系 统 科 学 与 数 学
J. Sys. Sci. & Math. Scis.
8 (1) (1988), 52—55

高维 Hadamard 猜想的新证明*

杨义先　　胡正名
（北京邮电学院科学研究所）

众所周知，2 维 Hadamard 矩阵的阶数必须是 1 或 2 或 $4t$（此处 t 是某个正整数）. 反过来，著名的 Hadamard 猜想则说："对任意正整数 t，至少存在一个 2 维 $4t$ 阶的 Hadamard 矩阵."此猜想至今已有近百年的历史了，虽然许多数学家都曾经或正在为此猜想而绞尽脑汁，但是仍然没人能证明或否定它. 1979 年美国学者 P. J. Shlichta 将 Hadamard 矩阵的理论从 2 维推广到高维情形[1]，并提出了这样一个高维 Hadamard 猜想："高维 Hadamard 矩阵的阶数不受 $4t$ 的限制，即有可能存在阶数为 $2s \neq 4t$ (s 是奇数)的高维 Hadamard 矩阵."最近杨义先已在[2]中证明了上述高维 Hadamard 猜想是正确的. 在本文中我们将再给出一个更简单、更有力的新证明. 最后我们还得出了如下一个重要的结论："如果 2 维情形的 Hadamard 猜想正确，那么对任意正整数 n，$t(n \geqslant 4)$，恒存在 n 维 $2t$ 阶的 Hadamard 矩阵".

首先复述高维 Hadamard 矩阵的定义[1].

定义 1. 一个 n 维 m 阶矩阵 $A = [A_{i_1 i_2 \cdots i_n}]$ $(1 \leqslant i_1, i_2, \cdots, i_n \leqslant m)$ 称为 n 维 m 阶 Hadamard 矩阵，当且仅当 $A_{i_1 i_2 \cdots i_n} = \pm 1$ 并且对任意 $1 \leqslant k \leqslant n$ 和 $1 \leqslant x, y \leqslant m$ 恒有

$$\sum_{\substack{1 \leqslant i_j \leqslant m \\ 1 \leqslant j \leqslant n \\ j \neq k}} A_{i_1 \cdots i_{k-1} x i_{k+1} \cdots i_n} \cdot A_{i_1 \cdots i_{k-1} y i_{k+1} \cdots i_n} = m^{(n-1)} \cdot \delta_{xy}.$$

其中

$$\delta_{xy} \triangleq \begin{cases} 1, & x = y, \\ 0, & x \neq y. \end{cases}$$

从定义 1 不难看出当 $n = 2$ 时它就是所熟知的 Hadamard 矩阵的定义. 仿照 2 维 Hadamard 矩阵理论中的方法很容易证明：高维 Hadamard 矩阵的阶数必须是 1 或 $2t$ (t 是某个正整数). 可是它的逆命题成立吗？下面就来回答这一问题.

定理 1. 设 $A = [A_{ij}]$ $(0 \leqslant i, j \leqslant (2t)^s - 1)$ 是一个 2 维 $(2t)^s$ 阶的 Hadamard 矩阵. 此处 $s > 1$，t 是任意正整数. 如果对任意 $0 \leqslant x_k, y_k \leqslant 2t - 1$，$0 \leqslant k \leqslant s - 1$，令

$$B_{x_0 \cdots x_{s-1}, y_0 \cdots y_{s-1}} = A_{(2t)^{s-1} x_{s-1} + (2t)^{s-2} x_{s-2} + \cdots + 2t x_1 + x_0, (2t)^{s-1} y_{s-1} + (2t)^{s-2} y_{s-2} + \cdots + 2t y_1 + y_0}.$$

那么矩阵 $B = [B_{x_0 \cdots x_{s-1}, y_0 \cdots y_{s-1}}]$，$(0 \leqslant x_i, y_i \leqslant 2t - 1)$ 就是一个 $2s$ 维 $2t$ 阶的 Hada-

* 中国科学院科学基金资助课题.
1986 年 11 月 2 日收到，1987 年 6 月 27 日收到修改稿.

mard 矩阵.

证. 记 $X \triangleq \{(x_0,\cdots,x_{s-1}),0\leqslant x_i\leqslant 2t-1\}$, $I_k \triangleq (x_0,x_0,\cdots,x_{s-1})$, $J_k \triangleq (y_0,y_1,\cdots,y_{s-1})$, 对 $0\leqslant k\leqslant s-1$, 此处 I_k 和 J_k 中的第 k 个足标是固定的.

又令 $I=\sum_{p=0}^{s-1} x_p(2t)^p$, $J=\sum_{p=0}^{s-1} y_p(2t)^p$,

$$\alpha_k(a,b) \triangleq \sum_{I_k,J} [B_{x_0,\cdots,x_{k-1},a,x_{k+1},\cdots,x_{s-1},y_0,\cdots,y_{s-1}} \cdot B_{x_0,\cdots,x_{k-1},b,x_{k+1},\cdots,x_{s-1},y_0,\cdots,y_{s-1}}].$$

$$\beta_k(a,b) \triangleq \sum_{I,J_k} [B_{x_0,\cdots,x_{s-1},y_0,\cdots,y_{k-1},a,y_{k+1},\cdots,y_{s-1}} \cdot B_{x_0,\cdots,x_{s-1},y_0,\cdots,y_{k-1},b,y_{k+1},\cdots,y_{s-1}}].$$

于是可知,

$$\alpha_k(a,b)=\sum_{I_k}\left[\sum_J A_{\langle I_x,a\rangle,J}\cdot A_{\langle I_x,b\rangle,J}\right]$$

$$=\sum_{I_k}\left[\sum_J^{(2t)^s-1} A_{\langle I_x,a\rangle,J}\cdot A_{\langle I_x,b\rangle,J}\right]=(2t)^{2s-1}\cdot\delta_{ab},$$

$$\beta_k(a,b)=\sum_{J_k}\left[\sum_I A_{I,\langle I_y,a\rangle}\cdot A_{I,\langle I_y,b\rangle}\right]=(2t)^{2s-1}\cdot\delta_{ab}.$$

(上述最后一个等式是因为矩阵 $A=[A_{ij}]$ 是一个 2 维 $(2t)^s$ 阶 Hadamard 矩阵.)根据定义 1 立即可知 $B=[B_{x_0,\cdots,x_{s-1},y_0,\cdots,y_{s-1}}]$ 的确是一个 $2s$ 维 $2t$ 阶的 Hadamard 矩阵.

注.证明过程中的一些符号的含义如下:

$$\langle I_{x,a}\rangle=\sum_{i=0}^{k-1} x_i(2t)^i+a\cdot(2t)^k+\sum_{i=k+1}^{s-1} x_i\cdot(2t)^i;$$

$\langle I_{x,b}\rangle$, $\langle I_{y,a}\rangle$, $\langle I_{y,b}\rangle$ 的含义与 $\langle I_{x,a}\rangle$ 同. 证毕.

利用定理 1 就可给出高维 Hadamard 猜想的一个新证明. 例如,我们已知 2 维 $36=6^2=(2\times 3)^2$ 阶的 Hadamard 矩阵是存在的,因此利用定理 1 就可造出 4 维 6 阶 Hadamard 矩阵. 而 6 显然不是 4 的倍数,这当然就证明了高维 Hadamard 猜想. 但是我们不打算就此停步,还要继续给出更深刻的结论.

引理. 如果 $0\leqslant a,b,j\leqslant N-1$, 并且 $a\neq b$, 那么 $[a+j]_N\neq[b+j]_N$. 此处 $[x]_N\equiv x(\mathrm{mod}N)$. $0\leqslant[x]_N\leqslant N-1$. 另外还有 $\{[a+x]_N:\ 0\leqslant x\leqslant N-1\}=\{x:0\leqslant x\leqslant N-1\}$.

证明很容易,略去.

定理 2. 设 $H=[H_{i_1,\cdots,i_n}]$ $(0\leqslant i_1,\cdots,i_n\leqslant N-1)$ 是一个 n 维 N 阶 Hadamard 矩阵. 如果对任意的 $0\leqslant i_1,\cdots,i_n,i_{n+1}\leqslant N-1$ 令

$$A_{i_1,\cdots,i_{n+1}} \triangleq H_{i_1,\cdots,i_{n-1},[i_n+i_{n+1}]_N}$$

那么矩阵 $A=[A_{i_1,\cdots,i_{n+1}}]$ 就是一个 $n+1$ 维 N 阶的 Hadamard 矩阵.

证.记

$$\alpha_k(a,b) \triangleq \sum_I A_{i_1,\cdots,i_{k-1},a,i_{k+1},\cdots,i_{n+1}}\cdot A_{i_1,i_{k-1},b,i_{k+1},\cdots,i_{n+1}},$$

其中 $1 \leqslant k \leqslant n$, $\sum_{I}$ 表示对所有 $0 \leqslant i_j \leqslant N-1$ 求和. 于是可知

$$\begin{aligned}\alpha_k(a,b) &= \sum_{I} H_{i_1,\cdots,i_{k-1},a,i_{k+1},\cdots,[i_n+i_{n+1}]_N} \cdot H_{i_1,\cdots,i_{k-1},b,i_{k+1},\cdots,[i_n+i_{n+1}]_N} \\ &= \sum_{i_{n+1}=0}^{N-1} \left\{ \sum_{0\leqslant i_1,\cdots,i_n\leqslant N-1} H_{i_1,\cdots,i_{k-1},a,i_{k+1},\cdots,i_n} \cdot H_{i_1,\cdots,i_{k-1},b,i_{k+1},\cdots,i_n} \right\} \\ &= \sum_{i_{n+1}=0}^{N-1} N^{n-1} \cdot \delta_{ab}\end{aligned}$$

(最后一个等式是因为 $H = [H_{i_1,\cdots,i_n}]$ 是 n 维 N 阶 Hadamard 矩阵).

根据引理知当 $a \neq b$ 时 $[i_n + a]_N \neq [i_n + b]_N$, 并且 $\{[x+a]_N : 0 \leqslant x \leqslant N-1\} = \{x : 0 \leqslant x \leqslant N-1\}$, 再由于 $H = [H_{i_1,\cdots,i_n}]$ 是 n 维 N 阶 Hadamard 矩阵, 所以

$$\begin{aligned}&\sum_{0\leqslant i_1,\cdots,i_n\leqslant N-1} H_{i_1,\cdots,i_{n-1},[i_n+a]_N} \cdot H_{i_1,\cdots,i_{n-1},[i_n+b]_N} \\ &= \sum_{i_n=0}^{N-1} \left[\sum_{0\leqslant i_1,\cdots,i_{n-1}\leqslant N-1} H_{i_1,\cdots,i_{n-1},[i_n+a]_N} \cdot H_{i_1,\cdots,i_{n-1},[i_n+b]_N} \right] \\ &= \sum_{i_n=0}^{N-1} N^{n-1} \cdot \delta_{ab} = N^n \cdot \delta_{ab}.\end{aligned}$$

综上所述可知 $A = [A_{i_1,\cdots,i_{n+1}}]$ 是 $n+1$ 维 N 阶的 Hadamard 矩阵. 证毕.

如果 2 维情形的 Hadamard 猜想正确, 那么由定理 1 知对任意 $2t(t>1)$ 和 $2s$ 都至少存在着一个 $2t$ 维 $2s$ 阶的 Hadamard 矩阵. 再由定理 2 知也至少存在着一个 $2t+1$ 维 $2s$ 阶的 Hadamard 矩阵, 综合起来就得到了.

定理 3. 若 2 维情形的 Hadamard 猜想正确, 那么对任意正整数 $n(n \geqslant 4)$, t, 恒存在 n 维 $2t$ 阶的 Hadamard 矩阵.

充分利用上述三个定理可以造出许多其它类型的阶数为 $2s \neq 4t$ 的高维 Hadamard 矩阵. 当然也就证明了高维 Hadamard 猜想. 如已知 2 维 216 阶 Hadamard 矩阵的存在性 (实际上现在已知道当 $4t < 428$ 时都至少存在一个 2 维 $4t$ 阶的 Hadamard 矩阵), 利用定理 1 就知 6 维 6 阶的 Hadamard 矩阵都存在, 这是因为 $216 = (2\times 3)^3$. 更进一步利用定理 2 知, 对任意 $n \geqslant 4$ 都至少存在一个 n 维 6 阶 Hadamard 矩阵.

在 Hadamard 矩阵理论中存在性问题一直是个很重要而且很难的问题. 在 2 维情形, 前人已取得了许多令人兴奋的结果. 当 $n \geqslant 4$ 时, 本文定理 3 又将 n 维 Hadamard 矩阵的存在性问题完全建立在 2 维情形之上. 可是对 3 维情形的存在性又怎样呢? 到目前为止还没有人找到一个 3 维 $2s \neq 4t$ 阶的 Hadamard 矩阵, 甚至连一个 3 维 6 阶 Hadamard 矩阵都未找到. 所以 3 维 Hadamard 矩阵的存在性问题目前还是一个谜. 欢迎有志的读者努力揭开这一个谜底.

致谢: 感谢周炯槃, 蔡长年教授的大力帮助. 感谢审稿同志的有益建议

参 考 文 献

[1] Shlichta, P. J., Higher Dimensional Hadamard Matrices, *IEEE Trans. on Inform.*, IT-**25**; 5(1979),

566-572.
[2] 杨义先,高维 Hadamard 矩阵的几个猜想之证明,科学通报,2(1986),85—88.
[3] 杨义先,胡正名,4 维 2 阶 Hadamard 矩阵的分类,系统科学与数学,7(1)(1987),47—54.
[4] 杨义先,朱庆棠,高维矩阵的运算及应用,成都电讯工程学院学报,2(1987),191—199.
[5] 潘新安,杨义先,5 维 2 阶 Hadamard 矩阵的计数,北京邮电学院学报, 4(1987).
[6] Hammer, J. and Seberry, J. R., Higher Drmensional orthogonal designs and Applications, *IEEE Trans. on Inform.*, IT-27: 6(1981), 772—779.
[7] Yang Yi Xian, New Public key distribution Systems, Electron. Letter. 21st May 1987 **23**:11, 560—561.
[8] 杨义先,关于等重码的 Johnson 界和 Graham 界的注记,电子科学学刊, 4(1987).

A NEW PROOF FOR THE HIGHER DIMENSIONAL HADAMARD MATRICES

YANG YI-XIAN HU ZHENG-MING
(Beijing Institute of Posts & Telecommunications)

ABSTRACT

A more powerful and simpler proof for the higher dimensional Hadamard conjecture (i.e. there may exist n-dimensional Hadamard matrices of order $m=2s\neq 4t$) proposed by P. J. Shlichta is provided. It is also proved that if the two-dimensional Hadamard conjecture is true, then for any integers $n(n\geqslant 4)$, there exists at least one n-dimensional Hadamard matrix of order $2t$.