On Orthogonal Matrices with Constant Diagonal

Jennifer Seberry
Department of Applied Mathematics
University of Sydney
Sydney, Australia

and

Clement W. H. Lam*
Department of Computer Science
Concordia University
Montreal, Canada

Submitted by W. G. Bridges

ABSTRACT

In connection with the problem of finding the best projections of k-dimensional spaces embedded in n-dimensional spaces Hermann König asked: Given $m \in \mathbb{R}$ and $n \in \mathbb{N}$, are there $n \times n$ matrices $C = (c_{ij})$, $i, j = 1, \ldots, n$, such that $c_{ii} = m$ for all i, $|c_{ij}| = 1$ for $i \neq j$, and $C^2 = (m^2 + n - 1)I_n$? König was especially interested in symmetric C, and we find some families of matrices satisfying this condition. We also find some families of matrices satisfying the less restrictive condition $CC^T = (m^2 + n - 1)I_n$.

1. INTRODUCTION

In this paper we shall be interested in constructing orthogonal matrices of order n with constant diagonal m (an integer) and off diagonal entries ± 1.

For completeness we first give some definitions.

An *Hadamard matrix* H of order n has elements ± 1 and satisfies $HH^T = nI_n$. A *symmetric conference* matrix N of order $n \equiv 2 \pmod 4$ has zero diagonal and other elements ± 1 and satisfies $NN^T = (n-1)I_n$.

An *orthogonal design of order n and type* $(u_1, u_2, \ldots, u_s)$ $(u_i > 0)$ on the commuting variables $x_1, x_2, \ldots, x_s$ is an $n \times n$ matrix A with entries from

*The research of this author is supported in part by NSERC of Canada and FCAC of Quebec.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/82/050117+13$02.75

$\{0, \pm x_1, \ldots, \pm x_s\}$ such that

$$AA^T = \sum_{i=1}^{s} (u_i x_i^2) I_n.$$

A may be written in the form $A = x_1 A_1 + x_2 A_2 + \cdots + x_s A_s$ where $A_i A_i^T = u_i I_n$ and $A_i A_j^T + A_j A_i^T = 0$, $1 \leq i \neq j \leq s$. In particular an orthogonal design of order $n \equiv 0 \pmod 4$, 2, or 1 and type (n) is an Hadamard matrix, and an orthogonal design of order $n \equiv 2 \pmod 4$ and type $(n-1)$ is a symmetric conference matrix. See [1] for more details.

A *balanced incomplete block design*, or BIBD, with parameters (v, b, r, k, λ) may be defined as a $v \times b$ matrix with elements 0 or 1 where each row has r ones, each column has k ones, and the inner product of each pair of rows is λ.

2. KNOWN RESULTS FOR THE SYMMETRIC CASE

(2.1) The matrix

$$C = \begin{bmatrix} m & & -1 \\ & \ddots & \\ -1 & & m \end{bmatrix}$$

where $m = \frac{1}{2}(n-2)$ satisfies $C^2 = (m^2 + n - 1) I_n$. This gives the result for $m = \frac{1}{2}(n-2)$ and any n.

(2.2) Suppose $C_n^2 = (n-1) I_n$, where $|c_{ij}| = 1$, $c_{ij} \in \{1, -1, i, -i\}$, $i^2 = -1$, and C has zero diagonal. Then

$$C_{2n} = I_n \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + C_n \otimes \begin{bmatrix} 1 & i \\ -i & -1 \end{bmatrix}$$

is the required matrix, and

$$C_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

is a sufficient starting matrix. In fact C is a Hermitian matrix when $t > 1$. This gives the results for $m = 0$ and $n = 2^t$ for any positive integer t.

(2.3) Suppose C is a symmetric conference matrix. The orders for which they are currently known can be found by referring to [4, 6] and also by using

results on skew-Hadamard matrices. This gives the results for $m = 0$, certain $n \equiv 2 \pmod 4$, and [by using (2.2)] for $m = 0$ and $n = 2^t(p+1)$ where $p \equiv 1 \pmod 4$ is a prime power.

(2.4) Suppose C is a symmetric Hadamard matrix with constant diagonal. The orders for which they are currently known can be found by referring to [6, p. 454]. This gives the result for $m = 1$, $n = 2^{2t}$; for $m = 1$ and $n = 2^{2t}q^2$, with q a natural number, $t \geq [2\log_2(q-3)]$ (see [1, p. 304]); and for $m = 1$ and certain other n.

3. KNOWN RESULTS FOR THE GENERAL CASE

A *skew-Hadamard matrix*, $H = I + S$, has $S^T = -S$. So $C = mI + S$ of order n will satisfy $CC^T = (m^2 + n - 1)I_n$ for any m when n is the order of a skew-Hadamard matrix. The article [5] gives a recent summary of the existence question for skew-Hadamard matrices.

4. SOME NECESSARY CONDITIONS

We consider now only the case where C is a $n \times n$ matrix of the form

$$C = \begin{bmatrix} m & & \pm 1 \\ & \ddots & \\ \mp 1 & & m \end{bmatrix}$$

and

$$C^2 = (m^2 + n - 1)I_n.$$

PROPOSITION 4.1. $C = C^T$.

Proof. Considering the ith diagonal element of C^2, we have

$$\sum_{j=1}^{n} c_{ij}c_{ji} = m^2 + n - 1.$$

Now if $c_{ij} \neq c_{ji}$ for some $j \neq i$, then $c_{ij}c_{ji} = -1$ and $\Sigma c_{ij}c_{ji} \neq m^2 + n - 1$. ∎

Row 1:	m	1	1	1	...	1	1	...	1	1	...	1	1	...	1
Row 2:	1	m	x	1	...	1	1	...	1	−	...	−	−	...	−
Row 3:	1	x	m	1	...	1	−	...	−	1	...	1	−	...	−
					a			b			c			d	

FIG. 1.

PROPOSITION 4.2. *Either* $m=\frac{1}{2}(n-2)$ *or* $m\leqslant\frac{1}{6}n-1$.

Proof. Consider the first three rows. We can multiply through the rows and columns until the first row and column contain only $+1$. Then clearly the first three rows can be put in the form of Figure 1 by appropriate rearrangement of rows and columns. The entry x can be either $+1$ or -1.

The row sum and inner products of the rows give us

$$3+a+b+c-d=n, \tag{4.1}$$

$$2m+x+a+b-c-d=0, \tag{4.2}$$

$$2m+x+a-b+c-d=0, \tag{4.3}$$

$$2mx+1+a-b-c+d=0. \tag{4.4}$$

Adding, we obtain

$$4m+2x+2mx+4+4a=n. \tag{4.5}$$

Now we have two cases:

Case 1, $x=1$,
$$6m+6+4a=n,$$
$$6m+6\leqslant n,$$
$$m\leqslant\tfrac{1}{6}n-1.$$

Case 2, $x=-1$,
$$2m+2+4a=n,$$
$$m\leqslant\tfrac{1}{2}(n-2).$$

But if $m<\frac{1}{2}(n-2)$, then $a>0$ and column 4 is $(1,1,1)^T$. So we can interchange columns 3 and 4 as well as rows 3 and 4 to get case 1. Thus the inequality of case 1 applies. ∎

PROPOSITION 4.3 *If* $m = \frac{1}{2}(n-2)$ *then*

$$C = \left[\begin{array}{c|ccc} m & 1 & \cdots & 1 \\ \hline 1 & m & & -1 \\ \vdots & & \ddots & \\ 1 & -1 & & m \end{array}\right].$$

Proof. In case 2 of the previous proposition we see that if $m = \frac{1}{2}(n-2)$ then $a = 0$. From (4.1)+(4.2)−(4.3)−(4.4) with $x = -1$ we get

$$-2mx + 2 + 4b = n \quad \text{or} \quad b = 0$$

From (4.1)−(4.2)+(4.3)−(4.4) with $x = -1$ we get

$$-2mx + 2 + 4c = n \quad \text{or} \quad c = 0.$$

Then from (4.1) we get $d = n-3$.

So rows 2 and 3 are

$$\begin{array}{ccccccc} 1 & m & - & - & \cdots & - \\ 1 & - & m & - & \cdots & - \end{array}.$$

Assume that in the submatrix X, where

$$C = \left[\begin{array}{cccc} m & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & X & \\ 1 & & & \end{array}\right],$$

there exists a one in the off diagonal position, say $c_{ij} = 1$; then we interchange row 2 with row i, column 2 with column i. Then this $+1$ will go to row 2, and row 2 will have $+1$. But this is not possible if $m = \frac{1}{2}(n-2)$, and so the case $m = \frac{1}{2}(n-2)$ is completely solved. ■

PROPOSITION 4.4.

(i) *The order n is even.*
(ii) *If m is even, $n \equiv 2 \pmod 4$.*
(iii) *If m is odd, $n \equiv 0 \pmod 4$.*

Proof. This is clearly true in case 2 of Proposition 2, where $m = \frac{1}{2}(n-2)$. In case 1, $6m+6+4a = n$, and again we have the result. ■

PROPOSITION 4.5. *If $m \neq 0$, then $m^2 + n - 1$ is a square and $2\sqrt{m^2+n-1} \mid mn$.*

Proof. Let $t = m^2 + n - 1$. The eigenvalues of tI are t with multiplicity n. Because $C^2 = tI$, the eigenvalues of C are $\pm\sqrt{t}$ with total multiplicity n. Let x and y be the multiplicity of the eigenvalue $+\sqrt{t}$ and $-\sqrt{t}$ respectively. (Trace of C) $= mn = \sqrt{t}(x-y)$. Hence, if $m \neq 0$, $\sqrt{t}$ is an integer. Since $x + y = n$, we have

$$n + \frac{nm}{\sqrt{t}} = 2x.$$

Since n is even, $nm/\sqrt{t}$ is even. ■

5. A CONSTRUCTION FOR MATRICES OF REQUIRED FORM

THEOREM 5.1. *Suppose we have a $(1, -1)$ matrix S of size $2s \times r$ such that*

(i) *$SS^T = rI + Q$, where Q has zero diagonal and ± 1 elsewhere, and*
(ii) *$S^T S = 2sI_{r\times r}$.*

Further suppose there exists a $(v, b, r, k, 1)$-BIBD. Then there exists a symmetric matrix C of order $n = 2sv$ with constant diagonal $m = sk - r$, and off diagonal elements ± 1.

Proof. Let N be the incidence matrix of the $(v, b, r, k, 1)$-BIBD. Define P by replacing the ith one in each row of N with the ith column of S, and each

zero with a $2s \times 1$ column of zeros. Then

$$PP^T = rI + A,$$

where A has zero diagonal, and off diagonal elements ± 1. Further

$$P^T P = 2skI.$$

Define

$$\begin{aligned} C &= (sk - r)I - A \\ &= (sk - r)I - PP^T + rI \\ &= skI - PP^T. \end{aligned}$$

Now C is symmetric, with constant diagonal $m = sk - r$, and off diagonal elements ± 1. Also

$$\begin{aligned} C^2 &= s^2k^2I - 2skPP^T + PP^TPP^T \\ &= s^2k^2I - 2skPP^T + P(2skI)P^T \\ &= s^2k^2I. \end{aligned}$$

Hence C is the required matrix with $m = sk - r$ and $n = 2sv$. ■

REMARK. We note that from the necessary conditions for the existence of a $(v, b, r, k, 1)$-BIBD we have

$$v = r(k-1)+1,$$

and

$$b = \frac{rv}{k} = \frac{r[r(k-1)+1]}{k} \quad \text{must be an integer.}$$

COROLLARY 5.2. *There exists a matrix C with diagonal $m = sk - 1 = \frac{1}{2}n - 1$, order $n = 2sk$, and off diagonal elements ± 1.*

Proof. Of course we discussed this matrix before, but it can be formed from the theorem by choosing S to be the $2s \times 1$ matrix of ones and the trivial BIBD with parameters $r = 1$, $v = k$, and $b = 1$. ∎

A more important application of the theorem is:

THEOREM 5.3. *Suppose there exists a BIBD with parameters* $v = (4t-1)(k-1)+1$, $b = (4t-1)[(4t-1)(k-1)+1]/k$, $r = 4t-1$, k, *and* $\lambda = 1$. *If an Hadamard matrix of order* $4t$ *exists, then there exists a symmetric orthogonal matrix of order* $n = 4t[(4t-1)(k-1)+1]$ *with constant diagonal* $m = 2t(k-2)+1$ *and off diagonal elements* ± 1.

Proof. In the proof of Theorem 5.1 let S be a $4t \times (4t-1)$ matrix obtained by making the first column of an Hadamard matrix all $+1$ and then deleting that column. We then proceed as in the theorem to obtain the result. ∎

Now we know from the work of Hanani that if $k = 3$ or 5 all the BIBDs we require exist. Hence, ensuring that $(4t-1)[(4t-1)(k-1)+1]/k$ is integer for $k = 3$ or 5, and using the BIBD $(91, 195, 15, 7, 1)$ (see [2, p. 298]) we have:

COROLLARY 5.4. *Assuming that all Hadamard matrices of order* $4t$ *exist, there exists a symmetric orthogonal matrix of order* n *with constant diagonal* m *and off diagonal elements* ± 1 *for*

(a) $m = 3(2u+1)$, $n = 4(3u+1)(24u+7)$,
(b) $m = 6u+5$, $n = 12(3u+2)(8u+5)$,
(c) $m = 30u+19$, $n = 20(5u+3)(16u+9)$,
(d) $m = 5(6u+5)$, $n = 4(5u+4)(80u+61)$, *and*
(e) $m = 41$, $n = 1456$,

where u *is any nonnegative integer.*

6. CONSTRUCTION FOR NONSYMMETRIC MATRICES

Since it appears to be a difficult problem in general to construct orthogonal matrices with constant diagonal and off diagonal elements ± 1, we now

construct such matrices C, for which the symmetric condition is relaxed and which satisfy

$$CC^T = (m^2 + n - 1)I_n.$$

THEOREM 6.1. *Let $p \equiv 3 \pmod 4$ be a prime power. Suppose $n = 2^t p$ and m, nonnegative integers, are given. Then, whenever the equation $x(p+1) + y(p-3) = 2^t + 2m - p + 1$ has solutions for nonnegative integers x and y, there is an orthogonal matrix of order $2^t p$ with constant diagonal m and off diagonal elements ± 1.*

Proof. Let X be the skew symmetric $(0, 1, -1)$ matrix defined by the quadratic character for order p. Then

$$XJ = 0 \quad \text{and} \quad XX^T = pI - J.$$

Use the back diagonal matrix, R, of order p to form $Y = (X + I)R$ which satisfies

$$YJ = J, \qquad Y^T = Y, \quad \text{and} \quad YY^T = (p+1)I - J.$$

Now every orthogonal design of type $(1, x, y, z)$, $1 + x + y + z = 2^t$, exists in every order 2^t. So let $D = x_1 I + x_2 A_2 + x_3 A_3 + x_4 A_4$ be an orthogonal design of this type, and define

$$E = \big(mI_p - (J_p - I_p)\big) \otimes I + J_p \otimes A_2 + (J_p - 2I_p) \otimes A_3 + Y \otimes A_4.$$

Then E has diagonal m and other elements ± 1 and satisfies

$$\begin{aligned} EE^T &= \big\{(m+1)^2 I_p - [2(m+1) - p]J_p\big\} \otimes I + xpI_p \otimes I \\ &\quad + y\big[4I_p + (p-4)J_p\big] \otimes I + (2^t - 1 - x - y)\big[(p+1)I_p - J_p\big] \otimes I \\ &= \big[(m+1)^2 + 4y + (2^t - 1 - x - y)(p+1)\big] I_p \otimes I \\ &\quad + \big[xp + (p-4)y - 2^t + 1 + x + y - 2m - 2 + p\big] J_p \otimes I \\ &= (m^2 + 2^t p - 1) I_{2^t p}. \end{aligned}$$

Hence E is the required matrix. ∎

EXAMPLE.

(i) There is an orthogonal matrix with diagonal 7, with other elements ± 1, and of order 96. It is obtained by using $t=5$, $m=7$, $p=3$, $x=11$, $y=0$ in the theorem.

(ii) There is an orthogonal matrix with diagonal 15, with other elements ± 1, and of order 176. It is obtained by using $t=4$, $m=15$, $p=11$, $x=3$, $y=0$ in the theorem.

LEMMA 6.2. *Let $p \equiv 3 \pmod 4$ be a prime power. Suppose $n = 2^t p$ and m, nonnegative integers, are given. Then whenever $(2^t+2m+2)/(p+1)$ or $(2^t+2m-2)/(p-3)$ are integers, there is an orthogonal matrix of order n with constant diagonal m and off diagonal elements ± 1.*

Proof. Use the theorem with $y=0$ and $x=0$ respectively. ∎

THEOREM 6.3. *Suppose every orthogonal design of type $(1, a, b, \frac{1}{2}(2^t-1-a-b), \frac{1}{2}(2^t-1-a-b))$ exists in every order 2^t. Further suppose the equation $a(p+1)+b(p-3)=2^t-p+1+2m$ has solutions for $p \equiv 1 \pmod 4$, a prime power, and a, b, t, m nonnegative integers. Then there is an orthogonal matrix of order $2^t p$ with constant diagonal m and off diagonal elements ± 1.*

Proof. Let X be the symmetric $(0,1,-1)$ matrix defined by the quadratic character for order p. Then

$$XJ = 0, \qquad XX^t = pI - J.$$

Let $D = x_1 I + x_2 A_2 + x_3 A_3 + x_4 A_4 + x_5 A_5$ be an orthogonal design of the required type in order 2^t. Define

$$E = \left[mI_p - (J_p - I_p) \right] \otimes I + J_p \otimes A_2 + (J_p - 2I_p) \otimes A_3$$
$$+ (X + I_p) \otimes A_4 + (X - I_p) \otimes A_5.$$

Then E has diagonal m and other elements ± 1 and satisfies

$$\begin{aligned} EE^T &= \left\{(m+1)^2 I_p - [2(m+1)-p]J_p\right\} \otimes I + pJ_p \otimes aI \\ &\quad + \left[4I_p + (p-4)J_p\right] \otimes bI + \left[(2p+2)I_p - 2J_p\right] \otimes \tfrac{1}{2}(2^t - 1 - a - b)I \\ &= \left[(m+1)^2 + 4b + (p+1)(2^t - 1 - a - b)\right] I_p \otimes I \\ &\quad + \left[ap + bp - 4b - 2^t + 1 + a + b - 2(m+1) + p\right] J_p \otimes I \\ &= (m^2 + 2^t p - 1) I_{2^t p}, \end{aligned}$$

using $a(p+1) + b(p-3) = 2^t - p + 1 + 2m$. Hence E is the required matrix. ■

EXAMPLE. When $p = 9$, $t = 5$, $m = 17$, $a = 4$, $b = 3$, we have a matrix of order 288 with diagonal 17. Unfortunately this matrix is not symmetric.

REMARK. The orthogonal designs required in the theorem are not always known, but if $a = 0$ or $b = 0$ they are known. So we have

COROLLARY 6.4. *Let $p \equiv 1 \pmod 4$ be a prime power. Suppose the nonnegative integers t, m, and p are given. Then if one of $(2^t + 2m + 6)/(p + 1)$, $(2^t + 2m + 2)/(p + 1)$, $(2^t + 2m - 2)/(p - 3)$, or $(2^t + 2m - 6)/(p - 3)$ is an integer, there is an orthogonal matrix of order $2^t p$ with constant diagonal and off diagonal elements ± 1.*

Proof. We use the equation $a(p+1) + b(p-3) = 2^t - p + 1 + 2m$. Now all orthogonal designs of type $(1, 1, x, y, z)$, $2 + x + y + z = 2^t$, exist in every order 2^t. So $a = 0$ or $b = 0$ requires only that a design of type $(1, x, y, y)$, $1 + x + 2y = 2^t$, should exist in 2^t, and $a = 1$ or $b = 1$ requires that a design of type $(1, 1, x, y, y)$, $2 + x + 2y = 2^t$, should exist. We put the appropriate values for a and b in the equation and solve to find the stated result. ■

7. NUMERICAL RESULTS

In Table 1 we give a list of values of $n < 2000$, $m > 1$ which satisfy the necessary conditions for the existence of symmetric C satisfying $C^2 = (m^2 + n - 1)I_n$ with off diagonal entries ± 1. Those known to exist are marked *. The

TABLE 1

n	m	m^2+n-1	s	n	m	m^2+n-1	s
28	3	36	6*	876	5	900	30
64	9	144	12	924	29	1764	42
76	5	100	10	936	19	1296	36
96	7	144	12	946	12	1089	33
120	5	144	12*	976	25	1600	40*
126	10	225	15	990	10	1089	33
136	3	144	12	1000	51	3600	60
148	7	196	14	1008	17	1296	36
176	15	400	20	1030	14	1225	35
190	6	225	15	1036	27	1764	42
210	4	225	15	1084	19	1444	38
244	9	324	18	1090	44	3025	55
246	14	441	21	1128	77	7056	84
276	25	900	30	1184	39	2704	52
280	11	400	20	1190	6	1225	35
288	17	576	24	1200	49	3600	60
320	9	400	20	1216	9	1296	36
344	21	784	28	1216	33	2304	48
352	15	576	24	1216	63	5184	72
364	11	484	22	1324	21	1764	42
376	5	400	20	1326	14	1521	39
378	8	441	21	1332	55	4356	66
406	6	441	21	1344	31	2304	48
460	21	900	30	1350	26	2025	45
496	9	576	24*	1376	15	1600	40
508	13	676	26	1378	12	1521	39
528	7	576	24	1408	23	1936	44
540	19	900	30*	1446	34	2601	51
540	35	1764	42	1456	41	3136	56*
560	15	784	28	1496	21	1936	44
568	27	1296	36	1520	9	1600	40
576	55	3600	60	1540	15	1764	42*
606	22	1089	33	1540	81	8100	90
616	13	784	28	1576	45	3600	60
640	31	1600	40	1588	23	2116	46
676	15	900	30	1596	13	1764	42
730	36	2025	45	1716	7	1764	42
736	7	784	28	1806	38	3249	57
736	49	3136	56	1816	11	1936	44
780	11	900	30*	1860	65	6084	78
820	9	900	30	1870	34	3025	55
826	20	1225	35	1876	25	2500	50
846	26	1521	39	1876	55	4900	70
848	33	1936	44	1920	41	3600	60
868	17	1156	34	1926	10	2025	45
				1976	27	2704	52

necessary conditions are:

(1) n is even, $m > 1$,
(2) $2m + 2 \equiv n \pmod 4$,
(3) $m^2 + n - 1 = \text{square} = s^2$, and
(4) $nm/2s$ is an integer.

Note added in proof. The authors recently learned that the symmetric orthogonal matrices with constant diagonal as studied in part of this paper are special cases of regular two-graphs. Much more is known about these graphs, as is evident in the survey paper "Two-graphs, a second survey," by J. J. Seidel and D. E. Taylor, which appeared in *Proceedings of the International Colloquium on Algebraic Methods in Graph Theory*, Szeged, 1978.

REFERENCES

1 Anthony V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York, 1979.
2 Marshall Hall, Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.
3 Hermann König, private communication.
4 Rudolf Mathon, Symmetric conference matrices of order $pq^2 + 1$, *Canad. J. Math.* 30: 321–331 (1978).
5 Jennifer Seberry, On skew-Hadamard matrices, *Ars Combin.*, 6: 255–275 (1978).
6 Jennifer Seberry Wallis, Hadamard matrices, in *Combinatorics: Room Squares, Sum Free Sets, Hadamard Matrices* (by W. D. Wallis, Anne Penfold Street, and Jennifer Seberry Wallis), Lecture Notes in Mathematics, No. 292, Springer, New York, 1972.

Received 6 July 1981