AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **35** (2006), Pages 83–87

Jacket matrices constructed from Hadamard matrices and generalized Hadamard matrices *

Ken Finlayson

Centre for Computer Security Research
University of Wollongong
N.S.W. 2522
Australia

Moon Ho Lee

Institute of Information and Communications
Chonbuk National University, Jeonju
Korea

Jennifer Seberry

Centre for Computer Security Research
University of Wollongong
N.S.W. 2522
Australia

Mieko Yamada

Department of Computational Science
Kanazawa University
Kakuma-machi, Kanazawa
Japan

Abstract

Jacket matrices are matrices $L = (\ell_{ij})$ with inverse $L^{-1} = \frac{1}{n}\left(\ell_{ij}^{-1}\right)$, where the inverse is over a group G. They have previously been constructed only from $(1, -1)$ Hadamard matrices. In this note, we give constructions for jacket matrices based on generalized Hadamard matrices.

* This work was partially supported by the Institute of Information Technology Assessment, Korea, the Korea Science and Engineering Foundation (KOSEF), Korea and the Australian Academy of Science.

1 Introduction

Let H be a matrix. We define $H^\dagger$ to be the Hermitian conjugate, or the transpose of the matrix with elements the complex conjugate of the corresponding elements of H. When the entries of H are from a group G, we define H^M to be the transpose of the matrix whose elements are the group inverse of the corresponding elements of H.

An Hadamard matrix H of order n is square, with entries ± 1 and satisfies $HH^T = H^TH = nI$. Seberry and Yamada [10] have surveyed Hadamard matrices and the reader is referred there for more details.

In this paper, if $HH^\dagger = H^\dagger H = nI$ then H is a generalized Hadamard matrix. More generally, generalized Hadamard matrices of two types are of interest. The first (see [1,4]) have entries which are roots of unity; the second (see [2,3,8,9]) have elements from a finite group.

Let p be an odd prime. Let $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$ be the pth roots of unity. A Butson generalized Hadamard matrix [1] $B = (b_{ij})$ of order p is defined as

$$b_{ij} = \begin{cases} 1 & i = 1 \text{ and } 1 \le j \le p \\ 1 & j = 1 \text{ and } 1 \le i \le p \\ \alpha^{(i-1)(j-1)} & 2 \le i, j \le p \end{cases}$$

Then the core C of B is the $(p-1) \times (p-1)$ matrix (b_{st}), $2 \le s, t \le p$. We observe that $C, C^\dagger$ and C^M are symmetric, and that $C^\dagger = C^M$ is a permutation of C.

A jacket matrix (sometimes called a reverse jacket matrix) $L = (\ell_{ij})$ is a matrix of order n with entries from a group G, with inverse $L^{-1} = \frac{1}{n}\left(\ell_{ij}^{-1}\right)$.

We can use a jacket matrix L in a jacket transform (also called a reverse jacket transform) as follows. For a vector $\mathbf{a}$ of length n, its transform $\mathbf{A}$ is given by $\mathbf{A} = \mathbf{a}L$. The inverse transform is $\mathbf{a} = \mathbf{A}L^{-1} = \frac{1}{n}\mathbf{A}L^M$.

2 Our constructions

Jacket matrices in their original formulation were constructed from $(1, -1)$ Hadamard matrices (see [5–7]). However, it is possible to construct jacket matrices from generalized Hadamard matrices. We present three such constructions. We also give a method of combining such jacket matrices to form larger jacket matrices.

Let A, B, D be symmetric matrices of order $\frac{n-2}{2}$, whose elements are in an Abelian group (including 1). Let e be a column vector whose elements are all 1. Put

$$X = \begin{pmatrix} 1 & e^t & e^t & 1 \\ e & A & B & e \\ e & B & -D & -e \\ 1 & e^t & -e^t & -1 \end{pmatrix}.$$

If X satisfies

$$XX^M = X^M X = nI$$

then X is a jacket matrix.

2.1 Case 1: $A = B = D$

Let

$$A = B = D = \begin{pmatrix} \omega & \omega^2 \\ \omega^2 & \omega \end{pmatrix},$$

where ω is the cube root of unity. Then

$$X = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \\ 1 & \omega & \omega^2 & -\omega & -\omega^2 & -1 \\ 1 & \omega^2 & \omega & -\omega^2 & -\omega & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix}$$

is a 6×6 jacket matrix.

2.2 Case 2: Butson Generalized Hadamard matrices

Let B be a Butson generalized Hadamard matrix of order p, p an odd prime. Let C be the core of B, as defined earlier. Let $A = C$, $B = C^M$, $D = -C$. Then

$$X = \begin{pmatrix} 1 & e^t & e^t & 1 \\ e & C & C^M & e \\ e & C^M & -C & -e \\ 1 & e^t & -e^t & -1 \end{pmatrix}$$

is a $2p \times 2p$ jacket matrix. We observe that the $p = 3$ case is a permutation of the jacket matrix in part 2.1.

Theorem 1 *Let p be an odd prime. Then for every order $2p$, there is a jacket matrix whose entries are the pth roots of unity.*

Taking the Kronecker product of X with t copies of $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $t \geq 1$, gives the following:

Theorem 2 *Let p be an odd prime. Then there are jacket matrices of order $2^{t+1}p$, $t \geq 0$.*

Where the matrix X has a border of ± 1, the jacket matrices constructed by the Kronecker product will have a t-deep border of $\pm H_2$. We call such a matrix a jacket matrix with t-size border.

2.3 Case 3: Other generalized Hadamard matrices

Theorem 3 *Given a symmetric generalised Hadamard matrix*

$$G = (g_{ij}) = GH(n, \boldsymbol{G})$$

of order n over the group $\boldsymbol{G}$, there exists a jacket matrix of order $2^{t+1}n, t \geq 1$.

For example, consider the matrix $GH(6; \mathbb{Z}_3)$

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & \omega & 1 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & 1 & \omega & \omega^2 \\ 1 & \omega & 1 & \omega & \omega^2 & \omega^2 \end{pmatrix}$$

Then the core C of G can be used to construct a jacket matrix of order 12, using the construction in part 2.2.

2.4 A general result

Theorem 4 *Let $D_1, D_2, \ldots, D_k$ be jacket matrices, where D_i has order $2^{t_i+1}n_i$, $t_i \geq 0$. Then the Kronecker product*

$$D_1 \otimes \cdots \otimes D_k \underbrace{\otimes H_2 \cdots \otimes H_2}_{\ell \text{ times}}$$

is a jacket matrix with ℓ-size border, of order $2^m \prod_{i=1}^k n_i$, where $m = k + \ell + \sum_{i=1}^k t_i$.

References

[1] A. T. Butson, Generalized Hadamard matrices, *Proceedings of the American Mathematical Society* 13 (1963), 894–898.

[2] W. de Launey, Generalised Hadamard matrices whose rows and columns form a group, in *Combinatorial Mathematics X*, volume 1036 of *Lecture Notes in Mathematics*, pp. 154–176, Berlin-Heidelberg-New York, 1983. Springer-Verlag.

[3] W. de Launey, A survey of generalised Hadamard matrices and difference matrices $D(k, \lambda; g)$ with large k, *Utilitas Math.* 30 (1986), 5–29.

[4] D. A. Drake, Partial λ-geometries and generalized matrices over groups, *Canad. J. Math.* 31 (1979), 617–627.

[5] M.H. Lee, The center weighted Hadamard transform, *IEEE Trans. Circuits Syst.* 36 (1989), 1247–1249.

[6] M.H. Lee, Fast complex reverse jacket transform, In *Proc. 22nd Symp. Information Theory and its Application (SITA99)*, Yuzawa, Niigata, Japan, Nov. 30–Dec. 3 1999.

[7] M.H. Lee, B. S. Rajan and J. Y. Park, A generalized reverse jacket transform, *IEEE Trans. Circuits Syst. II*, 48(7) (2001), 684–690.

[8] V. Mavron and V. D. Tonchev, On symmetric nets and generalized Hadamard matrices from affine designs, *J. Geometry* 67 (2000), 180–187.

[9] J. Seberry, A construction for generalized Hadamard matrices, *J. Statistical Inference and Planning* 6 (1980), 365–368.

[10] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in J. H. Dinitiz and D. R. Stinson, eds., *Contemporary design theory: a collection of surveys*, pp. 431–560. John Wiley & Sons, 1992.

(Received 4 Nov 2004)