# Hadamard 矩陣及其應用, 1893-1993

林參天 · 薛昭雄

1993 年 12 月初, Hadamard 矩陣專家 Seberry教授在澳大利亞 Wollongong 大學召開 Hadamard 論文 [5]發表一百週年學術討論紀念會, 來自許多國家的二十多位代表參加了會議。Hadamard 是近代著名的法國數學家, 他的研究領域主要在分析方面。組合數學研究人員爲何專題紀念 Hadamard 的這篇文章呢?

話要從1867年英國數學家 Sylvester[12]研究正交矩陣談起。Sylvester考慮這樣的$n$階正交矩陣$\mathbf{H}$, 其元素是+1或−1(在本文例子中, 我們用+, −表示+1, −1), 且滿足條件

$$\mathbf{H}\mathbf{H}^{\mathbf{T}} = n\mathbf{I}。$$

三個簡單的例子是

$$\mathbf{H}_1 = [+], \qquad \mathbf{H}_2 = \begin{bmatrix} + & + \\ + & - \end{bmatrix},$$

$$\mathbf{H}_4 = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix}.$$

這項課題引起 Hadamard 的注意與興趣。1893 年 Hadamard 發表論文 [5], 從最大行式值的觀點研究這類正交矩陣。Hadamard在這篇論文中證明了下述的一個事實: 如果一個$n$階實矩陣$\mathbf{A}$的所有元素的絕對值皆小於或等於1, 那麼$A$的行列式的絕對值小於或等於 $n^{\frac{n}{2}}$; 等式成立若且唯若$\mathbf{A}$的元素是+1或−1且滿足條件 $\mathbf{A}\cdot\ \mathbf{A}^{\mathbf{T}} = n\mathbf{I}$。由於 Hadamard 的這篇文章揭示了這類正交矩陣的特殊性質, 這類正交矩陣後來就稱爲 Hadamard 矩陣。

由於 Hadamard 矩陣具有正交性, 最大行列式值與元素二元性, 因此 Hadamard 矩陣的構造與應用就受到人們的重視。由 Sylvester 開始一百多年來, 尤其是在電子計算機迅速發展, 充分普及的今天, Hadamard 矩陣無論是在理論研究方面還是在實際應用方面都有極大的發展。

本文旨在拋磚引玉, 在 Hadamard 發表論文 [5]一百週年之際, 概述 Hadamard 矩陣的若干問題及其應用, 博得更多的專家和業餘愛好者對 Hadamard 矩陣的興趣和進行更深入廣泛的研究。

一般說來, Hadamard 矩陣的研究可分爲二大類: 存在性問題和應用問題。存在性問題又可分爲構造性問題和等價類問題。應用方面也可分爲理論應用和實際應用。

我們不難證明如果$n$階 Hadamard 矩陣存在的話, 那麼$n = 1$或$n = 2$ 或$n$是4的倍數。這是 Hadamard 矩陣存在的必要條件。一般人猜測這也是充分條件。雖然我們已找到許多方法來構造高階 Hadamard 矩陣, 但仍然無法證明這也是一個充分條件。至 1993 年 12 月, 仍未知其存在性的 Hadamard 矩陣中, 最低的階數是428, 因而構造性問題自然引起人們的極大興趣。

歷史上最有名的構造方法是 Sylvester, Paley 與 Williamson 等人的方法。Sylvester的方法 [12]是這樣的: 如果存在$n$階 Hada- mard矩陣$\mathbf{H}_n$, 那麼

$$\mathbf{H}_{2n} = \begin{bmatrix} \mathbf{H}_n & \mathbf{H}_n \\ \mathbf{H}_n & -\mathbf{H}_n \end{bmatrix}$$

是 $2n$ 階的 Hadamard 矩陣。特別的對 2 階 Hadamard矩陣 $\mathbf{H}_2 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$, 及任意正整數$k$我們不難構造出$n = 2^k$ 階的 Hadamard 矩陣。

Paley[10]構造 Hadamard 矩陣的方法極爲有用。對於任意形如$2^\alpha(p^k+1)$, 其中$p$爲奇質數且4整除$2^\alpha(p^k+1)$, 的正整數, 他用二次剩餘的方法, 成功地構造了$n = 2^\alpha(p^k+1)$階的 Hadamard 矩陣。例如, 下列$n = 8$階之 Hada -mard矩陣

$$\mathbf{H} = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & - & + & - & - & - \\ + & - & + & + & - & + & - & - \\ + & - & - & + & + & - & + & - \\ + & - & - & - & + & + & - & + \\ + & + & - & - & - & + & + & - \\ + & - & + & - & - & - & + & + \\ + & + & - & + & - & - & - & + \end{bmatrix}$$

即可用其方法構造, 詳細情形請參考 [10]。特別地, 當$k = 1$時, 這樣的質數有無窮多, 因此存在無窮多 Paley 型的 Hadamard 矩陣。

Williamson[15]利用四元數的原理, 探討了如下形式的 Hadamard 矩陣

$$\mathbf{H} = \begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & \mathbf{D} & -\mathbf{C} \\ -\mathbf{C} & -\mathbf{D} & \mathbf{A} & \mathbf{B} \\ \mathbf{D} & -\mathbf{C} & \mathbf{B} & -\mathbf{A} \end{bmatrix}$$

其中$\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}$是奇數$t$階循環矩陣, 且滿足條件:

$$\mathbf{A}\cdot\mathbf{A}^\mathbf{T} + \mathbf{B}\cdot\mathbf{B}^\mathbf{T} + \mathbf{C}\cdot\mathbf{C}^\mathbf{T} + \mathbf{D}\cdot\mathbf{D}^\mathbf{T} = 4t\mathbf{I}。$$

Williamson型 Hadamard 矩陣的一個簡單例子是$t = 3$的$n = 12$階 Hadamard 矩陣, 其中

$$\mathbf{A} = \begin{bmatrix} + & + & + \\ + & + & + \\ + & + & + \end{bmatrix}$$

$$\mathbf{B} = \mathbf{C} = \mathbf{D} = \begin{bmatrix} + & - & - \\ - & + & - \\ - & - & + \end{bmatrix}。$$

Williamson的方法雖還不能保證構造出所有階數的 Hadamard 矩陣, 但是 Williamson 以及後人借助於電子計算機的探索, 相繼發現了小階數的 Williamson 型 Hadamard 矩陣。當階數增大時, 僅僅借助電子計算機的探索就顯得很困難。但是後人沿著這個途徑探索, 用理論的方法構造出許多 Williamson 型的 Hadamard 矩陣。近來在這方面取得較大進展的是中國武漢華中師範大學的夏明遠教授 [16]。國際上不少人的工作也很好, 限於篇幅, 不能在此一一介

紹。有興趣的讀者, 不妨參看最新綜述文獻[11]。

另一條途徑是用交叉乘積的方法從若干已知的 Hadamard 矩陣中構造出高階的 Hada- mard 矩陣。Hadamard[5]證明了: 如果分別存在$h_1$階和$h_2$階 Hadamard 矩陣, 那麼存在$n = h_1h_2$階的 Hadamard 矩陣。這個結果後來被 Agaian 和 Sarukhanyan[1]改進爲: 如果分別存在$4h$階和$4k$階 Hadamard 矩陣, 那麼存在$n = 8hk$階 Hadamard 矩陣。這是一個很大的改進。近年來, 這結果又被 Craigen, Seberry 和張顯謨博士 [4]這一步改進爲: 如果分別存在$4a, 4b, 4c, 4d$階 Hadamard 矩陣, 那麼存在$n = 16abcd$階 Hadamard 矩陣。如果能繼續在這個方向進行探索, 取得突破的話, 我們有理由期望構造 Hadamard 矩陣就會像因子分解那樣由基本的 Hadamard 矩陣來構造任意高階的 Hadamard 矩陣。因此, 這也是一條很有希望的探索途徑。其他一些構造方法有許多都是上述方法的推廣和改進[11]。

我們下面談談等價類問題, 顯然 Hadamard 矩陣經過行交換、列交換、行乘$-1$, 列乘-1 後仍是 Hadamard 矩陣。如果 Hadamard 矩陣$\mathbf{H}_1$ 經過若干這樣的變換後得到 Hadamard 矩陣$\mathbf{H}_2$, 則稱$\mathbf{H}_1$和 $\mathbf{H}_2$是等價的。若記 $\mathbf{H}(n)$ 爲 $n$ 階 Hadamard 矩陣等價類的個數, 目前已知 $\mathbf{H}(1) = \mathbf{H}(2) = \mathbf{H}(4) = \mathbf{H}(8) = \mathbf{H}(12) = 1$, $\mathbf{H}(16) = 5, \mathbf{H}(20) = 3, \mathbf{H}(24) = 60$, $\mathbf{H}(28) \geq 487, \mathbf{H}(32) \geq 66,104, \mathbf{H}(36) \geq 110$ (參看 [9]), 當$n \geq 32$, 等價類數增長很快, 即使是借助於電子計算機也很難進行完整的分類。但是等價類問題的研究能促進構造方法的研究, 也能促進應用方面的研究。因此這是一個很有意義的研究方向。

在這方面, 有兩件事可以做。第一, 對給定的階數, 至少要有一種方法可以構造出一定數量的 Hadamard 矩陣; 第二, 要有簡單有效的分類方法對這些 Hadamard 矩陣進行分類處理。中國蘇州大學朱烈教授等人[9]對32階 Hadamard 矩陣的產生和分類做了有意義的工作。總的說來, 等價類問題還有待人們深入研究。

在理論應用方面, Hadamard 矩陣是同 Hadamard 組合設計、Hadamard 差集、 二元序列相互連繫的 [11],[7]。此外 Hadamard 矩陣可以用來構造 Walsh 函數[11], Williamson型 Hadamard 矩陣可以用來構造若干 PCS 序列 [7]。

另外, 大家已知大於4階的循環 Hadamard 矩陣的存在性問題是同長度大於13的 Barker 序列連結在一起的。普遍猜測是不存在大於4階的循環 Hadamard 矩陣。這個有三十多年歷史的猜想引起不少人的興趣。迄今爲止, 大家只知道當$n \leq 12$, 100時, 不存在$n$階循環 Hadamard 矩陣。猜想的眞正解決還有待於人們的進一步努力[8]。

在實際應用方面, Hadamard 矩陣已經有應用在影像處理和編碼方面的例子 [11][13]。但是, Hadamard 矩陣在圖像處理方面的效果不是最好的。$n$ =

$8t + 4$階的 Hadamard 矩陣可以用來構造自對偶$[2n, n, d]$糾錯碼, 這裡最小距離$d \geq 8$(參看 [13])。這是一個很好的性質。一個很有名的編碼問題是: 是否存在自對偶 [72,36,16]糾錯碼。大家自然想到用36階 Hadamard 矩陣來構造自對偶[72,36,16]糾錯碼, 但是現有已知的100多類36階 Hadamard 矩陣的等價類都只構造出自對偶 [72,36,8], [72,36,12]糾錯碼, 自對偶 [72,36,16]糾錯碼的存在性問題仍未獲解決 [6]。目前在這方面可以做的有兩件事。第一是至少要有一種新的構造方法產生大量的新的36階 Hadamard 矩陣等價類, 然後看能否找到自對偶 [72,36,16]糾錯碼, 第二是證明對36階 Hadamard 矩陣, 不存在自對偶 [72,36,16]糾錯碼。然而從現有的研究結果看來, 似乎任何一件事都不容易在短期內解決。

Hadamard 矩陣在科技日益發達的今天已經受到高度的重視。我們經常可以看到來自美國國防部和國家安全局的研究人員、來自澳大利亞國防部和密碼科研機構的研究人員活躍在國際組合數學和離散數學會議的講臺上報告 Hadamard 矩陣在組合設計、編碼和密碼方面的應用和研究。從 Sylvester 起126年來, Hadamard 矩陣的研究已有不少成果。但是許多老問題還沒有解決, 又有大量的新問題提出來, 等待我們去研究。我們可以發現 Hadamard 矩陣的研究是一個值得繼續開發的領域。

## 參考文獻


1. S.S. Agaian, "Hadamard Matrices and Their Applications," Lecture Notes in Math. No.1168, Springer-Verlag, 1985.
2. A.H. Baartmans, C. Lin and P.J.S. Shiue, On a criterion for symmetric Hadamard matrices, to appear in J. of Comb. Math. Comb. Comp., 15 (1994), 155-160.
3. J. Cooper, J. Milas and W.D. Wallis, Hadamard equivalence, "Combinatorial Mathematics," Lecture Notes in Math. No. 686, 126-135, Springer- Verlag, 1978.
4. R. Craigen, J. Seberry and X.M. Zhang, Product of four Hadamard matrices, J. Comb. Theory, A59(1992), 318-320.
5. J. Hadamard, Resolution dune question relative aux determinants, Bull. Sci. Math. 17(1893), 240-246.
6. C. Lin, H. Lin, W.D. Wallis and J.L. Yucas, Codes from Hadamard matrices and profiles of Hadamard matrices, J. of Comb. Math. Comb. Comp., 12 (1992), 57-64.
7. C. Lin and P.J.S. Shiue, Some families of periodic complementary binary sequences, preprint.
8. C. Lin and W.D. Wallis, Barker sequences and circulant Hadamard matrices, to appear in J. of Comb. Infor. and Sys Sci..
9. C. Lin, W.D. Wallis and Zhu Lie, Equivalence classes of Hadamard matrices of order 32, to appear in Cong Nume.
10. R.E.A.C. Paley, On orthogonal matrices, J. Math. and physics, 12(1933), 311-320.

11. J. Seberry and M. Yamad, Hadamard matrices, sequences, and block designs, "contemporary Design Theory:A Collection of Surveys," John Wiley, 1992, 431-560.
12. J.J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and lesselated pavements in two or more colours, with applications to Newton's rule, ornamental tilework and the theory of numbers, Phil. Mag. (4), 34 (1867), 461-475.
13. V.D. Tonchev, Self-orthogonal designs and extremal doubly even codes, J. Comb. Theory, A52(1989), 197-205.
14. W.D. Wallis, A.P. Street and J.S. Wallis, "Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices," Lecture Notes in Math. No.292, Springer-Verlag, 1972.
15. J. Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Math. J., 11(1944), 65-81.
16. M.Y. Xia, Some infinite classes of special Williamson matrices and difference sets, J. Comb. Theory, 61A(1992), 230-242.
17. X.M. Zhang, Semi-regular sets of matrices and applications, Australasian J. of Comb. 7(1993), 65-80.

**後記**: 本文作者感謝審稿人細心閱讀本文稿並提出寶貴建議。

—本文作者任教於美國Nevada 大學, Las Vegas校區數學系—