles Percy Snow, 1905-1980）在一九五九年五月給了一個著名的講演，題爲《兩種文化》（The Two Cultures），討論科學家與人文學者之間本來不應該存在的鴻溝，在文內他提出了「文化」的兩種含意，一方面是英國詩人柯爾律治（Samuel Taylor Coleridge, 1772-1834）所謂「那些表徵人性本質和才能的和諧發展（the harmonious development of those qualities and faculties which characterize our humanity）」，另一方面是指「生活於同一環境，由共同習慣、想法和生活方式聯結起來的群體（a group of persons living in the same environment, linked by common habits, common assumptions, a common way of life）」。說得白一些，爲了提升個人與社群的生活素質，人們在多方面努力有所成就，表現爲各種形式，包括宗教、哲學、道德、法律、教育、政治、經濟、風俗、禮儀、建築、藝術、音樂、戲劇、文學、科學、數學、工藝技術，這龐雜的總和，就是「文化」。德國哲學家史賓格勒（Oswald Spengler, 1880-1936）在其名著《西方的沒落》（*Der Untergang des Abendlandes, Volume 1 / 2*, 1918 / 1922）論及歷史上各個文化均有興衰，如生物生長，也如季節轉變，他用了整整一章談及數學，因爲他認爲數學乃重要的文化表徵，不同文化裏數學的發展及風格是探討該文化的關鍵題材。

懷爾特進一步闡明這種觀點，以人類學的角度把數學看成是某個主文化體系（host culture）裏的子文化體系（subculture）。一九五零年在美國麻省劍橋舉行的四年一度數學家大會上他作了一個主要發言，題爲「數學的文化基礎（The Cultural Basis of Mathematics）」〔文本刊於 *Proceedings of ICM 1950*, 258-271〕，提到了兩個重點：

> 「文化是由風俗習慣、禮儀、信念、工具、傳統習俗、等等組成，可以說是某一群體的文化元素，〔…〕一般而言，這並非是一成不變的，卻與時變更，不妨叫做一種 “文化流” (“culture stream”)〔…〕。」
>
> 「數學家之間共享一種 “數學的文化”，我們大家受到它的影響，同時也影響了它。〔…〕數學發展的情況及方向由一種普遍綜合的文化張力決定，這種張力既產自數學內部，也來自數學外部。」

懷爾特的意思是把數學嵌於一個更大的主文化體系裏面，這個主體系裏面有不同的子體系，數學只是其中之一，還有很多別的。數學子體系與某些子體系互相影響較多，例如哲學、工程、自然科學、生物科學、資訊科學、社會科學，懷爾特把這種影響稱作外部（或環境）張力（external/environmental stress）。但數學子體系自身也產生問題，影響著自身的發展，懷爾特把這種影響稱作內部（或遺傳）張力（internal/hereditary stress）。固然，這只是眾多主文化體系其中一個吧，在不同地域、不同時代、不同民族中有不同的主文化體系，它們之間也互相影響，史賓格勒討論的就是那眾多的主文化體系。讓我試以下面的示意圖（見圖 14）粗略地概括懷爾特的觀點。

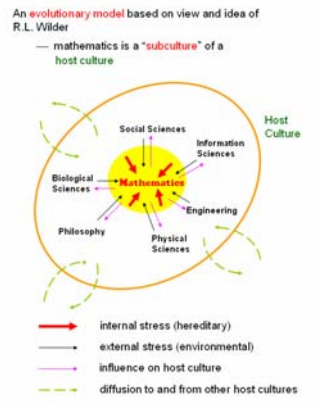

圖 14

從文化角度看數學，對數學教育是有益處和幫助的。約翰遜（Julian Johnson）在他的書《誰需要古典音樂呢？文化選擇與音樂價值》（*Who Needs Classical Music? Cultural Choice and Musical Value*, 2003）裏論及古典音樂受到大眾冷落，情景與數學無異*。了解箇中因由，讓學生看到數學除卻技術內容外更廣闊的一面，

*較詳細的敘述可參看書內另一篇文章：「數學、數學教育和滑鼠」，第二節和第六節。

或者能夠使他們增強學習數學的動機。其實，除了精神方面，在內容方面音樂跟數學也有相通的地方。德國數學名家外爾（Hermann Weyl, 1885-1955）說過：「我們並非宣稱數學應該享有科學之皇后的特權，有其他科目與數學有同等甚至更高的教育價值。但數學立下所有心智活動所追求的客觀真理標準，科學和技術是它的實用價值的見證。如同語言及音樂，數學也是人類思維的自由創作力之主要表現形式，同時它又是通過建立理論以認識客觀世界的一般工具。所以數學必須繼續成爲我們要教授給下一代的知識和技能中的基本成份，也是我們要留傳給下一代的文化中的基本成份。（We do not claim for mathematics the prerogative of a Queen of Science, there are other fields which are of the same or even higher importance in education. But mathematics sets the standard of objective truth for all intellectual endeavors; science and technology bear witness to its practical usefulness. Besides language and music, it is one of the primary manifestations of the free creative power of the human mind, and it is the universal organ for world-understanding through theoretical construction. Mathematics must therefore remain an essential element of the knowledge and abilities which we have to teach, of the culture we have to transmit, to the next generation.）」

6．同樣地，美術跟數學也有相通的地方。要好好討論這個話題，既非一個四十分鐘的講演可以兼顧，更非我的學識修養所能道出箇中微妙。不過我知道國偉兄近年對繪畫透視很感興趣，不如就單單拿透視學和射影幾何說一兩句，作爲講演的結尾一節吧。

早期的繪畫，沒有考慮到如何把三維景象在二維平面展示，例如在公元十世紀或十一世紀有一張描寫英國人晚宴的畫，桌子和上面的餐具，就像側掛在一旁，現代人看了會感到有點滑稽（見圖 15）。即使到了十五世紀，還可以在某些畫中找到不協調的透視畫法，例如有一張畫名叫「聖埃德蒙的誕生（The birth of St. Edmund）」，房間的陳設予人立體透視感，但地面的階磚，卻露出了馬腳（見圖 16）！〔圖 15 和圖 16 皆摘自：Lawrence Wright, *Perspective in Perspective* , 1983。〕

圖 15

圖 16

歐洲文藝復興期的畫家，在十五世紀期間已經提出透視畫法，最早的有亞爾貝蒂（Leone Battista Alberti, 1404-1472）的《論繪畫》（*De pictura*, 1435）及弗蘭切斯卡（Piero della Francesca, 1412-1492）的《繪畫透視法》（*De prospectiva pingendi*, 約 1470 年），後來又有達芬奇（Leonardo da Vinci, 1452-1519），丟勒（ Albrecht Dürer, 1471-1528）諸人的論述與美術作品，使透視法在西方繪畫成爲普遍不過的手法。上述的畫家都是多面手，身兼藝術家和數學家，庫利奇（Julian Lowell Coolidge, 1873-1954）寫了一本《業餘愛好者的數學》（ *The Mathematics of Great Amateurs*, 1949），裏面便有三個章節描述他們的成就。

丹麥數學史家安德遜（Kirsti Andersen）最近出版了一本內容豐富翔實的書：《藝術的幾何：由亞爾貝蒂到蒙日的數學透視理論》（*The Geometry of an Art: The History of the Mathematical Theory of Perspective from Alberti to Monge*, 2007），書長八百多頁，介紹西方繪畫透視理論的發展經過。她把意大利人蒙特侯爵圭多巴爾迪（Guidobaldo Marchese del Monte, 1545-1607）稱作繪畫透視理論之父，因爲圭多巴爾迪在《透視論六卷》（*Persepctivae libri sex*, 1600）提出了“消失點”（vanishing point）的概念，“消失點”在現代射影幾何具有重要的數學意義。

中國繪畫也不是完全沒有運用透視法，例如北宋李誡（1035-1110）的《營造法式》（約 1100 年）書內有好些插圖都有某種透視味道，但好像仍未有“消失點”的概念。到了清代年希堯（？-1738）從當時在宮廷任職的意大利畫家郎世寧（Giuseppe Castiglione, 1688-1766）那兒學西洋透視論，加上自己用心琢磨，寫成《視學》一書（1729 年 / 1735 年），書內有言：「視學之造詣無盡也，予曷敢遽言得其精蘊哉，雖然予究心於此者三十年矣。…近得數與郎先生諱石寧者往復再四研究其源流，凡仰陽合覆，歪斜倒置，下觀、高視等線法，莫不由一點而生。迨細究一點之理，又非泰西所有而中土所無者。…予復苦思力索，補縷五十餘圖，並爲圖說以附益之。…」

在西方，從繪畫透視論衍生了射影幾何。首先有法國工程師、建築師、數學家德札格（Girard Desargues, 1591-1661）在十七世紀三十年代寫了兩部重要著述，卻可能因爲他寫得不易明白，表述方式又介乎“工匠式幾何”與“理論化幾何”之間，兩不討好！也可能因爲他的思想比同時代的想法前行了許多，這兩部著述都受不到應有的重視，沒有給發展下去。回頭來看，德札格創立了射影幾何這門數學，但這門數學卻要等待一個半世紀之後，由於法國數學家蒙日（Gaspard Monge, 1746-1818 ）和他的門生龐斯列（Jean Victor Poncelet, 1788-1867）的工作成果才終於融入數學主流，尋且成爲十九世紀的重要數學領域（見圖 17）。懷爾特在《數學文化體系》一書中花了一章討論數學演化的“奇點”，即是那些本應發展卻停滯不前甚或消聲匿跡的意念。他採用的一個主要例子，便是德札格建立射影幾何這個案例。

圖 17

德札格發現了一條非常漂亮的定理：如果兩個三角形 $ab\ell$ 和 DEK 滿足 Da 、 Eb 、 $K\ell$ 有共點 H，而且 ab 和 DE 相交於 c， $b\ell$ 和 EK 相交於 f， $a\ell$ 和 DK 相交於 g，則 c、f、g 共線。（見圖 18）

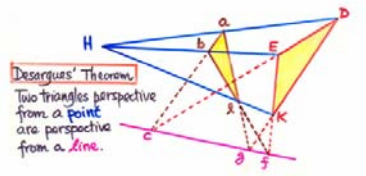

圖 18

除了是一條在平面歐氏幾何裏非常漂亮的定理，德札格定理還有它更深刻的意義，叫人詫異。利用德札格定理我們能夠對看似只有點和線及點線關聯的幾何賦予座標，以方便計算。無獨有偶，與德札格同時代的法國哲學家、數學家笛卡兒（René Descartes, 1597-1650）從方法論出發，也把幾何和代數結合，演化成後世的解析幾何，亦稱座標幾何（雖然笛卡兒從來沒有在他的著作裏提及座標系統）。其實，德札格和笛卡兒兩個是好朋友，大家在巴黎的時候都參加了圍繞在梅森 (Marin Mersenne, 1588-1648) 身邊的數學興趣小組，他們兩個既有會面，也互有書信往來，不知道私下談論數學時，大家有沒有交換設置座標系統的心得呢（見圖 19）？

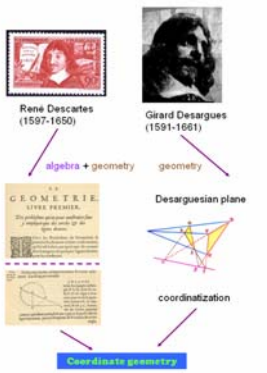

圖 19

7．在第五節開首我提過國偉兄師承熊菲爾，而熊菲爾則師承懷爾特。如果再往上追溯師源，可以尋到十九世紀法國幾何學家、數學史家沙勒（Michel Chasles, 1793-1880），而沙勒的老師是另一位法國數學家泊松（Siméon-Denis Poisson, 1781-1840）。泊松有另一名學生，是德國數學家狄利克雷（Peter Gustav Lejeune Dirichlet, 1805-1859），從這一條線尋下去，我竟然在其中找到自己（見圖 20）。說起來我與國偉兄原來有 “學術親屬”的緣份，他比我要高好幾輩！

圖 20

國偉兄的“師祖”泊松留下了一句話：「生活中只有兩件值得做的事，發現數學新知和講授數學（Life is good for only two things, discovering mathematics and teaching mathematics.）」國偉兄對於這項訓誨當然身體力行，不過，以我推測，國偉兄很可能會把這句話修改爲：「生活中有兩件值得做的事，發現數學新知和講授數學，還有更多別的。（Life is good for two things, discovering mathematics and teaching mathematics, and many more other things.）」國偉兄，祝您六十生辰快樂，生活愉快，多姿多彩！

****

〔這篇是 2008 年 8 月在台灣新竹國立交通大學舉行的第十七屆組合數學暨新苗研討會上的講演，也是藉此慶祝李國偉教授的六十歲生辰，並向他對離散數學、數學史、數學普及、文化推廣工作的貢獻表達敬意。〕