On G-Matrices

Christos Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 157 73
Athens
Greece

and

Jennifer Seberry
Department of Computer Science
University of Wollongong
Wollongong
NSW 2522
Australia

Abstract

G-matrices for the new orders 21, 23, 25 and 27 are constructed. Some constructions for Hadamard matrices and orthogonal designs using G-matrices are also presented.
Key words and phrases: Hadamard matrix, orthogonal design
AMS Subject Classification: Primary 05B20

1 Introduction

Let X_1, X_2, X_3, X_4, be four type 1 ± 1 matrices on the same group of order n (odd) with the properties :

(i) $(X_i - I)^T = -(X_i - I)$, $i = 1, 2$,

(ii) $X_i^T = X_i$, $i = 3, 4$ and the diagonal elements are positive,

(iii) $X_i X_j = X_j X_i$,

(iv) $X_1 X_1^T + X_2 X_2^T + X_3 X_3^T + X_4 X_4^T = 4nI_n$.

Call such matrices *G-matrices*. These were first introduced and applied to construct Hadamard matrices by Jennifer Seberry Wallis [3]. G-matrices of orders 3, 5, 7, 9, 13, 15, 19 were known previously, see [3, 5, 6]. This note constructs G-matrices of order 21, 23, 25 and 27 for the first time.

Remark 1 Multiplying both sides of (iv) by J shows G-matrices can only exist for orders n for which

$$4n = 1^2 + 1^2 + a^2 + b^2$$

where a, b are odd integers. So, for example, they cannot exist for the following orders ≤ 50: 11, 17, 29, 35, 39, 47.

G-matrices which are constructed using four circulants exist for at least $n = 3, 5, 7, 9, 13, 15$, and 19, see [3, 5, 6], and for $n = 21, 23, 25$, and 27 which are constructed in this note. This means the first unresolved case is for $n = 31$.

2 Construction of G-matrices

The following first rows may be used to give circulant matrices which can be used in the Goethals-Seidel array to find G-matrices of order:

$4n = 4 \times 21 = 84 = 1^2 + 1^2 + 1^2 + 9^2$,

$$\{+++---++-++--+--+++--\}$$
$$\{+++-+++----++++---+--\}$$
$$\{+-+-+-++-+--+-++-+-+-\}$$
$$\{+++++++--+--+--++++++\},$$

$4n = 4 \times 23 = 84 = 1^2 + 1^2 + 3^2 + 9^2$,

$$\{+++-+++---+-+-+++---+--\}$$
$$\{++++--+++++-+------++---\}$$
$$\{+--++-++-+-++-+-++-++--\}$$
$$\{++-+----+------+----+-+\},$$

$4n = 4 \times 25 = 100 = 1^2 + 1^2 + 7^2 + 7^2$,

$$\{++++-+--+++--++---++-+---\}$$
$$\{+++++-+++-++-+--+---+----\}$$
$$\{+--+---+---++++---+---+--\}$$
$$\{++-+-----+-+--+-+-----+-+\},$$

and $4n = 4 \times 27 = 108 = 1^2 + 1^2 + 5^2 + 9^2$,

$$\{++++-+-+----++--++++-+-+---\}$$
$$\{+++-++----+-+-+-+-++++--+--\}$$
$$\{+------++-++-++-++-++------\}$$
$$\{++----+--+---++---+--+----+\}.$$

3 Constructions using G-matrices

First we note that we have

Lemma 1 *If there exist circulant G-matrices of order n then there exists an* $OD(4n; 1, 1, 2n-1, 2n-1)$.

Corollary 1 *Let* $n = 3, 5, 7, 9, 13, 15, 19, 21, 23, 25,$ *or* 27. *Then an* $OD(4n; 1, 1, 2n-1, 2n-1)$ *exists.*

We recall the following definitions and results from [3]. The following theorem shows how the Williamson construction (the B_i) and the Goethals-Seidel construction (the A_i) may be combined to construct Hadamard matrices.

Theorem 1 (Jennifer Seberry Wallis (1975)) *Suppose A_i and B_i, $i = 1, 2, 3, 4$ are type 1 (± 1) matrices of order a and b, respectively, which satisfy*

(i) $A_iA_j = A_jA_i$ $i, j = 1,2,3,4$

(ii) $B_iB_j^T = B_jB_i^T$ $i, j = 1,2,3,4$

(iii) $\sum_{i=1}^{4}(A_i \times B_i)(A_i \times B_i)^T = 4abI_{ab}$

then H defined as

$$\begin{array}{cccc} A_1 \times B_1 & A_2R \times B_2 & A_3R \times B_3 & A_4R \times B_4 \\ -A_2R \times B_2 & A_1 \times B_1 & A_4^TR \times B_4 & -A_3^TR \times B_3 \\ -A_3R \times B_3 & -A_4^TR \times B_4 & A_1 \times B_1 & A_2^TR \times B_2 \\ -A_4R \times B_4 & A_3^TR \times B_3 & -A_2^TR \times B_2 & A_1 \times B_1 \end{array}$$

is an Hadamard matrix of order 4ab.

We will call the matrices $A_i \times B_i$, $i = 1, 2, 3, 4$ of the theorem F-matrices and we will say H is a Wallis-Whiteman like Hadamard matrix.

The A_i will be called the GS-part and the B_i the W-part of the F-matrix.

The following theorem shows how G-matrices may be used to construct F-matrices.

Theorem 2 (Jennifer Seberry Wallis (1975)) *Let X_1, X_2, X_3, X_4 be G-matrices of order n. Suppose A,B,C are suitable ± 1 matrices of order m for an $OD(4n; 1, 1, 4n-2)$ ie they satisfy*

(i) AB^T, AC^T, BC^T *are symmetric,*

(ii) $AA^T + BB^T + (4n-2)CC^T = 4nmI_m$.

Then

$$\begin{aligned} A_1 &= I \times A + (X_1 - I) \times C \\ A_2 &= I \times B + (X_2 - I) \times C \\ A_3 &= X_3 \times C \\ A_4 &= X_4 \times C \end{aligned}$$

are F-matrices of order mn.

Corollary 2 *Let $n = 3,5,7,9,13,15,19,21,23,25$ or 27. Suppose A, B, C are pairwise amicable (± 1) matrices of order m satisfying*

$$AA^T + BB^T + (4n-2)CC^T = 4mnI_m.$$

Then there are F-matrices of order mn and a Wallis-Whiteman like Hadamard matrix of order $4mn$.

Corollary 3 *Let $n = 3,5,7,9,13,15,21,23$. Set $A = J_{2n+1}$, $B = (J - 2I)_{2n+1}$, and C the back-circulant or type 1 matrix of order $2n+1$ obtained from the quadratic residues. Then*

$$AA^T + BB^T + (4n-2)CC^T = 4(2n+1)nI_{2n+1},$$

and hence there are F-matrices of order $(2n+1)n$ and a Wallis-Whiteman like Hadamard matrix of order $4(2n+1)n$.

We further extend the last theorem by observing

Theorem 3 *Let X_1, X_2, X_3, X_4 be G-matrices of order n. Suppose A,B,C,D are suitable ± 1 matrices of order m for an $OD(4n;1,1,2n-1,2n-1)$ ie they satisfy*

(i) *PQ^T is symmetric for all $P, Q \in \{A, B, C, D\}$,*

(ii) $AA^T + BB^T + (2n-1)CC^T + (2n-1)DD^T = 4nmI_m$,

Then defining $Y_1 = (X_1+X_2-2I)/2$, $Y_2 = (X_1-X_2)/2$, $Y_3 = (X_3+X_4)/2$ and $Y_4 = (X_3-X_4)/2$

$$B_1 = I \times A + Y_1 \times C + Y_2 \times D$$

$$B_2 = I \times B + Y_1 \times D + Y_2 \times C$$

$$B_3 = Y_3 \times C + Y_4 \times D$$

$$B_4 = Y_3 \times D + Y_4 \times C$$

are F-matrices of order mn.

Corollary 4 *Let $n = 3,5,7,9,13,15,19,21,23,25$ or 27. Suppose A, B, C, D are pairwise amicable (± 1) matrices of order m satisfying*

$$AA^T + BB^T + (2n-1)CC^T + (2n-1)DD^T = 4mnI_m.$$

Then there are F-matrices of order mn and a Wallis-Whiteman like Hadamard matrix of order $4mn$.

Corollary 5 *Let $n = 3,5,7,9,13,15,19,21,23,25$ or 27. Set $A = B = J_{2n-1}$, and $C - I = D + I$ the back-circulant or type 1 matrix of order $2n-1$ with zero diaginal obtained from the quadratic residues or the core of a symmetric conference matrix of order $2n+2$. Then*

$$AA^T + BB^T + (2n-1)CC^T + (2n-1)DD^T = 4(2n-1)nI_{2n-1}.$$

and hence there are F-matrices of order $(2n-1)n$ and a Wallis-Whiteman like Hadamard matrix of order $4(2n-1)n$.

References

[1] A. V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel, 1979.

[2] Jennifer Seberry and Mieko Yamada, Hadamard matrices, sequences and block designs, in *Contemporary Design Theory - a Collection of Surveys*, eds J. Dinitz and D.R. Stinson, John Wiley and Sons, New York, pp431-560, 1992.

[3] Jennifer Seberry Wallis, On Hadamard matrices, *J. Combin. Theory Ser. A* 18 (1975), 149-164.

[4] Jennifer Seberry Wallis, Hadamard matrices, Part IV, *Combinatorics: Room Squares, sum free sets and Hadamard Matrices*, Lecture Notes in Mathematics, Vol 292, eds. W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[5] Xian-Mo Zhang, *Constructing Orthogonal Matrices and Some Cryptographic Techniques* , Ph.D Thesis, University of NSW, 1991.

[6] Xian-Mo Zhang, G-matrices of order 19, *Bulletin of the ICA*, 4 (1992), 95-98.