Reprinted from JOURNAL OF COMBINATORIAL THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 19, No. 1, July 1975
Printed in Belgium

Orthogonal Designs IV: Existence Questions

ANTHONY V. GERAMITA[1]

Department of Mathematics, Queen's University, Kingston, Ontario, Canada

AND

JENNIFER SEBERRY WALLIS[2]

I.A.S., Australian National University, Canberra, Australia

Communicated by Marshall Hall, Jr.

Received October 23, 1974

INTRODUCTION

In [5] Raghavarao showed that if $n \equiv 2 \pmod 4$ and A is a $\{0, 1, -1\}$ matrix satisfying $AA^t = (n-1)I_n$, then $n - 1 = a^2 + b^2$ for a, b integers. In [4] van Lint and Seidel, giving a proof modeled on a proof of the Witt cancellation theorem, proved more generally that if n is as above and A is a rational matrix satisfying $AA^t = kI_n$ then $k = q_1^2 + q_2^2$ ($q_1, q_2 \in Q$, the rational numbers). Consequently, if k is an integer then $k = a^2 + b^2$ for two integers a and b. In [1] we showed that if, in addition, $A = -A^t$ then $k = s^2$.

Along these same lines we proved in [1] that if $n \equiv 0 \pmod 4$ and A is a rational matrix where $AA^t = kI_n$ and $A = -A^t$ then $k = q_1^2 + q_2^2 + q_3^2$ with q_1, q_2, q_3 rational and consequently if k is an integer then q_1, q_2, q_3 can be chosen as integers.

Both of these theorems had important consequences for the existence of orthogonal designs, which we defined and examined in [1].

We can now give a very simple proof of the van Lint–Seidel result, obtaining it as an immediate corollary of the Witt cancellation theorem. That such a proof might exist was a suggestion of H. J. Ryser, whose comments we gratefully acknowledge. We also prove some other theorems

[1] The work of this author was supported in part by the National Research Council of Canada under grant 8488.

[2] Written while this author was visiting the Department of Mathematics at SUNY at Buffalo.

in this same genre. The first states that if $n \equiv 2 \pmod 4$ and X is a matrix with entries in $Q(i)$ (Q = rationals, $i^2 = -1$) such that $X = -X^t$ and $XX^* = kI_n$ ($*$ denotes conjugate transpose) then $k = q_1^2 + q_2^2$ ($q_j \in Q$). As before, if $k \in Z$, the integers, then q_1 and q_2 may also be chosen in Z. The second theorem asserts that if X and Y have order $n \equiv 2 \pmod 4$ and entries in $Q(i)$ where $XX^* = I$, $YY^* = kI$, $XY^* + YX^* = 0$, and both X and Y are skew-symmetric then k is a square in Q.

These theorems affirmatively resolve questions (a), (b), and (e) of [1].

In the last part of the paper we use some recent work of Blake and Mullin on coding theory to answer part of question (*h*) in [1]. We include, in Appendix I, a tabulation of some of the results on this question.

We have raised some conjectures in this paper about the types of orthogonal designs that may exist in order $4t$, t odd. We include, in Appendix II, the status of these conjectures in order $4 \cdot 5 = 20$.

1. Orthogonal Matrices

Theorem 1 (Raghavarao–van Lint–Seidel). *Let $n \equiv 2 \pmod 4$ and let A be a matrix of order n with entries in Q satisfying $AA^t = kI_n$. Then $k = q_1^2 + q_2^2$, where $q_1, q_2 \in Q$. Moreover, if $k \in Z$ then $k = a^2 + b^2$, $a, b \in Z$.*

Proof. By the theorem of Lagrange, every positive rational number may be written as the sum of four squares of rational numbers. Since k, above, is necessarily $\geqslant 0$ we may write $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$.

Now, let

$$M = \begin{bmatrix} k_1 & k_2 & k_3 & k_4 \\ -k_2 & k_1 & -k_4 & k_3 \\ -k_3 & k_4 & k_1 & -k_2 \\ -k_4 & -k_3 & k_2 & k_1 \end{bmatrix}.$$

One easily sees that

$$MM^t = kI_4. \tag{†}$$

The matrix equation $AA^t = kI_n$ tells us that I_n is congruent to kI_n over Q while (†) shows that I_4 is congruent to kI_4 over Q. Now since $n \equiv 2$ (mod 4) we obtain, by Witt's cancellation theorem (see e.g. [8, p. 64]) that I_2 is congruent to kI_2 over Q. Thus, there is a 2×2 matrix B, with entries in Q, such that $BB^t = kI_2$ and hence $k = q_1^2 + q_2^2$ for $q_1, q_2 \in Q$. The proof is complete when we observe that if an integer is a sum of two rational squares it is also the sum of two integer squares.

THEOREM 2. *Let X be a matrix of order $n \equiv 2 \pmod 4$ with entries in the field $Q(i)$ ($i^2 = -1$). Suppose*

(i) $X = -X^t$ and
(ii) $XX^* = kI_n$.

Then $k = q_1^2 + q_2^2$, where $q_1, q_2 \in Q$. If, in addition, $k \in Z$ then q_1 and q_2 may be chosen in Z.

Proof. Our proof closely parallels the proof of our Theorem 1 that was given by van Lint and Seidel in [4]. We write $n = 2s$ and we proceed by induction on odd s.

We first note that the assertion is trivially true for $s = 1$, for then

$$X = \begin{bmatrix} 0 & z \\ -z & 0 \end{bmatrix}, \qquad z \in Q(i)$$

and $k = z\bar{z}$ ("—" denoting the usual complex conjugation) which is a sum of two squares.

To continue the proof, we need the following lemma from [1, Corollary 2 of lemma to Proposition 25].

LEMMA. *Let M and A be skew—symmetric matrices of order n and $\mathscr{D}$ be the set of diagonal matrices of order n all of whose diagonal entries are in $\{1, -1\}$. Then if M is nonsingular there is a $D \in \mathscr{D}$ such that $DMD + A$ is nonsingular.*

Now, we write X (of order $2s$, s odd, $s > 1$) as

$$X = \begin{bmatrix} A & B \\ C & E \end{bmatrix},$$

where A is a 4×4 matrix. Now, write $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$, $k_i \in Q$, and form the 4×4 matrix

$$N = \begin{bmatrix} k_1 & k_2 & k_3 & k_4 \\ -k_2 & k_1 & -k_4 & k_3 \\ -k_3 & k_4 & k_1 & -k_2 \\ -k_4 & -k_3 & k_2 & k_1 \end{bmatrix}$$

and observe that N may be identified with the 2×2 matrix

$$\mathbf{N} = \begin{bmatrix} k_1 + k_2 i & k_3 + k_4 i \\ -k_3 + k_4 i & k_1 - k_2 i \end{bmatrix}.$$

Since $NN^t = kI_4$ we obtain $\mathbf{N}\mathbf{N}^* = kI_2$. Form

$$M = \begin{bmatrix} 0 & \mathbf{N} \\ -\mathbf{N}^t & 0 \end{bmatrix},$$

and observe that

(i) $MM^* = kI_4$ and
(ii) $M = -M^t$.

We now use the lemma to deduce that there is a 4×4 diagonal matrix D with diagonal entries $\{\pm 1\}$ such that $A + DMD$ is invertible. (For convenience we will still denote DMD by M and observe that DMD satisfies (i) and (ii) as M did.)

Now form the matrix

$$P = E - C(A + M)^{-1} B.$$

Claim. P is a matrix of order $2(s - 2)$ with entries in $Q(i)$ and satisfying

(i) $P^t = -P$ and
(ii) $PP^* = kI_{2(s-2)}$.

Proof. Clearly P has order and entries as stated and since $A^t = -A$, $B^t = -C$, $C^t = -B$, and $E^t = -E$ we easily obtain (i).

To prove (ii) we consider the product of four matrices, $STUV$ (set $A + M = L$),

$$[-B^*(L^*)^{-1} \mid I_{2(s-2)}] \begin{bmatrix} A^* & C^* \\ B^* & E^* \end{bmatrix} \begin{bmatrix} A & B \\ C & E \end{bmatrix} \begin{bmatrix} -L^{-1}B \\ \hline I_{2(s-2)} \end{bmatrix},$$

by first calculating this product as $S(TU)V$ and then as $(ST)(UV)$.

Thus, the induction hypothesis may be used on P to complete the proof of the theorem.

There is one more theorem of this type we would like to prove. Its importance will be clear in the next section when we discuss the applications of these results to orthogonal designs.

THEOREM 3. *Let X and Y be matrices of order $n \equiv 2 \pmod 4$ and with entries in $Q(i)$. Suppose*

(1) $XX^* = I$, $YY^* = qI$
(2) $XY^* + YX^* = 0$
(3) $X = -X^t$, $Y = -Y^t$;

then $q = r^2$ for $r \in Q$.

Proof. Let $a = \det X$, $b = \det Y$. Then (1) gives $\| a \|^2 = 1$ and $\| b \|^2 = q^n$. Rewrite (2) as $XY^* = -YX^*$ and observe that, since n is even, $a\bar{b} = b\bar{a} = \overline{(a\bar{b})}$, i.e. $a\bar{b} \in Q$. Thus $a = sb$ for some $s \in Q$. Taking norms we have $\| a \|^2 = s^2 \cdot \| b \|^2$ and so $1 = s^2 \cdot q^n$ and since $n = 2l$, l odd, $1 = (| s | q^l)^2$ and so $| s | = 1/q^l$. Consequently $q^l a = \pm b$.

From (3) we have $a = z_1^2$, $b = z_2^2$, since for skew-symmetric matrices $\det = (\mathrm{Pf})^2$ (Pf = Pfaffian), where $z_1, z_2 \in Q(i)$. Thus $q^l = \pm z_2^2/z_1^2 = \pm(z_2/z_1)^2$.

A simple calculation shows that if the square of $z \in Q(i)$ is in Q then z is pure real or pure imaginary. In either case, $q^l = p^2$ for some $p \in Q$. But, since l is odd, q must already be a square in Q.

2. Applications to Orthogonal Designs

We recall a few definitions and theorems which may all be found in [1].

Definition. An orthogonal design of order n and type $(s_1, ..., s_l)$ on the commuting variables $x_1, ..., x_l$ is an $n \times n$ matrix, A, with entries chosen from $\{0, \pm x_1, \pm x_2, ..., \pm x_l\}$ such that

$$AA^t = (s_1 x_1^2 + \cdots + s_l x_l^2) I_n .$$

Alternatively, the rows (and hence columns) of A are formally orthogonal and every row (column) contains s_i entries of the type $\pm x_i$.

If A is as above, we may write

$$A = x_1 A_1 + x_2 A_2 + \cdots + x_l A_l ,$$

where

(i) $A_i A_i^t = s_i I_n$;
(ii) $A_i A_j^t + A_j A_i^t = 0$, $1 \leqslant i \neq j \leqslant l$;
(iii) the A_i are $\{0, 1, -1\}$ matrices.

We have shown [1] that if $n \equiv 2 \pmod 4$ then $l \leqslant 2$ and if $n \equiv 0 \pmod 4$ then $l \leqslant 4$.

Theorem 4 [1]. *Let $n \equiv 4 \pmod 8$ and let X be an orthogonal design of order n and type (s_1, s_2). Then $s_1 \cdot s_2$ must be a sum of $\leqslant$ three squares.*

Remark. In [1] we showed that if $n = 4 \cdot 3$ then Theorem 4 gave necessary and sufficient conditions for the existence of a design (s_1, s_2) in order 12. We conjecture that Theorem 4 always gives necessary and sufficient conditions for the existence of orthogonal designs on two variables in order $n \equiv 4 \pmod 8$.

Let X be an orthogonal design of type $(1, 1, k)$ in order n and write $X = A_1x_1 + A_2x_2 + A_3x_3$. If

$$P = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and

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

and $n = 4s$, then, with no loss of generality we may assume

$$A_1 = \bigoplus_{2s} P, \qquad A_2 = \bigoplus_{2s} H.$$

The patient reader will then discover that if A_3 is partitioned into 2×2 blocks, denoted a_{ij}, $1 \leqslant i, j \leqslant 2s$, then, since $A_1A_3^t + A_3A_1^t = 0$ and $A_2A_3^t + A_3A_2^t = 0$ we have

$$a_{ii} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \qquad a_{ij} = \begin{bmatrix} u & v \\ -v & u \end{bmatrix}, \qquad a_{ji} = \begin{bmatrix} -u & -v \\ v & -u \end{bmatrix}$$

(for $i \neq j$). Thus, A_3 may be considered as a matrix, which we will denote $\mathbf{A}_3$, of order $2s$ with entries in $Q(i)$, $i^2 = -1$, by replacing the block

$$\begin{bmatrix} u & v \\ -v & u \end{bmatrix}$$

by $[u + iv]$. We observe that $\mathbf{A}_3^t = -\mathbf{A}_3$ and since $A_3A_3^t = kI_n$ then $\mathbf{A}_3\mathbf{A}_3^* = kI_{2s}$. We may now state

THEOREM 5. *Let $n \equiv 4 \pmod 8$ and let X be an orthogonal design of type $(1, 1, k)$ in order n. Then $k = a^2 + b^2$.*

Proof. From the discussion above we see that the existence of such a design implies the existence of a matrix Y of order $n/2 = m \equiv 2 \pmod 4$ with entries in $Q(i)$ satisfying $Y^t = -Y$ and $YY^* = kI_m$. Thus, from Theorem 2 we conclude that k is a sum of $\leqslant 2$ squares.

We would now like to generalize Theorem 5. We need an easy lemma about rational matrices for which we have been unable to find a reference. We include a proof here for completeness.

LEMMA. *Let A be a rational matrix of order $n = 2l$ satisfying*

(i) $AA^t = I$,
(ii) $A = -A^t$.

Then there is an orthogonal matrix P (i.e. $PP^t = I$) *such that*

$$PAP^t = \bigoplus_l \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

(Note: This fact is well known for real matrices and follows immediately from the Gram–Schmidt orthonormalization theorem, which, unfortunately, is not avaialable for the rational field.)

Proof. We write $\langle , \rangle$ to denote the standard inner product on Q^n. Let $\mathbf{v}$ be any vector of unit length in Q^n and let V be the subspace spanned by $\mathbf{v}$ and $A\mathbf{v}$. Note that this subspace is invariant under A. Clearly Av has unit length also and $\langle \mathbf{v}, A\mathbf{v} \rangle = 0$. By Witt's theorem $A\mathbf{v} = v_1$ and $\mathbf{v} = v_2$ can be extended to an ortho*normal* basis for Q^n. We use this basis to form the rows of a matrix P. Then, with respect to this basis, the matrix for A is

$$\left[\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & \bigcirc \\ \hline \multicolumn{2}{c|}{\bigcirc} & * \end{array}\right]$$

and the proof proceeds by induction on l.

THEOREM 6. *Let X be an orthogonal design of type (a, a, b) in order n, $n \equiv 4 \pmod 8$. Then $b/a = q_1^2 + q_2^2$ for $q_1, q_2 \in Q$.*

Proof. Write $X = A_1x_1 + A_2x_2 + A_3x_3$, then $A_1A_1^t = A_2A_2^t = aI_n$, $A_3A_3^t = bI_n$, and $A_iA_j^t + A_jA_i^t = 0$ for $i \neq j$, $1 \leqslant i, j \leqslant 3$. Multiply the family $\{A_1, A_2, A_3\}$ on the right by $(1/a)\, A_1^t$ to obtain the family $\{I, B, C\}$. We observe that $B^t = -B$, $BB^t = I$, $C^t = -C$, $CC^t = (b/a)\, I$, and

$$BC^t + CB^t = 0.$$

By the lemma, there is an orthogonal matrix Q such that

$$QBQ^t = \bigoplus_{n/2} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = L,$$

and hence, if we multiply the family $\{I, B, C\}$ on the left by Q and on the right by Q^t we obtain a family

$$\left\{ I, \bigoplus_{n/2} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, D \right\} = \{I, L, D\},$$

where $DD^t = (b/a) I$, $D = -D^t$, and $DL^t + LD^t = 0$. Let

$$P = \bigoplus_{n/2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and multiply the family $\{I, L, D\}$ on the left by P. If

$$H = \bigoplus_{n/2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

then we obtain the family $\{P, H, PD = E\}$. Now the remarks preceding Theorem 5 are in force since $PE^t + EP^t = 0$ and $HE^t + EH^t = 0$. We may thus use the proof of Theorem 5 to conclude that since $EE^t = (b/a) I$, then $b/a = q_1^2 + q_2^2$ for $q_1, q_2 \in Q$.

Now, let X be an orthogonal design of type (a, a, a, b) in order $4s$, s odd, and write

$$X = A_1x_1 + A_2x_2 + A_3x_3 + A_4x_4 .$$

We may proceed as in the proof of Theorem 6 to change the family of matrices A_1, A_2, A_3, A_4 to

$$\left\{P = \bigoplus_{2s} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \bigoplus_{2s} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, B_1, B_2\right\}.$$

where for M, N in this latter family $MN^t + NM^t = 0$ and $B_1B_1^t = I$, $B_2B_2^t = (b/a) I$. As we have seen in the proof of Theorem 6, this then gives two complex matrices $\mathbf{B}_1, \mathbf{B}_2$ of order $2s$, which are skew-symmetric and further $\mathbf{B}_1\mathbf{B}_1^* = I$, $\mathbf{B}_2\mathbf{B}_2^* = (b/a) I$, and $\mathbf{B}_1\mathbf{B}_2^* + \mathbf{B}_2\mathbf{B}_1^* = 0$. We can now use Theorem 3 to conclude that b/a is a square. These remarks then constitute a proof of

THEOREM 7. *Let $n \equiv 4 \pmod 8$ and let X be an orthogonal design of order n and type (a, a, a, b), then b/a is a square.*

3. Some Applications and Conjectures

ORDER 12. In [1] we constructed many orthogonal designs in order 12. We also were unable to construct some whose existence was not denied by any of the theorems in that paper. For the reader's convenience we will recall that list.

I.	1. (1, 1, 1, 2)	6. (1, 3, 3, 3)
	2. (1, 1, 1, 3)	7. (2, 2, 2, 3)
	3. (1, 1, 1, 8)	8. (2, 2, 2, 4)
	4. (1, 1, 2, 3)	9. (2, 2, 2, 6)
	5. (1, 2, 2, 2)	
II.	1. (1, 1, 3)	4. (2, 2, 6)
	2. (1, 3, 3)	5. (3, 3, 4)
	3. (2, 2, 3)	

Theorem 7 now shows that I (1, 2, 3, 5, 6, 7, 8, 9) do not exist and Theorem 6 shows that II (1, 2, 3, 4, 5) (and as a consequence I (4)) do not exist.

Thus, the designs in order 12 that were constructed in [1] are the *only* orthogonal designs in order 12. We note also that all the orthogonal designs in order 12 were constructed using the Goethals–Seidel array (see [1, Theorem 13]), including the important Baumert–Hall array of order 12.

In view of our experience in order 12 and some calculations that we will exhibit in Appendix II we make the following conjectures concerning the existence of orthogonal designs in order $n = 4t$, t odd.

Conjecture I. A necessary and sufficient condition that there exist a design of type (a, a, b) in order n is that b/a be a sum of $\leqslant$ two rational squares.

Conjecture II. A necessary and sufficient condition that there exist a design of type (a, a, a, b) in order n is that b/a be a rational square.

Conjecture III. A necessary and sufficient condition that there exist a design of type (a, b) in order n is that b/a be a sum of $\leqslant$ three rational squares.

The "necessary" parts of conjectures I, II, and III have all been verified (Theorems 6, 7, and 4 of this paper).

The conjectures are all valid for $n = 4, 12$. We shall report on our investigations for $n = 20$ in Appendix II.

Our feeling is that Conjectures I–III in fact tell the whole story about orthogonal designs in order $n = 4t$, t odd, in the sense that any design not excluded by these conjectures from existing does in fact exist. For example, at first glance our conjectures say nothing about whether a design of type (1, 2, 2, 10) should exist in order 20. But, if it did there would be a design of type (2, 2, 11) in order 20, which is precluded by Theorem 6. On the other hand, a design of type (1, 2, 3, 9) in order 20 is not excluded by any of the conjectures, nor are any of the orthogonal designs in order 20 that one can obtain from it (like the designs (1, 9), (6, 9), (3, 3, 9), etc.) and so we conjecture that this design exists. Perhaps these remarks really constitute Conjecture 0!

4. Weighing Matrices of Odd Order

Definition. A weighing matrix of weight k and order n is an $n \times n$ $\{0, 1, -1\}$ matrix A satisfying

$$AA^t = kI_n .$$

(We usually denote such a matrix by $W(n, k)$).

In [1] we showed

Proposition 8. *Let n be odd. If a $W(n, k)$ exists then*

(i) $k = a^2$ *for some* $a \in Z$,
(ii) $(n - k)^2 - (n - k) + 2 > n$.

(We have shown that these conditions are not sufficiently sharp to give sufficient conditions for a $W(n, k)$ to exist, by showing that a $W(9, 4)$ does not exist.)

In [1] we showed that a $W(n, 4)$ exists for every $n \geqslant 10$ and a $W(n, 9)$ exists for every $n \geqslant 31$. (In the latter case we actually had a $W(n, 9)$ for all $n \geqslant 22$ except for $n = 31$.) In [1] we conjectured that if $k = a^2$ then there is always an m (depending on k) such that for every $n \geqslant m$ a $W(n, k)$ exists. We can now solve that problem. Our results are based on some recent work of I. Blake and R. C. Mullin.

Lemma 9. *If a and b are two relatively prime integers then every integer* $\geqslant (a - 1)(b - 1)$ *is a positive linear combination of "a" and "b".*

Proof. The proof is left as an exercise. We have been unable to locate any analagous bound for a collection of t integers that are relatively prime. Such a formula would be very useful.

Theorem 10 (Blake–Mullin). *Let p be an odd prime and let t be even. If* $n = (p^{t+1} - 1)/(p - 1)$ *then there is a* $W(n, p^t)$.

(Note that t even $\Rightarrow n$ odd.)

Lemma 11. *Let* p^t *be an odd prime power. Then there is a* $W(p^t + 1, p^t)$.

Proof. If $p^t \equiv 1 \pmod 4$ then a $W(p^t + 1, p^t)$ is called a conference matrix and if $p^t \equiv 3 \pmod 4$ the matrix exists because there is a skew-Hadamard matrix of order $p^t + 1$. (See [7, pp. 292, 313] for details on this.)

LEMMA 12. *Let p be an odd prime and let t be even. There exists an integer m such that for all $n \geqslant m$ a $W(n, p^t)$ exists.*

Proof. In view of Lemma 9 it is sufficient to show that for t even,

$$a = (p^{t+1} - 1)/(p - 1) \quad \text{and} \quad b = p^t + 1$$

are relatively prime. Note that

$$(p - 1)(p^{t+1} - 1)/(p - 1) - p(p^t + 1) = -(p + 1);$$

thus the GCD (a, b) divides $p + 1$. Let $x = \text{GCD}\,(a, b)$, then $p + 1 = sx$.
Now

$$\begin{aligned} a &= 1 + p + p^2 + \cdots + p^t \\ &= (1 + p) + p^2(1 + p) + p^4(1 + p) + \cdots + p^{t-2}(1 + p) + p^t \\ &= (1 + p)[1 + p^2 + p^4 + \cdots + p^{t-2}] + p^t, \end{aligned}$$

since $x \mid a$ and $x \mid (1 + p)[1 + p^2 + \cdots + p^{t-2}] \Rightarrow x \mid p^t$.
Thus $x = p^\alpha$. But $p^\alpha \mid p^t + 1 \Leftrightarrow \alpha = 0$ and so $x = 1$.

THEOREM 14. *Let $k = a^2$ for some integer a. Then there is an integer N (depending on a) such that for all $n \geqslant N$, a $W(n, k)$ exists.*

Proof. By Lemma 12 we have the theorem for k an even prime power. Thus, it will be sufficient to prove that if the theorem is true for $k = r^2$ and true for $k = s^2$ it is true for $k = (rs)^2$.

Assume the theorem is true for $k = r^2$, i.e. there is an integer N_r such that for all $n \geqslant N_r$, a $W(n, r^2)$ exists. Let P_r and Q_r be two distinct primes $\geqslant N_r$. Similarly, let P_s and Q_s be two distinct primes $\geqslant N_s$ (different from P_r, Q_r).

Now $W(P_r, r^2) \otimes W(Q_s, s^2) = W(P_rQ_s, r^2s^2)$ and

$$W(Q_r, r^2) \otimes W(P_s, s^2) = W(Q_rP_s, r^2s^2).$$

Thus, there is a $W(m, (rs)^2)$ for $m = P_rQ_s$ and for $m = Q_rP_s$. Since GCD $(P_rQ_s, Q_rP_s) = 1$ the theorem follows from Lemma 9.

APPENDIX I: SOME NUMERICAL RESULTS FOR WEIGHING MATRICES OF ODD ORDER

We have already mentioned some results about weighing matrices of weight 4 and weight 9. The computations on weight 4 are in [1], while those on weight 9 may be deduced from [2] and [3].

From [2] we have a $W(2m, 16)$ for every $m \geq 8$. From the known $W(7, 4)$ we obtain a $W(49, 16)$.

From Lemma 11 we obtain a $W(26, 25)$. A $W(m, 25)$ is exhibited in [3] for $m \in \{28, 32, 36, 40, 44, 48, 52\}$. Theorem 10 gives a $W(31, 25)$.

From the $W(13, 9)$, $W(6, 4)$, and $W(7, 4)$ given in [1] we obtain a $W(78, 36)$ and a $W(91, 36)$. In [3] we have a $W(m, 36)$ for $m \in \{36, 40, 44, 48, 52, 56, 60, 64, 72\}$. The following two sequences of length 37 may be used to generate circulant matrices A and B which may then be used in

$$\begin{bmatrix} A & B \\ -B & A^t \end{bmatrix}$$

to give a $W(74, 36)$.

11– –0–0–11010011010100–101000–0100000

0000–0100010– –00–0–01–001011–0–011–10.

Also Theorem 10 gives a $W(57, 49)$. In [3] $W(m, 49)$'s are exhibited for $m \in \{56, 60, 64, 72, 80, 96\}$. Lemma 11 gives a $W(50, 49)$.

These remarks may be used to prove the following proposition.

PROPOSITION 15. *There exists a $W(m, k)$, where k is the indicated integer square for every $m \geq n$ as shown*:

(i) $k = 4$, $n = 4$ (except $m = 5,9$ which do not exist);
(ii) $k = 9$, $n = 22$ (*except possibly $m = 31$ which is undecided*);
(iii) $k = 16$, $n = 64$;
(iv) $k = 25$, $n = 82$.

It is perhaps worth mentioning that the existence of a $W(m, k)$ is undecided for the following values of m and k.

$k = 9$, $m = 15, 17, 18, 19, 21, 31$;

$k = 16$, $m = 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 51, 53, 55, 57, 59, 61, 63$.

The situation about weighing matrices of odd order is thus in a very unsatisfactory state and we can offer no conjectures at this time. It is clear that this area merits a more comprehensive investigation.

Appendix II

In this appendix we would like to report on our investigations concerning Conjectures I, II, and III of Section 3 for order 20. Theorems 4, 5, 6, and 7 eliminate many tuples as the types of orthogonal designs in order 20. The designs not eliminated are given in Table I. A check (√) next to the design indicates that we have constructed it.

The designs we have checked have all come from the Goethal's-Seidel construction. The idea is to find four circulant matrices, A_1, A_2, A_3, A_4, such that

$$\sum_{i=1}^{4} A_i A_i^t = f I_n ,$$

where

$$f = s_1 x_1^2 + s_2 x_2^2 + s_3 x_3^2 + s_4 x_4^2,$$

to obtain an orthogonal design of type (s_1, s_2, s_3, s_4). (See [1, Theorem 13] for details.) In Table II we list the first rows of the circulants we used to construct the designs in question.

TABLE I

A.		
(1, 1, 1, 1) √	(1, 1, 9, 9) √	(2, 2, 2, 8) √
(1, 1, 1, 4) √	(1, 2, 2, 4) √	(2, 2, 4, 4) √
(1, 1, 1, 9) √	(1, 2, 2, 8)	(2, 2, 4, 9) √
(1, 1, 1, 16)	(1, 2, 2, 9)	(2, 2, 5, 5)
(1, 1, 2, 2) √	(1, 2, 3, 6) √	(2, 2, 8, 8) √
(1, 1, 2, 8) √	(1, 2, 4, 8) √	(2, 3, 4, 6) √
(1, 1, 2, 16)	(1, 2, 6, 11)	(2, 3, 6, 9) √
(1, 1, 4, 4) √	(1, 2, 8, 9)	(2, 3, 7, 8)
(1, 1, 4, 9) √	(1, 3, 6, 8)	(2, 4, 4, 8) √
(1, 1, 5, 5) √	(1, 4, 4, 4) √	(2, 5, 5, 8) √
(1, 1, 5, 8)	(1, 4, 4, 9)	(3, 3, 3, 3) √
(1, 1, 5, 13)	(1, 4, 5, 5)	(3, 3, 6, 6)
(1, 1, 8, 8) √	(1, 5, 5, 8)	(4, 4, 4, 4) √
(1, 1, 8, 9)	(1, 5, 5, 9)	(4, 4, 5, 5) √
(1, 1, 8, 10)	(2, 2, 2, 2) √	(5, 5, 5, 5) √

Table continued

TABLE I (*continued*)

D.

(1, 1, 1) √	(1, 5, 5) √	(2, 4, 11) √
(1, 1, 2) √	(1, 5, 6) √	(2, 4, 12) √
(1, 1, 4) √	(1, 5, 8)	(2, 5, 5) √
(1, 1, 5) √	(1, 5, 9) √	(2, 5, 6)
(1, 1, 8) √	(1, 5, 13)	(2, 5, 7)
(1, 1, 9) √	(1, 5, 14) √	(2, 5, 8) √
(1, 1, 10) √	(1, 6, 8) √	(2, 5, 13) √
(1, 1, 13) √	(1, 6, 11) √	(2, 6, 7) √
(1, 1, 16) √	(1, 6, 12)	(2, 6, 9) √
(1, 1, 17)	(1, 6, 13)	(2, 6, 11)
(1, 1, 18) √	(1, 8, 8) √	(2, 6, 12) √
(1, 2, 2) √	(1, 8, 9) √	(2, 7, 8)
(1, 2, 3) √	(1, 8, 10)	(2, 7, 10)
(1, 2, 4) √	(1, 8, 11) √	(2, 7, 11)
(1, 2, 6) √	(1, 9, 9) √	(2, 8, 8) √
(1, 2, 8) √	(1, 9, 10) √	(2, 8, 9)
(1, 2, 9) √	(2, 2, 2) √	(2, 8, 10) √
(1, 2, 10)	(2, 2, 4) √	(2, 9, 9) √
(1, 2, 11) √	(2, 2, 5) √	(3, 3, 3) √
(1, 2, 12) √	(2, 2, 8) √	(3, 3, 6) √
(1, 2, 16)	(2, 2, 9) √	(3, 3, 12)
(1, 2, 17) √	(2, 2, 10) √	(3, 4, 6) √
(1, 3, 6) √	(2, 2, 13) √	(3, 4, 8) √
(1, 3, 8) √	(2, 2, 16) √	(3, 4, 10)
(1, 3, 9)	(2, 3, 4) √	(3, 4, 11)
(1, 3, 10)	(2, 3, 6) √	(3, 6, 6) √
(1, 3, 11)	(2, 3, 7) √	(3, 6, 8)
(1, 3, 14)	(2, 3, 8)	(3, 6, 9) √
(1, 3, 16)	(2, 3, 9) √	(3, 6, 11) √
(1, 4, 4) √	(2, 3, 10) √	(3, 7, 8)
(1, 4, 5) √	(2, 3, 13)	(3, 7, 10)
(1, 4, 6)	(2, 3, 15) √	(3, 8, 9) √
(1, 4, 8) √	(2, 4, 4) √	(4, 4, 4) √
(1, 4, 9) √	(2, 4, 6) √	(4, 4, 5) √
(1, 4, 10) √	(2, 4, 8) √	(4, 4, 8) √
(1, 4, 13)	(2, 4, 9) √	(4, 4, 9) √

Table continued

TABLE I (*continued*)

D. (*continued*)		
(4, 4, 10) √	(4, 8, 8) √	(5, 6, 7)
(4, 5, 5) √	(5, 5, 5) √	(5, 6, 8)
(4, 5, 6) √	(5, 5, 8) √	(5, 6, 9) √
(4, 5, 9) √	(5, 5, 9)	(5, 7, 8) √
(4, 6, 8) √	(5, 5, 10) √	(6, 6, 6) √

E.		
(1, 1) √	(2, 16) √	(5, 8) √
(1, 2) √	(2, 17) √	(5, 9) √
(1, 3) √	(2, 18) √	(5, 10) √
(1, 4) √	(3, 3) √	(5, 13) √
(1, 5) √	(3, 4) √	(5, 14) √
(1, 6) √	(3, 6) √	(5, 15) √
(1, 8) √	(3, 7) √	(6, 6) √
(1, 9) √	(3, 8) √	(6, 7) √
(1, 10) √	(3, 9) √	(6, 8) √
(1, 11) √	(3, 10) √	(6, 9) √
(1, 12) √	(3, 11) √	(6, 11) √
(1, 13) √	(3, 12) √	(6, 12) √
(1, 14) √	(3, 14) √	(6, 13)
(1, 16) √	(3, 15) √	(6, 14) √
(1, 17) √	(3, 16)	(7, 7) √
(1, 18) √	(3, 17) √	(7, 8) √
(1, 19) √	(4, 4) √	(7, 10)
(2, 2) √	(4, 5) √	(7, 11) √
(2, 3) √	(4, 6) √	(7, 12)
(2, 4) √	(4, 8) √	(7, 13) √
(2, 5) √	(4, 9) √	(8, 8) √
(2, 6) √	(4, 10) √	(8, 9) √
(2, 7) √	(4, 11) √	(8, 10) √
(2, 8) √	(4, 12) √	(8, 11) √
(2, 9) √	(4, 13) √	(8, 12) √
(2, 10) √	(4, 14) √	(9, 9) √
(2, 11) √	(4, 16) √	(9, 10) √
(2, 12) √	(5, 5) √	(9, 11) √
(2, 13) √	(5, 6) √	(10, 10) √
(2, 15) √	(5, 7) √	

TABLE II

Design	A_1					A_2					A_3					A_4				
(1, 1, 1, 1)	x_1	0	0	0	0	x_2	0	0	0	0	x_3	0	0	0	0	x_4	0	0	0	0
(1, 1, 1, 4)	x_1	0	0	0	0	x_2	0	0	0	0	x_3	0	x_4	$-x_4$	0	0	0	x_4	x_4	0
(1, 1, 1, 9)	x_1	0	x_4	$-x_4$	0	x_2	0	x_4	$-x_4$	0	x_3	$-x_4$	0	0	x_4	x_4	x_4	x_4	0	0
(1, 1, 2, 2)	x_1	0	0	0	0	x_2	0	0	0	0	x_3	x_4	0	0	0	x_4	$-x_3$	0	0	0
(1, 1, 2, 8)	x_1	0	x_4	$-x_4$	0	x_2	0	x_4	$-x_4$	0	x_3	0	x_4	x_4	0	$-x_3$	0	x_4	x_4	0
(1, 1, 4, 4)	x_1	0	x_3	$-x_3$	0	0	0	x_3	x_3	0	x_2	0	x_4	$-x_4$	0	0	0	x_4	x_4	0
(1, 1, 4, 9)	x_1	0	x_4	$-x_4$	0	x_2	0	x_4	$-x_4$	0	0	x_4	x_3	x_3	$-x_4$	x_4	x_4	x_3	$-x_3$	x_4
(1, 1, 5, 5)	x_1	0	x_3	$-x_3$	0	x_2	0	x_4	$-x_4$	0	x_3	0	x_4	x_4	0	$-x_4$	0	x_3	x_3	0
(1, 1, 8, 8)	x_1	x_3	x_4	$-x_4$	$-x_3$	x_2	x_3	$-x_4$	x_4	$-x_3$	0	x_3	x_4	x_4	x_3	0	x_3	$-x_4$	$-x_4$	x_3
(1, 1, 9, 9)	x_1	x_3	x_4	$-x_4$	$-x_3$	x_2	x_4	$-x_3$	x_3	$-x_4$	$-x_3$	x_3	x_3	x_3	x_3	$-x_4$	x_4	x_4	x_4	x_4
(1, 2, 2, 4)	x_1	0	x_4	$-x_4$	0	0	0	x_4	x_4	0	x_2	x_3	0	0	0	x_3	$-x_2$	0	0	0
(1, 2, 3, 6)	x_1	0	x_4	$-x_4$	0	x_2	x_3	0	x_4	0	x_2	$-x_3$	0	$-x_4$	0	x_3	0	$-x_4$	$-x_4$	0
(1, 2, 4, 8)	x_1	0	x_4	$-x_4$	0	x_2	x_3	x_4	x_4	$-x_3$	x_2	0	$-x_4$	$-x_4$	0	x_4	$-x_4$	x_3	0	x_3
(1, 4, 4, 4)	x_1	0	x_2	$-x_2$	0	0	0	x_2	x_2	0	0	x_3	x_4	$-x_4$	x_3	0	x_3	x_4	x_4	$-x_3$
(2, 2, 2, 2)	x_1	x_2	0	0	0	x_2	$-x_1$	0	0	0	x_3	x_4	0	0	0	x_4	$-x_3$	0	0	0
(2, 2, 2, 8)	x_1	x_4	x_2	$-x_4$	0	x_1	$-x_4$	$-x_2$	x_4	0	x_3	0	x_4	0	x_4	x_3	0	$-x_4$	0	$-x_4$
(2, 2, 4, 4)	x_1	x_2	0	0	0	x_2	$-x_1$	0	0	0	0	x_3	x_4	$-x_4$	x_3	0	x_3	x_4	x_4	$-x_3$
(2, 2, 4, 9)	x_1	x_2	x_4	$-x_4$	0	x_1	$-x_2$	x_4	$-x_4$	0	0	x_4	x_3	x_3	$-x_4$	x_4	x_4	x_3	$-x_3$	x_4

Table continued

TABLE II (*continued*)

Design	A_1					A_2					A_3					A_4				
(2, 2, 8, 8)	x_1	x_4	x_3	x_4	$-x_3$	x_1	$-x_4$	$-x_3$	$-x_4$	x_3	x_2	x_3	$-x_4$	x_3	x_4	x_2	$-x_3$	x_4	$-x_3$	$-x_4$
(2, 3, 4, 6)	x_2	x_4	x_1	0	0	x_2	x_4	$-x_1$	0	0	$-x_2$	x_4	x_3	$-x_3$	x_4	0	x_4	x_3	x_3	$-x_4$
(2, 3, 6, 9)	x_2	x_4	x_3	x_1	$-x_4$	x_1	x_4	$-x_4$	$-x_2$	$-x_3$	$-x_2$	x_4	$-x_4$	x_3	x_3	x_4	x_4	$-x_3$	x_3	x_4
(2, 4, 4, 8)	x_3	0	x_2	x_4	x_4	x_3	0	x_2	$-x_4$	$-x_4$	x_2	x_1	$-x_3$	x_4	$-x_4$	x_2	$-x_1$	$-x_3$	$-x_4$	x_4
(2, 5, 5, 8)	x_3	x_2	x_4	$-x_4$	x_2	x_1	x_3	x_4	x_4	$-x_3$	$-x_1$	x_2	x_4	x_4	$-x_2$	$-x_2$	x_3	x_4	$-x_4$	x_3
(3, 3, 3, 3)	x_1	x_2	x_3	0	0	x_1	$-x_2$	0	x_4	0	x_1	0	$-x_3$	$-x_4$	0	x_2	$-x_3$	x_4	0	0
(4, 4, 4, 4)	0	x_1	x_2	$-x_2$	x_1	0	x_1	x_2	x_2	$-x_1$	0	x_3	x_4	$-x_4$	x_3	0	x_3	x_4	x_4	$-x_3$
(4, 4, 5, 5)	x_4	x_3	x_1	$-x_1$	x_3	0	x_4	x_1	x_1	$-x_4$	0	x_3	x_2	x_2	$-x_3$	$-x_3$	x_4	x_2	$-x_2$	x_4
(5, 5, 5, 5)	x_1	x_2	x_2	x_4	$-x_4$	$-x_2$	x_1	x_1	x_3	$-x_3$	x_4	x_3	x_3	$-x_1$	x_1	$-x_3$	x_4	x_4	$-x_2$	x_2
(1, 1, 13)	x_1	x_3	$-x_3$	x_3	$-x_3$	0	x_3	$-x_3$	$-x_3$	$-x_3$	x_2	x_3	0	0	$-x_3$	0	x_3	x_3	x_3	0
(1, 2, 17)	x_1	x_3	$-x_3$	x_3	$-x_3$	x_2	x_3	$-x_3$	$-x_3$	$-x_3$	x_2	$-x_3$	x_3	x_3	x_3	x_3	$-x_3$	$-x_3$	$-x_3$	$-x_3$
(1, 2, 11)	x_1	0	x_3	$-x_3$	0	x_2	0	x_3	$-x_3$	$-x_3$	x_2	0	$-x_3$	x_3	x_3	0	x_3	0	x_3	x_3
(1, 5, 9)	x_1	0	x_2	$-x_2$	0	x_2	x_3	x_3	$-x_3$	x_2	$-x_2$	0	x_3	x_3	0	0	x_3	$-x_3$	x_3	x_3
(1, 5, 14)	x_1	x_3	x_3	$-x_3$	$-x_3$	x_3	$-x_3$	x_2	x_2	$-x_3$	x_2	x_3	x_2	$-x_2$	x_3	$-x_3$	x_3	x_3	x_3	x_3
(1, 6, 11)	x_1	x_3	x_2	$-x_2$	$-x_3$	x_3	x_3	x_2	x_2	$-x_3$	x_3	$-x_2$	x_3	x_3	0	x_3	0	x_3	$-x_3$	x_2
(1, 8, 11)	x_1	x_3	$-x_2$	x_2	$-x_3$	$-x_3$	x_3	x_2	x_2	$-x_3$	x_3	$-x_2$	x_3	x_3	x_2	x_3	x_2	x_3	$-x_3$	x_2
(6, 6, 6)	x_1	x_2	x_3	x_1	$-x_2$	x_1	x_2	x_3	$-x_1$	x_2	x_1	0	$-x_3$	x_2	$-x_3$	x_1	0	$-x_3$	$-x_2$	x_3
(3, 14)	x_1	$-x_2$	x_2	$-x_2$	0	x_1	0	x_2	x_2	x_2	x_1	x_2	$-x_2$	$-x_2$	$-x_2$	0	x_2	$-x_2$	$-x_2$	x_2
(7, 7)	x_1	0	x_1	x_2	0	x_2	0	x_2	$-x_1$	0	x_1	x_1	$-x_1$	x_2	0	x_2	x_2	$-x_2$	$-x_1$	0

Acknowledgments

We thank Professor Stephan Cavior for helpful conversations on the material in Section 4 and Professor Peter Taylor for a crucial remark which enabled us to complete the proof of Theorem 7.

Note added in proof. The conjectures mentioned in section 3 have all been disproved. These results will appear in a paper by A. V. Geramita and J. H. Verner entitled "Orthogonal Designs with Zero Diagonal."

References

1. Anthony V. Geramita, Joan Murphy Geramita, and Jennifer Seberry Wallis, Orthogonal designs, linear and multilinear algebra, to appear.
2. Anthony V. Geramita and Jennifer Seberry Wallis, Orthogonal designs II, *Aequationes Mathematicae*, to appear.
3. Anthony V. Geramita and Jennifer Seberry Wallis, Orthogonal designs III: Weighing matrices, "Proceedings Fifth Southeastern Conference on Combinatorics, Graph Theory and Computing," to appear.
4. J. H. Van Lint and J. J. Seidel, Equilateral point sets in elliptic geometry, *Nederl. Akad. Wetensch. Indag. Math.* **28** (1966), 335–348.
5. D. Raghavarao, Some aspects of weighing designs, *Ann. Math. Statist.* **31** (1960), 878–884.
6. Jennifer Wallis, Orthogonal $(0,1,-1)$-matrices, "Proceedings of the First Australian Conference on Combinatorial Mathematics" (Jennifer Wallis and W. D. Wallis, Eds.), pp. 61–84, Tunra, Newcastle, Australia, 1972.
7. W. D. Wallis, Anne Penfold Street, and Jennifer Seberry Wallis, "Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices," Lecture Notes in Mathematics, Vol. 292, Springer–Verlag, Berlin–Heidelberg–New York, 1972.
8. Morris Newman, "Integral Matrices," Pure and Applied Mathematics, Vol. 45, Academic Press, New York and London, 1972.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.