數學傳播　36卷1期, pp. 48-63

Hurwitz-Radon 矩陣方程

林開亮

一. 記號約定

本文中考慮的域 F 的特徵不等於 2。

$M(n,F)$　表示係數在 F 中的 n 階方陣的集合, $GL(n,F)$ 表示 $M(n,F)$ 中的可逆方陣的集合。

$\mathbb{R}$ 和 $\mathbb{C}$　分別表示實數域和複數域。

A'　表示矩陣 A 的轉置。

$tr(A)$　表示矩陣 A 的跡。

E　表示單位陣。

$i=\sqrt{-1}$　是虛數單位, 不引起混淆時也作指標使用。

二. 內容簡介

接下來我們將簡單介紹一下本文討論的主要問題和正文的框架結構。

所謂 Hurwitz 矩陣問題, 就是對給定的域 F 以及正整數 n, 求 $M(n,F)$ 中滿足兩兩反交換並且每個矩陣的平方爲 -1 的反對稱矩陣集的最大基數。借助於 Kronecker 符號 δ_{ij}, 這個問題可以表述如下。

設 F 是一個域, 如果 $A_1,\ldots,A_k\in M(n,F)$ 滿足以下 Hurwitz 矩陣方程

$$A_iA_j+A_jA_i=-2\delta_{ij};\qquad A_i'=-A_i \tag{1}$$

則稱它們是 $M(n,F)$ 中的一組 Hurwitz 矩陣。

著名的 Hurwitz 矩陣問題, 就是對給定的 F 以及 n, 求 $M(n,F)$ 中的一組 Hurwitz 矩陣 $A_1,\ldots,A_k$ 的所含的矩陣個數 k 的最大值 $K_F(n)$。

首先我們指出, 這個問題是有意義的。實際上, 我們有下述

引理1. 設 $A_1, \ldots, A_k \in M(n, F)$ 滿足方程

$$A_i A_j + A_j A_i = -2\delta_{ij} \tag{2}$$

則它們是 $F-$ 線性無關的。

證明: 假定 $c_1, \ldots, c_k \in F$ 使得

$$c_1 A_1 + \cdots + c_k A_k = 0$$

對每一個 $i = 1, \ldots, k$, 等式兩邊分別左右乘以 A_i, 並將得到的兩個式子相加, 利用 (2) 得到

$$c_i = 0。$$

即 $A_1, \ldots, A_k$ 線性無關。 □

對於 $F = \mathbb{C}$ 及 $\mathbb{R}$ 的情形, Hurwitz [6] 和 Radon [13] 分別在1920年代前後給出 Hurwitz 矩陣問題解答, 這就是 Hurwitz-Radon 定理。

定理1.

$$K_{\mathbb{C}}(n) = K_{\mathbb{R}}(n) = K(n) = \begin{cases} 2q & q \equiv 0 \pmod 4 \\ 2q-1 & q \equiv 1 \pmod 4 \\ 2q-1 & q \equiv 2 \pmod 4 \\ 2q+1 & q \equiv 3 \pmod 4 \end{cases}$$

其中 q 滿足 $n = 2^q p$, p 是奇數。

這個經典的定理已經有許多證明, 除了 Hurwitz 與 Radon 的原始證明, 還有 Eckmann [3]的有限群表示論證明, 李華宗 [9]的利用 Clifford 代數表示論的證明以及 Shapiro [16]的二次型理論的抽象證明。[1]

我們簡要評述一下 Hurwitz, Radon , Eckmann 和 李華宗的文章。

Hurwitz 早在 1898 年的文章 [5]中就提出了 Hurwitz 問題, 這是關於這個論題的最早文獻。文章 [6]是在他1919年逝世以後發表的。Hurwitz 問題的最一般情形是針對任意的 $m \times n$ 矩陣的, 事實上, 這個問題遠遠沒有解決, 見 Shapiro [16]的論述。對於 $n \times n$ 的情況, Hurwitz 以近乎完美的方式得到了解答。

Radon 的貢獻是給出了 Hurwitz 定理的一個等價表述和獨立證明, Radon 的表述形式—-本質上也就是我們在定理中採取的形式——比 Hurwitz 的表述簡單。

[1] Hurwitz 的原始證明的敍述可以參考黃用諏 [20], Radon 的證明的一個轉述可見 Rajwade [14] 第十章, Eckmann 的證明可見 [18], 李華宗的證明的變體可參看 林節玄 [8] 與 Prasolov [12]。

Eckmann 認識到, Hurwitz 問題對 $\mathbb{R}$ 和 $\mathbb{C}$ 有相同的解這個事實是有限群表示論裡的 Frobenius-Schur 定理[2] 的必然推論, 從而給出了 Hurwitz-Radon 定理的統一表述。

李華宗認識到, Eckmann 的有限群表示證明本質上是群代數的證明, 而那個群代數不是別的, 正是由關係 (2) 生成的 Clifford 代數。此觀點後來被普遍採用,例如林節玄 [8] 的前身, 又如 Atiyah-Bott-Shapiro 的工作。[3]

本文將給出 Hurwitz-Radon 定理的一個比較簡單的證明, 這個證明源於1930年代 Newman [11]和 Von Neumann-Veblen [19]的工作, 並且對任意的特徵不等於 2 的域都適用。我們的證明對實數域 $\mathbb{R}$ 最自然, 所以我們首先考慮這個特殊情況。

我們遵循 Shapiro [16]的基本建議, 引入一個混合型的 Hurwitz 矩陣方程如下

$$\begin{cases} A_i' = -A_i \\ B_k' = B_k \\ A_iA_j + A_jA_i = -2\delta_{ij} \qquad (i,j = 1,\ldots,s;\ k,l = 1,\ldots,t.) \\ B_kB_l + B_lB_k = 2\delta_{kl} \\ A_iB_k + B_kA_i = 0 \end{cases} \tag{3}$$

如果 $A_1,\ldots,A_s,B_1,\ldots,B_t \in M(n,F)$ 滿足方程 (3), 則稱之爲 (3) 的一組 (s,t) 型解。爲說話方便, 我們將滿足 $A^2 = -E$, $A' = -A$ 的矩陣 A 稱爲 A 型矩陣, 類似的, 滿足 $B^2 = E$, $B' = B$ 的矩陣 B 稱爲 B 型矩陣. 對混合型方程 (3), 我們引入一個相應的問題: 求 $M(n,F)$ 中的一組極大的 (s,t) 型解的數偶 (s,t) 的所有可能分佈。

通過與 Newman [11]中的主要結果類比, 我們得到以下定理。

定理2. 記 $n = 2^qp$ 其中 p 是奇數。則方程 (3) 在 $M(n,\mathbb{R})$ 中的任意一組解 $A_1,\ldots,A_s,B_1,\ldots,B_t$ 滿足 $s+t \le 2q+1$; 並且, 存在一組使得 $s+t = 2q+1$ 的 (s,t) 型解當且僅當 t 滿足 $0 \le t \le 2q+1$ 且 $t \equiv q+1 \pmod 4$。

我們將在第三節介紹定理 2 的證明思想, 詳細的證明在第四節給出。

在第五節將指出, 由定理 2 可以非常容易地推出實數情形的定理1, 這就給出了 Radon 定理的一個簡單證明。

在第六節將指出, 定理 2 可以推廣到任意的域 (定理3), 並由此得到 Hurwitz-Radon 定理在任意域上的推廣 (定理4)。並且指出我們的方法可以處理更簡單的方程 (2), 由此得到林節玄 [8] 中一些結果 (定理5) 的直接證明。

在第七節我們將給出定理 1 的一個著名推論 (定理7) 及其在幾何與代數中的兩個應用 (定理 6 和定理 8)。

---

[2]關於該定理可見 Serre [13] 第十三章。

[3]M.F. Atiyah, R. Bott, A. Shapiro, Clifford Modules, *Topology* **3**(suppl.1)(1964), 3-38。

三. 定理2的證明思想

這一節我們假定考慮的矩陣都是實矩陣。

爲理解下邊給出的定理2的證明, 讀者只需要具備線性代數的一些基本經驗, 特別是關於分塊矩陣的乘法運算和實對稱矩陣的譜定理: 實對稱矩陣正交相似於對角陣。

證明的基本想法是數學歸納法, 把高階的情形歸結爲低階的情形。下邊的引理提供了約化的可能。首先注意到, 我們考慮的方程 (3) 在正交相似變換下是不變的: 若

$$A_1, \ldots, A_s, B_1, \ldots, B_t$$

滿足方程 (3) , 則對任意的同階正交矩陣 P,

$$PA_1P^{-1}, \ldots, PA_sP^{-1}, PB_1P^{-1}, \ldots, PB_tP^{-1}$$

也滿足 (3)。

引理2.

(i) 設兩個 n 階對稱矩陣 B_1, B_2 滿足

$$B_1^2 = B_2^2 = E, \qquad B_1B_2 = -B_2B_1。$$

則 $n = 2m$ 且存在正交矩陣 P 使得

$$PB_1P^{-1} = \widetilde{B_1} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix} \qquad 且 \qquad PB_2P^{-1} = \widetilde{B_2} = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}.$$

(ii) 設 $A, B \in M(n, \mathbb{R})$, A 是反對稱的, B 是對稱的, 並且滿足

$$A^2 = -E, \quad B^2 = E, \quad AB = -BA$$

則 $n = 2m$ 且存在正交矩陣 P 使得

$$PAP^{-1} = \widetilde{A} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \qquad 且 \qquad PBP^{-1} = \widetilde{B} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}.$$

證明: 對於 (i), 首先我們注意到

$$tr(B_1) = 0$$

這是對等式

$$B_1 = -B_2B_1B_2^{-1}$$

兩邊取跡的結果。於是根據實對稱矩陣的譜定理, 存在正交矩陣 P_1 使得

$$P_1B_1P_1^{-1}=\begin{pmatrix}E & 0\\ 0 & -E\end{pmatrix}=\widetilde{B_1}$$

這裡我們用到 $B_1^2=E$ 以及 $tr(B_1)=0$ 的事實。現在 $P_1B_2P_1^{-1}$ 與 $\widetilde{B_1}$ 反交換, 容易求得 $P_1B_2P_1^{-1}$ 具有形式

$$P_1B_2P_1^{-1}=\begin{pmatrix}0 & Y\\ Z & 0\end{pmatrix}$$

進一步, 從 $(P_1B_2P_1^{-1})^2=E$ 推出 Y,Z 滿足 $YZ=E$。從而 $P_1B_2P_1^{-1}$ 具有形式

$$P_1B_2P_1^{-1}=\begin{pmatrix}0 & Y\\ Y^{-1} & 0\end{pmatrix}$$

其中 Y 是正交矩陣。

我們現在找一個正交矩陣 P_2 使得

$$P_2\widetilde{B_1}P_2^{-1}=\widetilde{B_1},\quad P_2(P_1B_2P_1^{-1})P_2^{-1}=\widetilde{B_2}。$$

容易求出這樣一個矩陣

$$P_2=\begin{pmatrix}E & 0\\ 0 & Y\end{pmatrix}$$

從而, 如果我們令 $P=P_2P_1$, 則得到 (i)。

對於 (ii), 若令

$$B_1=B,\quad B_2=BA,$$

則 B_1,B_2 滿足 (i) 的條件, 從而

$$PBP^{-1}=PB_1P^{-1}=\widetilde{B_1}=\widetilde{B},\quad PB_2P^{-1}=\widetilde{B_2}$$
$$PAP^{-1}=P(B_1B_2)P^{-1}=(PB_1P^{-1})(PB_2P^{-1})=\widetilde{B_1}\widetilde{B_2}=\widetilde{A}。$$

這就完成了引理2的證明。 □

在對定理2展開證明之前, 我們先給出兩點說明。

根據引理2, 若 (s,t) 型解 $A_1,\dots,A_s,B_1,\dots,B_t$ 中有兩個矩陣是 B 型的, 不妨設 $B_1=\widetilde{B_1},B_2=\widetilde{B_2}$, 於是與它們同時反交換的矩陣 X 有形式

$$X=\begin{pmatrix}0 & Y\\ -Y & 0\end{pmatrix}$$

並且容易驗證, X 是 A 型或 B 型的當且僅當對應的 Y 是 B 型或 A 型的。進一步, 兩個這樣的矩陣 X_1, X_2 反交換當且僅當與之對應的 Y_1, Y_2 反交換。於是, $M(n,\mathbb{R})$ 中存在一組 (s,t) 型解 $(t \geq 2)$ 當且僅當 $M(n/2,\mathbb{R})$ 的中存在一組 $(t-2,s)$ 型解。

類似地, 若 $A_1, \ldots, A_s, B_1, \ldots, B_t$ 中有一個 A 型的和一個 B 型的, 則不妨設

$$A_1 = \widetilde{A_1}, \quad B_1 = \widetilde{B_1},$$

於是與它們同時反交換的矩陣 Z 具有形式

$$Z = \begin{pmatrix} 0 & W \\ W & 0 \end{pmatrix},$$

並且 Z 是 A 型或 B 型的當且僅當對應的 W 是 A 型或 B 型的。進一步, 兩個這樣的矩陣 Z_1, Z_2 反交換當且僅當對應的 W_1, W_2 反交換。於是, $M(n,\mathbb{R})$ 中存在一組 (s,t) 型解 $(s \geq 1, t \geq 1)$ 當且僅當 $M(n/2,\mathbb{R})$ 存在一組 $(s-1,t-1)$ 型解。

其次, 我們要介紹由 Newman 和 Williamson 引入的一個技巧[4] , 它可以把一組 (s,t) 型解 ($s \geq 4$) 轉換爲一組 $(s-4,t+4)$ 型解。這個轉換如下給出。

設

$$A_1, \ldots, A_s, B_1, \ldots, B_t$$

是 (3) 的一組解, 其中 $s \geq 4$。令

$$\widetilde{A_i} = A_{i+4}, \quad (i = 1, \ldots, s-4); \qquad \widetilde{B_j} = B_j \, (j = 1, \ldots, t),$$

以及

$$\widetilde{B}_{t+1} = A_2A_3A_4, \quad \widetilde{B}_{t+2} = A_1A_3A_4, \quad \widetilde{B}_{t+3} = A_1A_2A_4, \quad \widetilde{B}_{t+4} = A_1A_2A_3$$

容易驗證 $\widetilde{A_1}, \ldots, \widetilde{A}_{s-4}, \widetilde{B_1}, \ldots, \widetilde{B}_{t+4}$ 是 (3) 的一組 $(s-4,t+4)$ 型解。同樣, 在上述轉換中交換 A, B 的位置, 可以把一組 (s,t) 型解 ($t \geq 4$) 轉換成一組 $(s+4,t-4)$ 型解。這個事實我們稱之爲 Newman-Williamson 技巧, 它對定理2中出現的模 4 條件給出了一個合理的解釋, 由此也給出了 Hurwitz-Radon 定理中的模 4 條件的一個合理解釋。

爲便於敍述, 我們把上邊提到的各個約化結果分別表述成以下3個引理。

引理3. $M(n,\mathbb{R})$ 中存在一組 (s,t) 型解 $(t \geq 2)$ 滿足 (3) 當且僅當 $M(n/2,\mathbb{R})$ 中存在一組 $(t-2,s)$ 型解滿足 (3)。

[4]Newman [11]最初得到的結果是錯誤的, Williamson 向他指出了錯誤並建議了一個修正方案, 這就是通過引入該技巧。

引理4. $M(n,\mathbb{R})$ 中存在一組 (s,t) 型解 $(s\geq 1,t\geq 1)$ 滿足 (3) 當且僅當 $M(n/2,\mathbb{R})$ 存在一組 $(s-1,t-1)$ 型解滿足 (3)。

引理5. $M(n,\mathbb{R})$ 中存在一組 (s,t) 型解 $(s\geq 4)$ 滿足 (3) 當且僅當 $M(n,\mathbb{R})$ 存在一組 $(s-4,t+4)$ 型解滿足 (3); $M(n,\mathbb{R})$ 中存在一組 (s,t) 型解 $(t\geq 4)$ 滿足 (3) 當且僅當 $M(n,\mathbb{R})$ 存在一組 $(s+4,t-4)$ 型解滿足 (3)。

四. 定理2的證明

本節我們給出定理2的證明。

證明: 對 $n=2^q p$ 的 2 指數 q 用數學歸納法。

第一步. $q=0$ 的情況。此時 $n=p$ 是奇數。

首先, $s=0$。否則將存在 p 階的反對稱矩陣 A 滿足 $A^2=-E$, 這與奇數階反對稱矩陣不可逆矛盾。

其次, $t\leq 1$。這是引理 2(i) 的結論。又, 單位陣是 B 型陣, 所以 s 可以取到最大值1。

於是我們證明了, $q=0$ 時方程 (3) 僅存在 $(0,1)$ 型的極大解。

第二步. $q=1$ 的情況。

我們先證明, 對 $M(2p,\mathbb{R})$ 的任意一組 (s,t) 型解, 必定有 $s+t\leq 3$。

若 $t\geq 2$, 由引理3, $M(p,\mathbb{R})$ 中存在一組 $(t-2,s)$ 型解, 於是 $t-2=0$, 且 $s\leq 1$, 從而 $s+t\leq 3$。

若 $t=1$, 且 $s\geq 1$, 則由引理4, $M(p,\mathbb{R})$ 中存在一組 $(s-1,0)$ 型解, 從而 $s=1$, $s+t=2\leq 3$。

若 $t=0$ 我們用反證法證明 $s=\leq 3$. 若 $s\geq 4$, 則由引理5, $M(2p,\mathbb{R})$ 中存在一組 $(s-4,4)$ 型解, 由此第一種情況得證的結果 $s\leq 3$, 矛盾!

接下來我們考慮 (3) 的極大解的分佈. 一共有以下四種可能 $(3,0),(2,1),(0,3),(1,2)$. 我們將排除前三種可能。

爲排除前兩種情形, 只要證明 $s\leq 1$。用反證法。假定 $s\geq 2$。由於 $A_1^2=-E$, 根據實反對稱矩陣的譜定理[5] , 存在正交矩陣 P 使得

$$PA_1P^{-1}=\begin{pmatrix}0 & E\\ -E & 0\end{pmatrix}=\widetilde{A_1}.$$

[5]見 Kaplansky [7]。

由於反對稱矩陣 PA_2P^{-1} 與 $\widetilde{A_1}$ 反交換, 於是 PA_2P^{-1} 具有形式

$$PA_2P^{-1} = \begin{pmatrix} X & Y \\ Y & -X \end{pmatrix}$$

其中 $X, Y \in M(m, \mathbb{R})$ 皆爲反對稱矩陣. 如果 A_2 進一步滿足 $A_2 = -E$, 則 X, Y 將滿足

$$X^2 + Y^2 = -E, \quad XY = YX.$$

這兩個式子可以拼成一個緊湊的式子

$$(X + iY)(X - iY) = -E$$

這個式子表明 p 階 (复) 反對稱矩陣 $X + iY$ 與 $X - iY$ 可逆。矛盾!

根據引理3可以排除第三種可能, 否則將有一個 p 階 A 型陣。

又, 根據引理 4, 我們可以構造出一組 $(1, 2)$ 型極大解如下:

$$A_1 = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}, \qquad B_2 = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}$$

第三步. 我們將對 $q \geq 0$ 歸納證明, $M(n, \mathbb{R})$ 中任意一組 (s, t) 型解滿足 $s + t \leq 2q + 1$ 而且等號可以成立, 對於 $n = 2^q p$。

一方面, 我們利用引理4可以從 $M(p, \mathbb{R})$ 中的 $(0, 1)$ 型解歸? 構造出 $M(2^q p, \mathbb{R})$ 中的一組 $(q, q + 1)$ 型解。例如, $n = 2p$ 時我們有上述 $(1, 2)$ 型解。一般的, 設

$$A_1^{(q-1)}, \cdots, A_{q-1}^{(q-1)}, B_1^{(q-1)}, \cdots, B_q^{(q-1)}$$

爲 $M(2^{q-1}p, \mathbb{R})$ 中的一組 $(q - 1, q)$ 型解, 則

$$A_i^{(q)} = \begin{pmatrix} 0 & A_i^{(q-1)} \\ A_i^{(q-1)} & 0 \end{pmatrix} \quad (i = 1, \cdots, q-1), \qquad A_q^{(q)} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix},$$

$$B_k^{(q)} = \begin{pmatrix} 0 & B_k^{(q-1)} \\ B_k^{(q-1)} & 0 \end{pmatrix} \quad (k = 1, \cdots, q), \qquad B_{q+1}^{(q)} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix} \tag{4}$$

是 $M(2^q p, \mathbb{R})$ 中的一組 $(q, q + 1)$ 型解。

下面我們將說明, $M(n, \mathbb{R})$ 中任何一組 (s, t) 解都滿足 $s + t \leq 2q + 1$。

這是因爲 $M(n,\mathbb{R})$ 中任何一組 (s,t) 解都可以通過引理3-5化歸爲 $M(n/2,\mathbb{R})$ 中的一組個數爲 $s+t-2$ 的解: 如果 $t\geq 2$ 應用引理3; 如果 $t=1$ 且 $s\geq 1$ 應用引理4; 如果 $t=0$, 應用引理5。

作爲例子, 我們考慮最後一種情況. 用反證法. 假定存在一組 $(s,0)$ 型解使得 $s\geq 2q+2$, 由於 $q\geq 2$ 所以 $s\geq 2\times 2+2=6$, 利用引理5可以得到一組 $(s-4,4)$ 型解, 從而化歸爲第一種情況。

最後, 我們歸納證明, $M(n,\mathbb{R})$ 中存在一組 (s,t) 型的極大解當且僅當 $t\in[0,2q+1]$ 滿足 $t\equiv q+1 \pmod 4$。

充分性. 將表明對 $[0,2q+1]$ 中任意的滿足 $t\equiv q+1 \pmod 4$ 的自然數 t, $M(n,\mathbb{R})$ 中存在一組 $(2q+1-t,t)$ 型解。注意到總是存在一組 $(q,q+1)$ 型解, 從這組解出發, 通過若干次 Newman 轉換, 可以得到一組 $(2q+1-t,t)$ 型解, 這由同餘條件 $t\equiv q+1 \pmod 4$ 所保證。

必要性. 設 $n=2^q p$, 其中 $q\geq 2$, 如果 $M(n,\mathbb{R})$ 中存在一組 (s,t) 型的極大解, 根據 Newman 轉換, 可以不妨設 $s\geq 1, t\geq 1$, 於是由引理4 $M(n=2^{q-1}p,\mathbb{R})$ 中存在一組 $(s-1,t-1)$ 型的極大解, 由 $q-1$ 時的歸納假設, $t-1\equiv q \pmod 4$, 也就是 $t\equiv q+1 \pmod 4$。

五. Hurwitz-Radon 定理的證明

這一節我們將從定理2推出 Hurwitz-Radon 定理的 Radon 部分。

證明: 首先注意到 (1) 相當於純 A 型的方程 (3), 根據定理2, 總有 $K(n)\leq 2q+1$。下邊我們要對 $K(n)$ 給出更精確的估計。

基本的想法是, 對給定的 $n=2^q p$, 從 (3) 的所有可能的 (s,t) 極大解中選出一組使得 A 型矩陣最多的解, 再看能不能添加 A 型陣得到更多個數的一組解。注意到, $s+t=2q+1$, 所以 s 取得最大等價於 t 取得最小。下邊我們分情況討論。

(i) 若 $q\equiv 3 \pmod 4$, 則 (3) 的一組 (s,t) 型極大解滿足 $t\equiv q+1\equiv 0 \pmod 4$, 取 $t=0$, 此時 $s=2q+1$ 達到最大, 換言之, $K(n)=2q+1$。

(ii) 若 $q\equiv 0 \pmod 4$, 則 (3) 的一組 (s,t) 型極大解滿足 $t\equiv q+1\equiv 1 \pmod 4$, 取 $t=1$, 此時 $s=2q$, 於是 $K(n)\geq 2q$。事實上此時等號成立: $K(n)=2q$。我們用反證法來說明這一點。假設 $K(n)=2q+1$, 這就意味著 (3) 存在一組 $(2q+1,0)$ 型的極大解, 根據定理2, 這當且僅當 $0\equiv q+1 \pmod 4$, 即 $q\equiv 3 \pmod 4$, 矛盾。

(iii) 若 $q \equiv 1 \pmod 4$, 則 (3) 的一組 (s,t) 型極大解滿足 $t \equiv q+1 \equiv 2 \pmod 4$, 取 $t=2$, 此時 $s=2q-1$, 於是 $K(n) \geq 2q-1$。我們斷言此時 $K(n)=2q-1$。假定存在 $2q$ 個矩陣 $A_1,\ldots,A_{2q}$ 滿足 (1), 則令

$$A_{2q+1} = A_1 \cdots A_{2q},$$

則容易看到 A_{2q+1} 是一個 A 型矩陣, 且與 $A_1,\ldots,A_{2q}$ 反交換, 於是我們得到 (3) 的一組 $(2q+1,0)$ 型的極大解, 這與定理2矛盾。

(iv) 若 $q \equiv 2 \pmod 4$, 則 (3) 的一組 (s,t) 型極大解滿足 $t \equiv q+1 \equiv 3 \pmod 4$, 取 $t=3$, 此時 $s=2q-2$, 於是 $K(n) \geq 2q-2$。設 $A_1,\ldots,A_{2q-2}$ 滿足 (1), 則我們可以添加矩陣

$$A_{2q-1} = A_1 \cdots A_{2q-2}$$

得到一組滿足 (1) 的 $2q-1$ 個矩陣. 於是進一步有 $K(n) \geq 2q-1$, 我們斷言 $K(n) = 2q-1$。用反證法來說明這一點, 假設 $A_1,\ldots,A_{2q}$ 滿足 (1), 則

$$B_1 = A_1 \cdots A_{2q}$$

與 $A_1,\ldots,A_{2q}$ 一起給出 (3) 的一組 $(2q,1)$ 型的極大解, 根據定理2, 這當且僅當 $1 \equiv q+1 \pmod 4$, 即 $q \equiv 0 \pmod 4$, 矛盾。

綜上, 我們確定出 $K_{\mathbb{R}}(n)$ 的值如下:

$$K_{\mathbb{R}}(n) = \begin{cases} 2q & q \equiv 0 \pmod 4 \\ 2q-1 & q \equiv 1 \pmod 4 \\ 2q-1 & q \equiv 2 \pmod 4 \\ 2q+1 & q \equiv 3 \pmod 4 \end{cases}$$

□

六. Newman 定理與 Hurwitz 定理到任意域的推廣

本節我們將說明定理1與定理2都可以推廣到任意的特徵不等於 2 的域。

因爲從定理2推導定理1完全不需要用到關於域 F 的任何特性, 所以我們只需證明定理2對任意的域成立。

我們先考慮 F 爲代數封閉域的情況。此時, 下述矩陣定理是關鍵的。

引理6. 設 F 是特徵不等於 2 的代數封閉域。$A_1, \ldots, A_k$ 與 $B_1, \ldots, B_k$ 同是 F 上的 n 階對稱矩陣或反對稱矩陣, 若存在矩陣 $P \in GL(n, F)$ 使得

$$PA_iP^{-1} = B_i, \quad (i = 1, \ldots, k)。$$

則存在矩陣 $Q \in GL(n, F)$, $QQ' = E$ 使得

$$QA_iQ^{-1} = B_i, \quad (i = 1, \ldots, k)。$$

這個定理似乎是 Albert 首先發現的, 見 [1, Theorem 27], 一個簡單的證明可見 Kaplansky [7]。

利用引理6可以證明引理2-5對代數閉域成立, 從而定理2對代數閉域成立。

我們只在此說明如何從引理6推導代數閉域情形的引理2。爲此, 我們需要下述更一般的引理。

引理7.

(i) 設 $B_1, B_2 \in M(n, F)$ 滿足

$$B_1^2 = B_2^2 = E, \qquad B_1B_2 = -B_2B_1。$$

則 $n = 2m$ 且存在 $P \in GL(n, F)$ 使得

$$PB_1P^{-1} = \widetilde{B_1} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix} \qquad 且 \qquad PB_2P^{-1} = \widetilde{B_2} = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}.$$

(ii) 設 $A, B \in M(n, F)$ 滿足

$$A^2 = -E, \quad B^2 = E, \quad AB = -BA$$

則 $n = 2m$ 且 $P \in GL(n, F)$ 使得

$$PAP^{-1} = \widetilde{A} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \qquad 且 \qquad PBP^{-1} = \widetilde{B} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}.$$

引理7的證明完全平行於引理2的證明, 我們留給感興趣的讀者。

從引理6和引理7可以很容易推出下述引理8, 它就是引理2在代數封閉域上的對應結果。

引理8. 設 F 是一個特徵不等於 2 的代數閉域。

(i) 設 $B_1, B_2 \in M(n,F)$ 都是對稱矩陣且滿足

$$B_1^2 = B_2^2 = E, \qquad B_1B_2 = -B_2B_1。$$

則 $n = 2m$ 且存在 $Q \in GL(n,F)$, $QQ' = E$ 使得

$$QB_1Q^{-1} = \widetilde{B_1} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix} \qquad 且 \qquad QB_2Q^{-1} = \widetilde{B_2} = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}.$$

(ii) 設 $A, B \in M(n,F)$, A 是反對稱的, B 是對稱的, 並且滿足

$$A^2 = -E, \quad B^2 = E, \quad AB = -BA$$

則 $n = 2m$ 且存在 $Q \in GL(n,F)$, $QQ' = E$ 使得

$$QAQ^{-1} = \widetilde{A} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \qquad 且 \qquad QBQ^{-1} = \widetilde{B} = \begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix}.$$

由此可以得到引理3–5在代數閉域上的對應結果。

現在考慮最一般的情況。假定 F 是任意一個特徵不等於2的域, $\overline{F}$ 爲其代數閉包。設 $A_1, \ldots, A_s, B_1, \ldots, B_t$ 是 $M(n,F)$ 中的一組 (s,t) 型解, 它自然是 $M(n,\overline{F})$ 中的一組 (s,t) 型解, 所以根據代數封閉域 F 上的定理2, 可以推出 $s+t \le 2q+1$, 而且如果 $s+t = 2q+1$, 則 $t \equiv q+1 \pmod 4$。爲證明當 t 滿足同餘條件 $t \equiv q+1 \pmod 4$ 時存在一組 $(2q+1-t, t)$ 型極大解, 只注意定理2的證明中給出的那組 $(q, q+1)$ 型極大解矩陣 (4) 本質上是由 $0, 1, -1$ 三個數經加減乘除生成的, 所以在任何一個特徵不等於2的域上都有定義。這就證明了當 $t = q+1$ 時存在一組 $(q, q+1)$ 型解, 再注意到 Newman-Williamson 轉換不依賴於域 F 的任何特性, 所以由此可以衍生出所有滿足同餘條件 $t \equiv q+1 \pmod 4$ 的 $(2q+1-t, t)$ 型解。這樣我們就得到了定理2的下述推廣:

定理3. 設域 F 的特徵不等於 2。記 $n = 2^q p$ 其中 p 是奇數。則方程 (3) 在 $M(n,F)$ 中的任意一組解 $A_1, \ldots, A_s, B_1, \ldots, B_t$ 滿足 $s+t \le 2q+1$; 並且, 存在一組使得 $s+t = 2q+1$ 的 (s,t) 型解當且僅當 t 滿足 $0 \le t \le 2q+1$ 且 $t \equiv q+1 \pmod 4$。

由此, 我們得到 Hurwitz-Radon 定理的最一般的版本。[6]

定理4. 對於任意的特徵不等於 2 的域 F, 滿足 Hurwitz 方程 (1) 的一組矩陣的基數有最大

[6]很抱歉, 作者尚不清楚這個結果最初由誰發現。

值, 並且其最大值 $K_F(n)$ 如下給出:

$$K_F(n) = K(n) = \begin{cases} 2q & q \equiv 0 \pmod 4 \\ 2q-1 & q \equiv 1 \pmod 4 \\ 2q-1 & q \equiv 2 \pmod 4 \\ 2q+1 & q \equiv 3 \pmod 4 \end{cases}$$

其中 q 滿足 $n = 2^q p$, p 是奇數。

最後, 作者想就本文提供的這個證明思想做一個小結: 我們沒有直接考慮方程 (1) 而是考慮了混合型方程 (3) 然後從中提取出 (1) 的資訊。我們得到的教益是: 如果一個物件有對偶, 那麼連同它的對偶一起來考慮會看得更清楚。 這就好比粒子物理中的 Bose-Fermi 對應的哲學一樣。同樣的想法可以應用于方程 (2), 對應的結果由下述定理給出。

定理5. 設 F 是一個特徵不等於 2 的域, 記 $n = 2^q\, p$, p 爲奇數。若 $A_1, \ldots, A_k \in M(n, F)$ 滿足 (2), 則 k 有最大值 $E_F(n)$, 且 $E_F(n)$ 如下給出:

(i) 若 -1 是 F 中的平方數, 則 $E_F(n) = 2q + 1$;

(ii) 若 -1 不是 F 中的平方數, 但可以寫成 F 中兩個平方數的和, 則

$$E_F(n) = \begin{cases} 2q & q \equiv 0 \pmod 2 \\ 2q+1 & q \equiv 1 \pmod 2 \end{cases};$$

(iii) 若 -1 不能寫成 F 中兩個平方數的和, 則

$$E_F(n) = K(n) = \begin{cases} 2q & q \equiv 0 \pmod 4 \\ 2q-1 & q \equiv 1 \pmod 4 \\ 2q-1 & q \equiv 2 \pmod 4 \\ 2q+1 & q \equiv 3 \pmod 4 \end{cases}$$

這本質上就是林節玄 [8] pp.125–126 對應的定理 4.4, 4.6, 4.8, 那是是作爲關於 Clifford 代數理論的副產品給出的。

七. Hurwitz-Radon 定理的一些應用

在本節我們將介紹 Hurwitz-Radon 定理的兩個應用, 也可以說是 Hurwitz-Radon 定理的背景。

應該指出, Hurwitz 矩陣方程與代數和幾何中的許多問題關聯密切, 有興趣的讀者可以參考 Ebbinghaus [2]或 Eckmann [4]。

特別值得介紹的是1983年 Massey [10]給出的下述關於歐氏空間的向量積的基本結果:

定理6. $n \geq 2$ 維歐氏空間 $\mathbb{R}^n$ 中存在滿足以下兩個條件的雙線性向量積當且僅當 $n = 3$ 或 $n = 7$。

(i) $(x \times y, x) = (x \times y, y) = 0$。

(ii) $\|x \times y\|^2 = \|x\|^2\|y\|^2 - (x, y)^2$。

定理6可以從定理1的下述簡單推論得到, 具體推導 Ebbinghaus [2] 或 Prasolov [10]。

定理7. $K(n) \leq n - 1$, 等號成立當且僅當 $n = 1, 3, 7$。

定理7是 Hurwitz 在1898年的文章 [5]中得到的, 只不過 Hurwitz 是以另一種等價的方式來描述這個結果。他的表述是 (見 [2, p.274])

定理8. 設 $n \geq 1$。如果存在 $x_1, \ldots, x_n$ 與 $y_1, \ldots, y_n$ 的實雙線性函數 $z_1, \ldots, z_n$ 使得

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = (z_1^2 + \cdots + z_n^2) \tag{5}$$

對一切實變數 $x_1, \ldots, x_n$ 與 $y_1, \ldots, y_n$ 成立, 則 $n = 1, 2, 4, 8$。

對於 $n = 1$ 等式是平凡的: $x_1^2 y_1^2 = (x_1 y_1)^2$。

對 $n = 2$ 我們有

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2 \tag{6}$$

這不過是複數模長的乘法法則的實形式。

類似地, 由四元數範數的可乘性質可以得到由 Euler 發現的四平方和乘積公式。[7]

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{7}$$

其中 z_1, z_2, z_3, z_4 爲[8]

$$z_1 = x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4, \quad z_2 = x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3$$
$$z_3 = x_1 y_3 - x_2 y_4 + x_3 y_1 + x_4 y_2, \quad z_4 = x_1 y_4 + x_2 y_3 - x_3 y_2 + x_4 y_1$$

八元數 (又稱 Cayley 數) 的範數乘法公式給出 $n = 8$ 的平方和公式, 見 [2, p.259]。

Hurwitz 正是在研究這種平方和的乘積問題時匯出著名的 Hurwitz 矩陣方程。

---

[7] Lagrange 和 Euler 正是利用這個公式證明了每一個正整數可以寫成四個整數的平方和。

[8] 事實上, 它們分別是四元數 $(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k})(y_1 + y_2\mathbf{i} + y_3\mathbf{j} + y_4\mathbf{k})$ 的各個係數。

他在 [5] 中給出的定理 7 的證明非常簡單, 甚至不需要用到譜定理, 讀者可以參考 C. W. Curtis, Linear Algebra, An Introduction Approach, UTM, Springer, 1996.

與平方和有關的歷史可以參考 Taussky [17]的精彩論述。

致謝. 作者在寫作過程中從清華大學劉雲朋同學處得到許多教益, 還要感謝天津大學田代軍老師、田長亮、鄭景銳、徐澤同學以及南開大學白承銘老師、劉會同學與首都師範大學許權、陳見柯、段紅偉和趙潔同學的鼓勵和幫助。

參考文獻

1. A. A. Albert, Symmetric and alternate matrices in an arbitrary fields, *Trans. A.M.S.*, **43**(1938), 193–228.
2. Ebbinghaus, *et al.* Numbers, GTM Vol.123, Springer.
3. B. Eckmann, Gruppentheorectischer Beweis des Satzes von Hurwitz-Radon uber die Komposition quadratischer Formen, *Comment. Math. Helv.*, **15**(1942), 358–366.
4. B.Eckmann, Topology, Algebra, Analysis-Relations and missing links, *Notices A.M.S.*, **46**(1999), 520–527.
5. A. Hurwitz, quadratischen Formen von beliebig vielen Variablen, *Nachrichten Ges. der Wiss. Gottingen* 1898, 309–316.
6. A. Hurwitz, *Ü*ber die Komposition der quadratischen Formen, *Math. Ann.* **88**(1923), 1–25.
7. I. Kaplansky, *Linear Algabra and Geometry–A Second Course*, Allyn and Bacon, 1969.
8. T. Y. Lam, Introduction to Quadratic Forms over Fields, Graduate Studies in Mathematics, Vol.**67**, American Mathematical Society, Providence, Rhode Island, 2005.
9. H. C. Lee, Sur le theoreme de Hurwitz-Radon pour la composition des formes quadratiques, *Comment. Math. Helv.*, **21)**(1948), 261–269.
10. M. S. Massey, Cross products of vectors in higher-dimensional Euclidean spaces. *Amer. Math. Monthly*, **90**, no.10, (1983), 697-701.
11. M. A. H. Newman, Note on an algebraic theorem of Eddington, *Journal London Math. Soc.*, **7**(1932), 93–99; Corrigenda, 272.
12. V. V. Prasolov, Problems and Theorems in Linear Algebra, Translation of Mathematical monographs, Vol.134, American Mathematical Society, 1994.
13. J. Radon, Lineare Scharen orthogonaler Matrizen, *Abhandlungen aus dem mathematischen Seminar der Hambergischen Univerdität* **1**(1922), 1–14.
14. A. R. Rajwade, Squares, London Mathematical Society Lecture Note Series **171**, Cambridge University Press, 1993.
15. J. P. Serre, *Linear Representations of Finite Groups*, GTM Vol.42, Springer.
16. D. B. Shapiro, Compositions of Quadratic Forms, de Gruyter Expositions in Mathematics **33**, 2000.

17. O. Taussky, Sums of Squares, *The American Mathematical Monthly*, **77**, No.8, (1970), 805–830.
18. J. A. Tyrrell and J. G. Semple, *Generalized Clifford Parallelism*, Cambridge University Press, 1971.
19. O. Veblen and J. von Neumann, Geometry of Complex Domain, Princeton Mimeographed Notes, Notes by W.Givens and A.H.Taub, Institute for Advanced Study, 1935–1936.
20. Yung-Chow Wong, Isoclinic n-Planes in $2n$-Spaces, Clifford Parallels in Elliptic $(2n-1)$-Spaces, and Hurwitz Matrix Equations, *Memoirs A.M.S.*, **no.41**, 1961.

—本文作者爲中國首都師範大學數學科學院研究生—

中央研究院數學所2012暑期研習活動

研 習 日 期：2012年7月9日 (星期一) ～ 2012年8月17日 (星期五)
研 習 地 點：台北市大安區羅斯福路四段1號 天文數學館6樓 中研院數學所
研 習 資 格：大學部學生 (系、所不限), 具各課程所需預備知識者。
預 定 課 程：(1) 組合數學與圖論專題 (2) 錯誤改正碼 (3) 數理金融
詳細情形請查詢中研院數學所網頁 http://www.math.sinica.edu.tw

The 12th International Congress on Mathematical Education

時間：2012年7月8日 (星期日) ～ 2012年7月15日 (星期日)
地點: 韓國首爾 COEX
詳細情形請查詢活動網頁http://www.icme12.org/

Conference of the International Group for the Psychology of Mathematics Education (PME 36)

時間：2012年7月18日 (星期三) ～ 2012年7月22日 (星期日)
地點: 台北市文山區汀州路4段88號國立臺灣師範大學
詳細情形請查詢活動網頁http://tame.tw/pme36/

數學教育 SIG: Reading Mathematics 讀書會

地點: 國立台灣師範大學教育學院
1. 2012年4月14日 (六) 主題: 閱讀測驗 (陳美芳老師)
2. 2012年5月05日 (六) 主題: 閱讀教學 (陳茹玲老師)
3. 2012年5月26日 (六) 主題: 閱讀困難學生的特徵與補救策略 (洪儷瑜老師)
4. 2012年6月16日 (六) 主題: 數學閱讀 (吳昭容老師)

詳細情形請查詢國科會科教處數學教育學門學門資訊網
http://w3.math.sinica.edu.tw/nsc_mathedu/