組合學上一些待決的問題

王子俠

本文係作者於六十八年八月八日應國立清華大學之邀對參加暑期進修之國中教員所作之演講，今將原稿寄給數學傳播，希望能藉此引起國內數學界對組合學更廣泛的興趣及更深入的研究。

1. 導　引

今天我要向各位介紹的是組合學上一些尚未解決的問題。**組合學** (Combinatorics; 或稱 Combinatorial Mathematics, Combinatorial Analysis, Combinatorial Theory) 在數學上並非是後起之秀，它的一些基本概念，諸如排列 (Permutation) 及組合 (Combination) 可以說是源遠流長，（據說在西元前 2200 年，中國人就發現了 3×3 的魔方陣 (Magic Square)），但在過去，它一直未受到數學家的普遍重視，主要是因爲大家認爲它不過是一些數學遊戲 (Mathematical Games) 的雕蟲小技。這種態度，當然無可厚非，因爲許多組合學上的問題原本是從消遣數學 (Recreational Mathematics) 產生，雖然經過研究分析後，大部份都演變成純粹的數學問題。但到了最近幾十年，組合學終於翻身而受到數學界的普遍重視，它的一些論題，像八爪魚的脚，伸向數學上許多不同的分支，於是乎現在有了 Combinatorial Lattice Theory, Combinatorial Group Theory, Combinatorial Matrix Theory, Combinatorial Set Theory 以及 Combinatorial Topology 等等。造成這個「雨後春筍」局面的原因當然很多，但最重要的有三個: ㈠組合學本身的許多論題，被發現是彼此關連，息息相通的。㈡組合學上的許多觀念和技巧被發現可以應用到許多純數學以外的 fields 上去，諸如統計學，社會學，生物學，心理學以及一些交通問題。㈢電子計算機的問世及日新月異。

要給組合學下個定義，就如要給數學下個定義一樣困難，但概略地來講，它討論的不外乎是一些 Counting, Selection 及 Arrangement 之類的問題。它的範圍包括甚廣，例如 Codes, Graphs, Ramsey Theory, Combinatorial Designs, Finite Boolean Algebra, Generating Functions, and Recursions, Finite Geometries, Matroids, System of Distinct Representatives 以及 Combinatorial Matrix Theory 等等。

組合學的最大特色是: 許多問題容易敍述，容易了解（當然並不一定容易解決，事實上往往正相反）。在這點上，它和古典數論非常相似。舉個例來說，近百年來，數學家所謂的三大難題是(1)Fermat's Last Theorem (2) Riemann Hypothesis 以及(3)4-Color Theorem 其中的(1)是衆人皆知的數論名題; (2)也和數論有密切的關係而(3)便是組合學中一支所謂圖形學 (Graph Theory) 上一世紀以來未決之臆測，這個臆測一直到1976年才被 Illinois 大學的兩位教授 K. Appel 及 W. Haken 證明正確（註）。總之，這三個問題，都是敍述簡單明瞭，而解答卻難得出乎意料。

（註）四色難題的證明，雖然是數學家在數學史上的一大勝利，但在精神上，人類却是吃了一次敗仗，因爲他們的證明，除了高深的理論外，最後還要用 1200 小時的 Computer Time。身爲"萬物之靈"的人類所不能解決的問題，居然要靠沒有靈性的機器幫忙，才能解決，難怪許多人對這個問題仍然認爲是尚未"蓋棺論定"。

2. 問題簡介

（I）第一個我要介紹的是 Hadamard Matrix 的問題；大家都知道，Hadamard 是法國數學家，曾應邀來中國講過學。Hadamard Matrix 的起源是 Hadamard 的一個不等式:

定理 (Hadamard's Inequality): 如果$A=(a_{ij})$是個 $n\times n$ 的實矩陣，而滿足，對所有的 i, j, $|a_{ij}|\leqslant 1$ 的條件，則 $|detA|\leq n^{n/2}$. (此處之 det 表行列式) 等號成立若且唯若對所有的 i, j, $a_{ij}=\pm 1$ 而滿足 $AA^t=nI_n$ (此處之 A^t 表示A之 transpose)

觀察使等號成立的條件，很自然的導致下面的定義:

定義: 一個 $n\times n$ 的實矩陣$H=(a_{ij})$，若滿足，對所有的 i, j, $a_{ij}=\pm 1$ 而且 $HH^t=nI_n$ 的條件，則稱爲一個 Hadamard Matrix (簡稱 H-Matrix) of order n。

如果我們用 R_i 表H的第 i 列 (row), $i=1,2,\cdots,n$, 用δ_{ij} 表 Kronecker's delta, 用 $<R_i, R_j>$ 表 R_i 與 R_j 的內積 (Inner Product), 則從 $(HH^t)_{ij}=(nI_n)_{ij}=n\delta_{ij}$ 得到，對所有的 $i\neq j$, $<R_i, R_j>=0$, 而對所有的 i, 有$<R_i, R_i>=n$. 因爲，$a_{ij}=\pm 1$, 故$<R_i, R_i>=n$ 自動滿足。所以我們看出來，如果$a_{ij}=\pm 1$, 則 $H=(a_{ij})$ 是個 H-Matrix 的充分且必要條件是對所有的 $i\neq j$, $<R_i, R_j>=0$, 也就是說，任何兩個H相異列的內積，心須是零。

很明顯地，如果我們交換一個 H-Matrix 的任何兩行 (Column) 或兩列，或者用-1遍乘一行或一列，則 H-Matrix 的性質並不改變，所以我們可以假定第一行及第一列的元素全等於 1，這樣的 H-Matrix 稱爲**正規化**的 (Normalized) H-Matrix 下面的圖一及圖二是 1×1 及 2×2 的正規化的 H-Matrix

〔1〕 $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\left(\begin{array}{c|c} 1 \quad 1 \cdots\cdots & \cdots\cdots\cdots 1 \\ 1 \quad 1 \cdots & -1 \; -1 \; \cdots -1 \\ 1 & \\ \underbrace{\quad t \text{ 個 } 1's \quad} & \underbrace{\quad t' \text{個} 1's \quad} \\ \vdots & \\ 1 & \end{array}\right) \leftarrow R_3$$

圖一　　圖二　　圖三

如果我們考慮一個 $n\times n$ 的正規化的H-Matrix, $n\geq 3$ 則顯然n必須是偶數，交換它的行，我們可以假定，$R_2=(1,1,\cdots,1,-1,-1,\cdots,-1,)$ 其中前 $n/2$ 個分量 (Component) 都是 1，而後 $n/2$ 個分量都是-1 如果以 t 表 R_3 裏前 $n/2$ 個分量中 1 的個數，以 t' 表 R_3 裏後 $n/2$ 個分量中 1 的個數，那麼因爲$<R_1, R_3>=0$，我們得到

$$t+t'=\frac{n}{2} \text{——(1)}$$

同樣地，因爲$<R_2, R_3>=0$，我們得到

$$(n/2-t)+t'=\frac{n}{2} \text{——(2)}$$

由(1)式及(2)式，我們便得到$n=4t$, 也就是說$n\equiv 0\ (mod\ 4)$所以我們證到如果是H一個 $n\times n$ 的 H-Matrix, 則$n=1$, 2 或者是 4 的倍數；但是反過來說，是不是對所有 4 的倍數n，都存在一個 $n\times n$ 的 H-Matrix 呢？ Hadamard 認爲是對的，這就是有名的 Hadamard 臆測 (Conjecture)，這是一個非常困難的問題，目前雖然有種種不同的方法來造 (Construct) 許多 infinite Classes 的 H-Matrices, 而且對於所有$n\leqslant 264$, $n\equiv 0\ (mod\ 4)$, $n\times n$ 的 H-Matrix 都已發現，但這些 Constructions 都相當複雜，往往要用到數論及有限體 (Finite Field) 的理論，而且無一致性。所以要完全解決這個問題，恐怕還路途遙遠。順便要一提的是，H-Matrix 的問題，並非是獨立的；例如它和一種叫作 **B. I. B. D.** 的 **design** 就

有密切的關連。

(II) 我今天要介紹的第二個問題是所謂的 Sum-Free Sets of Integers，顧名思義，一個整數的集合 S 如果滿足對所有的 $a, b \in S$，恆有 $a+b \notin S$，則稱之爲 *Sum-Free*（簡稱 S.F.，這個概念的起源是 1916 年 I. Schur 氏爲了研究 $x^m+y^m \equiv z^m \pmod{p}$ 的解（某種形式的 Fermat's Last Theorem）而證到的一個結果；如果將 $\{1, 2, \cdots, \lfloor k!e \rfloor\}$ 這個集合（此處之〔 〕表最大整數函數）任意分解（Partition）成 k 個子集合，則至少有一個子集合不是S.F.。換句話說，如果我們要將 $N_n=\{1, 2, \cdots, n\}$ 分解成 k 個S.F. 集合，則 $n \leq \lfloor k!e \rfloor - 1$。但這個上限，當 k 大時，非常不精確。由Schur的結果，我們可以定義 $f(k)$ 爲滿足使得 $\{1, 2, \cdots, f(k)\}$ 可以分解成 k 個S.F. 集合的最大正整數，則不難看出 $f(1)=1$，$f(2)=4$ 稍微花一點時間也可以驗證出 $f(3)=13$，而 $N_{13}=\{1, 4, 10, 13\} \cap \{2, 3, 11, 12\} \cap \{5, 6, 7, 8, 9, \}$ 是一個分解 N_{13} 爲三個S.F. 集合的方法。在 1961 年，Jet Propulsion Laboratory 的 Baumert 氏靠了電子計算機的幫助決定出 $f(4)=44$。而對於 $k \geq 5$ 時，$f(k)$ 之值，至今未定。在 1977 年，E. Wang（即筆者本人）考慮下面的問題：如果**固定** n 和 k 的值，那麼從 N_n 裏可以選出多大的一個子集合 S 使得 S 可以分解成 k 個 S.F. 集合？說得更精確一點，如果 $g(n, k)=max\{|S|: S \subset N_n, S=S_1 \cap S_2 \cap \cdots \cap S_k; S_i$ 是 S.F., $i=1, 2, \cdots, k\}$ 那麼 $g(n, k)$ 的值是如何呢？舉例來說，當 $k=1$ 時，所有從 1 到 n 的奇數很顯然地構成一個 S.F. 集合，所以

$$g(n, 1) \geq \left\lceil \frac{n+1}{2} \right\rceil = n - \left\lfloor \frac{n}{2} \right\rfloor$$

事實上，不難證明等號成立。

定理： $g(n, 1)=\left\lceil \frac{n+1}{2} \right\rceil$

證明： 假定 $A=\{a_1, a_2, \cdots, a_t\} \subset N_n$ 是個 S.F. 集合，$1 \leq a_1 < a_2 < \cdots < a_t \leq n$ 那麼下面 $2t-1$ 個 N_n 中的數，全部相異，$a_1, a_2, \cdots, a_t, a_t-a_1, a_t-a_2, \cdots, a_t-a_{t-1}$ 故有 $2t-1 \leq n$，所以 $t \leq \left\lfloor \frac{(n+1)}{2} \right\rfloor$

那麼 $g(n, 2)$ 的值是多少呢？前面我們提到 $f(2)=4$ 這個理由非常簡單，假定 A 和 B 是兩個空集合而我們想把 $1, 2, \cdots$ 分配到這兩個集合，使得它們變成 S.F. 集合。則 $1 \in A \Rightarrow 2 \notin A \Rightarrow 2 \in B \Rightarrow 4 \notin B \Rightarrow 4 \in A \Rightarrow 3 \notin A \Rightarrow 3 \in B$ 所以 $A=\{1, 4\}$, $B=\{2, 3\}$。很明顯地，5 不能被放進 A 或者 B。所以 $f(2)=4$ 由此我們可以想到，如果將 N_n 裏面 5 的倍數去掉，而將其他的數依照它們被 5 除所得的餘數是 1, 4 或是 2, 3 分成兩個集合，也就是說：$S_1=\{a: 1 \leq a \leq n, a \equiv 1, 4 \pmod{5}\}$，$S_2=\{b: 1 \leq b \leq n, b \equiv 2, 3 \pmod{5}\}$ 那麼顯然 S_1 及 S_2 都是 S.F. 所以我們便得到 $g(n, 2) \geq n - \lfloor n/5 \rfloor$ 事實上，我認爲等號在此成立。

臆測 對所有的 n，$g(n, 2)=n-\lfloor n/5 \rfloor$

在1977年，筆者和另外一位加拿大的數學家H. Abbott 用相當複雜的方法證明了對於所有 $n \leq 54$，這個臆測都成立。但對一般的 n 至今未能解決（註）。如果這個臆測可以證到，那麼更進一步可以作

$$g(n, k)=n-\left\lceil \frac{n}{f(k)+1} \right\rceil$$

的臆測。當然，解決 $k=2$ 的情形，應該是第一步。順便要一提的是 S.F. 集合的問題與其他許多組合學上的題目，諸如 Ramsey Number 等等，都有密切的關連。

(III) 今天我所要介紹的最後一個題目是在 Combinatorial Matrix Theory 非常有名而已有 50 多年歷史的 van der Waerden 臆測。在介紹它之前，首先讓我們來定義所謂的 Permanent Function. 對於任意一個 $n \times n$ 的矩陣 $A=(a_{ij})_{n \times n}$，A 的 Permanent 之值是定義作

$$Per(A)=\sum_{\sigma} \prod_{i=1}^{n} a_{i\sigma(i)},$$

註：這個臆測在本文付印前已由本所的胡門昌教授證到，他的證明將發表在 Proceedings of American Mathematical Society。

此處之 σ 是 Symmetric Group of degree n 裏面任意一個元素；也就是說，σ 是任何一個在 $\{1,2,\cdots,n\}$ 上面的排列。（對於一般 $m\times n$ 的矩陣 A, $m\neq n$, $Per(A)$ 也可以定義，但我們此處用不到。）大家一定很快就注意到這個定義和行列式

$$det(A)=\sum_{\sigma}(sgn\sigma)\prod_{i=1}^{n}a_{i\sigma(i)}$$

的定義非常相似（此處之 $sgn\sigma=\begin{Bmatrix}1 & if\ \sigma\ is\ even\\ -1 & if\ \sigma\ is\ odd\end{Bmatrix}$）只不過是去掉 $sgn\sigma$ 這個 factor。但失之毫釐，差之千里，這些微之差，使得 det 和 Per 相去甚遠。乍看之下，也許會認爲 $Per(A)$ 較 $det(A)$ 容易計算，但事實上，正相反。最大的原因是行列式的一些重要性質，Per 都不滿足，例如 $Per(AB)\neq Per(A)Per(B)$。另外，任何兩行或兩列相同則行列式之值爲零這個性質對 Per 也不成立，舉例說，如果 A 是一個每一列都是 $R_i=(1,2,\cdots,n)$ 的 $n\times n$ 矩陣，$i=1,2,\cdots,n$，則，$det(A)=0$，但 $Per(A)=(n!)^2$。因爲這些原因，使 Per 至少在表面上變成了一個純粹的**組合量** (Combinatorial Quantity)，而不像行列式一樣，具有種種**代數性質** (Algebraic Property)。於是乎，它的計算就變得非常困難。雖然像行列式一樣，它也可以用降階展開，或用更一般化的 Laplace expansion formula，但一般來說，只有當 A 是相當特殊的矩陣時，$Per(A)$ 才可以算出。其次，我們須要一個定義。

定義：一個 $n\times n$ 的實矩陣 $A=(a_{ij})_{n\times n}$，如果滿足（i）對所有的 $i,j,a_{ij}\geq 0$，（ii）對所有的 i，$\sum_{j=1}^{n}a_{ij}=1$；對所有的 j，$\sum_{i=1}^{n}a_{ij}=1$，這兩個條件，則稱爲**雙重隨機** (doubly stochastic, 或簡稱 d.s.) 矩陣。

這種矩陣是從統計學及或然率的理論裏產生出來的。例如 $n\times n$ 的 identity matrix $\mathbf{I}_n$，所有的排列矩陣 (Permutation Matrix) 以及所有元素全是 $1/n$ 的 $n\times n$ 矩陣 $\mathbf{J}_n$ 等等，都是 $d.s.$ 矩陣的例子。如果我們用 Ω_n 來表示所有 $n\times n$ $d.s.$ 矩陣的集合，則不難驗證出(i)$A\in\Omega_n B\in\Omega_n,\Rightarrow A\cdot B\in\Omega_n$ (ii)$AJ_n=J_nA=J_n$，對所有的 $A\in\Omega_n$。事實上，下面這個定理告訴我們，Ω_n 是一個以所有排列矩陣作爲頂點 (Vertices) 所構成的 Convex Polyhedron.

定理 (Birkhoff)：如果 $A\in\Omega_n$ 則可以找到一組排列矩陣 $P_1,P_2,\cdots,P_k$ 及一組實數 $\lambda_i\geq 0$，$i=1,2,\cdots,k$ $\sum_{i=1}^{k}\lambda_i=1$ 使得 $A=\sum_{i=1}^{k}\lambda_iP_i$

$d.s.$ 矩陣的理論，包含甚廣，例如它和不等式理論中的 Majorization of Vector 就有密切的關係。但我們今天無法詳細討論。現在，我們要進入主題，也就是連接 d.s. 矩陣及 Permanent 的一個臆測。

臆測 (Van der Waerden, 1926)：對所有的 $A\in\Omega_n$，$Per(A)\geq n!/n^n$ 等號成立若且唯若 $A=J_n$

對於 $n=1,2$，這個臆測，很容易驗證，例如當 $n=2$，如果 $A\in\Omega_2$，則

$$A=\begin{bmatrix}x & 1-x\\ 1-x & x\end{bmatrix}$$

故 $Per(A)=x^2+(1-x)^2$. 從而

$$Per(A)\geq\frac{2!}{2^2}\Longleftrightarrow x^2+(1-x)^2\geq\frac{1}{2}\Longleftrightarrow 2x^2+2(1-x)^2\geq 1\Longleftrightarrow 4x^2-4x+1\geq 0\Longleftrightarrow(2x-1)^2\geq 0$$

顯然地，等號成立，若且唯若 $x=1/2$；也就是說 $A=J_2$。但當 $n=3$ 時，因爲有 4 個變數，直接驗證已相當困難，而在 1959 年，由兩位美國數學家 M. Marcus 及 M. Newman 首先證到。然後在1968年，美國的 Eberlein 及 Mudholker 二人證明了 $n=4$ 的情形；$n=5$ 的情形則在次年 (1969)，由 Eberlein 獨力解決；至於 $n\geq 6$ 的一般情形，除了一些部份結果外，至今未決。

3. 結　論

組合學包羅甚廣，未決之問題，多如天上繁星，上面所舉，不過其中三例，對這些問題有興趣的人，（或對一般組合學有興趣的人）可以參考我剛才所發的 references 上面所列的書和論文；若有疑難之處，歡迎各位寫信或直接到中央研究院數學研究所和我聯絡，可以共同討論，研究；謝謝大家。

REFERENCES

(The number(s) at the end of each reference , indicates the fact that it contains discussions of the corresponding topic(s) given in this talk)

[1] H. L. Abbott and E. T. H. Wang, *Sum-free sets of integers*, Proc. Amer. Math. Soc. **67**(1977), 11-16. (2)

[2] M. Hall. Jr. *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967. (1)

[3] M. Marcus and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*, Boston, 1964. (3)

[4] H. Minc, Permanent, *Encyclopedia of Mathematics and its Applications*, Vol. **6** Addison-Wesley, 1978. (3)

[5] G-C Rota (editor), *Studies in Combinatorics* (*MAA Studies in Mathematics*, Vol. **17**.), Mathematical Association of America, 1978. (3)

[6] H. Ryser, *Combinatorial Mathematics*, *Carus Math. Monograph.* No. **14** Mathematical Association of America, 1963. (1, 3)

[7] A. P. Street and W. D. Wallis, *Combinatorial Theory*: *An introduction*, The Charles Babbage Research Centre, Winnipeg, Canada, 1977. (1, 2)

[8] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics*: *Room squares*, *Sum-free sets*, *Hadamard matrices*, #292, Lecture Notes in Math., Springer-Verlag, Berlin, 1972, (1, 2)

——本文作者爲本所客座專家，本刊編輯委員