A Product for Twelve Hadamard Matrices

Warwick de Launey
Cryptomathematics Research Group
Communications Division, ERL,
Defence Science and Technology Organisation,
Australia

Abstract

In 1867, Syvlester noted that the Kronecker product of two Hadamard matrices is an Hadamard matrix. This gave a way to obtain an Hadamard matrix of exponent four from two of exponent two. Early last decade, Agayan and Sarukhanyan found a way to combine two Hadamard matrices of exponent two to obtain one of exponent three, and just last year Craigen, Seberry and Zhang discovered how to combine four Hadamard matrices of exponent two to obtain one of exponent four. Using these products one can combine twelve Hadamard matrices of exponent two to obtain one of exponent ten. This paper describes how to obtain one of exponent nine.

1 Introduction

Recently, product constructions for Hadamard matrices which improve on the Kronecker product have been discovered. Agayan [1] gave a method for combining two Hadamard matrices of orders $4a$ and $4b$ to obtain one of order $8ab$. Later, Craigen, Seberry and Zhang [3] showed how to obtain an Hadamard matrix of order $16abcd$ from four Hadamard matrices of orders $4a, 4b, 4c$ and $4d$, respectively. Both these "product" constructions were improvements on earlier methods: (i) the first construction gives a matrix of order $8ab$ whereas the Kronecker product gives a matrix of order $16ab$; and (ii) the second construction gives a matrix of order $16abcd$ whereas two applications of the Agayan-Sarukhanyan product gives a matrix of order $32abcd$.

These constructions generated considerable interest, and it was asked whether further improvements could be made when more matrices are to be combined.

In this paper, we describe an improvement when twelve Hadamard matrices are to be combined. We frame our discussions in terms of the exponent: an Hadamard matrix of order $2^e q$, where q is odd, has exponent equal to e. Using previous products, the smallest order which can be obtained is acheived by using the Craigen-Seberry-Zhang product three times and the Agayan-Sarukhanyan product twice. If the initial twelve Hadamard matrices have exponent equal to two, then the resulting matrix has exponent equal to ten. We give a construction which produces a matrix of exponent nine.

2 Orthogonal Pairs and Disjoint Weighing Matrices

The Agayan-Sarukhanyan product and the Craigen-Seberry-Zhang product can be described in terms of two key concepts: orthogonal pairs and disjoint weighing matrices.

Two $a \times a$ $(1,-1)$-matrices X and Y comprise an *orthogonal pair* if

$$XX^T + YY^T = 2aI_a,$$

and

$$XY^T = 0.$$

Two weighing matrices $W(2b, b)$, $W = (w_{ij})$ and $Z = (z_{ij})$ are *disjoint* if $w_{ij}z_{ij} = 0$ for all $1 \leq i, j \leq 2b$. We say X and Y comprise an $OP(a)$, and W and Z are $DW(2b)$.

Craigen [2] and Seberry and Zhang [4] proved the following results.

Theorem A (Craigen). *If there are Hadamard matrices of orders* $4a$ *and* $4b$, *then there is an* $OP(4ab)$.

Theorem B (Seberry and Zhang). *If there are Hadamard matrices of orders* $4a$ *and* $4b$, *then there are* $DW(4ab)$.

We give brief proofs of these results, and show how they lead to the Agayan-Sarukhanyan product and the Craigen-Seberry-Zhang product. Let the two

Hadamard matrices be partitioned as below.

$$\begin{bmatrix} H_1 & H_2 & H_3 & H_4 \end{bmatrix} \qquad\qquad \begin{bmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{bmatrix}$$

The matrices H_i are $4a \times a$ matrices, and the matrices K_i are $b \times 4b$ matrices.

The matrices A and B, defined by the equations below, comprise an $OP(4ab)$.

$$2A = (H_1 + H_2) \times K_1 + (H_1 - H_2) \times K_2,$$

and

$$2B = (H_3 + H_4) \times K_3 + (H_3 - H_4) \times K_4.$$

The required disjoint weighing matrices W and Z are given by the following equations.

$$2W = A + B,$$

and

$$2Z = A - B.$$

Similarly, starting with Hadamard matrices of orders $4c$ and $4d$, we could produce $DW(4cd)$ matrices X and Y.

The Agayan-Sarukhanyan product and the Craigen-Seberry-Zhang product follow from the observation that the matrices

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

and

$$A \times X + B \times Y$$

are respectively Hadamard matrices of orders $8ab$ and $16abcd$.

3 A Product for Twelve Hadamard Matrices

Theorem. *Suppose there are twelve Hadamard matrices with the orders $4a, 4b, 4c, \cdots, 4k, 4l$; then there is an orthogonal pair of order $256abcd \cdots kl$, and an Hadamard matrix of order $512abcd \cdots kl$.*

Proof. Use the Craigen-Seberry-Zhang product to obtain Hadamard matrices of orders $16abcd$ and $16efgh$. Partition these matrices as follows.

$$\begin{bmatrix} H_1 & H_2 & \cdots & H_{16} \end{bmatrix} \qquad \begin{bmatrix} K_1 \\ K_2 \\ \vdots \\ K_{16} \end{bmatrix}$$

The matrices H_i are $16abcd \times abcd$ matrices, and the matrices K_i are $efgh \times 16efgh$ matrices. Next, use the remaining Hadamard matrices to obtain $DW(4ij)$, W and X, and $DW(4kl)$, Y and Z. Define the matrices A and B by the following equations.

$$\begin{aligned} 2A = & \quad W \times Y \times (H_1 + H_2) \times K_1 + (H_1 - H_2) \times K_2 \\ & + \; W \times Z \times (H_3 + H_4) \times K_3 + (H_3 - H_4) \times K_4 \\ & + \; X \times Y \times (H_5 + H_6) \times K_5 + (H_5 - H_6) \times K_6 \\ & + \; X \times Z \times (H_7 + H_8) \times K_7 + (H_7 - H_8) \times K_8, \end{aligned}$$

and

$$\begin{aligned} 2B = & \quad W \times Y \times (H_9 + H_{10}) \times K_9 + (H_9 - H_{10}) \times K_{10} \\ & + \; W \times Z \times (H_{13} + H_{12}) \times K_{11} + (H_{11} - H_{12}) \times K_{12} \\ & + \; X \times Y \times (H_{13} + H_{14}) \times K_{13} + (H_{13} - H_{14}) \times K_{14} \\ & + \; X \times Z \times (H_{15} + H_{16}) \times K_{15} + (H_{15} - H_{16}) \times K_{16}. \end{aligned}$$

It is simple to check that A and B comprise an orthogonal pair of the required order.

References

[1] S. S. AGAYAN. *Hadamard Matrices and their Applications. Vol. 1168 of Lecture Notes in Mathematics*, Springer-Verlag, Berlin-Heidelberg-New York,1985.

[2] R. CRAIGEN. Constructing Hadamard matrices with orthogonal pairs. *Ars Comb.*. To appear.

[3] R. CRAIGEN, J. SEBERRY and XIAN-MO ZHANG. Product of four Hadamard matrices. *J. Comb. Th. Ser. A.* 59:318-320, 1992.

[4] J. SEBERRY and XIAN-MO ZHANG. Some orthogonal matrices constructed by strong Kronecker multiplication. *Austral. J. Comb.*. To appear.

[5] J. J. SYLVESTER. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's Rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.*, 34:4:461-475, 1867.

(Received 16/7/92)