## Some results on weighing matrices

## Jennifer Seberry Wallis and Albert Leon Whiteman


#### Abstract

It is shown that if $q$ is a prime power then there exists a circulant weighing matrix of order $q^{2}+q+1$ with $q^{2}$ nonzero elements per row and column.

This result allows the bound $N$ to be lowered in the theorem of Geramita and Wallis that "given a square integer $k$ there exists an integer $N$ dependent on $k$ such that weighing matrices of weight $k$ and order $n$ and orthogonal designs $(1, k)$ of order $2 n$ exist for every $n>N$ ".


## 1. Introduction

An orthogonal design of order $n$ and type $\left(s_{1}, s_{2}, \ldots, s_{2}\right)$
$\left(s_{i}>0\right)$ on the commuting variables $x_{1}, x_{2}, \ldots, x_{2}$ is an $n \times n$ matrix $A$ with entries from $\left\{0, \pm x_{1}, \ldots, \pm x_{2}\right\}$ such that

$$
A A^{t}=\left(\sum_{i=1}^{2} \quad s_{i} x_{i}^{2}\right) I_{n} .
$$

Alternatively, the rows of $A$ are formally orthogonal and each row has precisely $s_{i}$ entries of the type $\pm x_{i}$.

In [2], where this was first defined and many examples and properties of such designs were investigated, it is mentioned that

$$
A^{t} A=\left(\sum_{i=1}^{l} s_{i} x_{i}^{2}\right) I_{n}
$$

and so the alternative description of $A$ applies equally well to the
Received 17 February 1975.
columns of $A$. It is also shown in [2] that $l \leq \rho(n)$, where $\rho(n)$ (Radon's function) is defined by

$$
\rho(n)=8 c+2^{d}
$$

when

$$
n=2^{a} \cdot b, \quad b \text { odd, } \quad a=4 c+d, \quad 0 \leq d<4
$$

Also in [2] it is shown that if there is an orthogonal design of order $n$ and type $\left(a^{2}, b\right)$, then
(i) $n \equiv 2(\bmod 4) \Rightarrow b=c^{2}$ for some integer $c$,
(ii) $n=4 t, t$ odd $\Rightarrow b$ is the sum of three integer squares;
while in [5] it is shown that if $n \equiv 4(\bmod 8)$ and if there exists an orthogonal design of order $n$ and type
(i) $(a, a, a, b)$, then $\frac{b}{a}$ is a rational square;
(ii) $(a, a, b)$, then $\frac{b}{a}$ is the sum of two rational squares;
(iii) ( $a, b$ ), then $\frac{b}{a}$ is the sum of three rational squares.

A weighing matrix of weight $k$ and order $n$ is a square $\{0,1,-1\}$ matrix, $W=W(n, k)$, of order $n$ satisfying

$$
W W^{t}=k I_{n}
$$

In [2] it is shown that the existence of an orthogonal design of order $n$ and type $\left(s_{1}, \ldots, s_{\ell}\right)$ is equivalent to the existence of weighing matrices $A_{1}, \ldots, A_{\eta}$, of order $n$, where $A_{i}$ has weight $s_{i}$ and the matrices, $\left\{A_{i}\right\}_{i=1}^{Z}$, satisfy the matrix equation

$$
X Y^{t}+Y X^{t}=0
$$

in pairs. In particular, the existence of an orthogonal design of order $n$ and type $(1, k)$ is equivalent to the existence of a skew-symmetric weighing matrix of weight $k$ and order $n$.

It is conjectured that:
(i) for $n \equiv 2(\bmod 4)$ there is a weighing matrix of weight $k$ and order $n$ for every $k<n-1$ which is the sum of two integer squares;
(ii) for $n \equiv 0(\bmod 4)$ there is a weighing matrix of weight $k$ and order $n$ for every $k \leq n$;
(iii) for $n \equiv 4(\bmod 8)$ there is a skew-symmetric weighing matrix of order $n$ for every $k<n$, where $k$ is the sum of at most three squares of integers (equivalently, there is an orthogonal design of type ( $1, k$ ) in order $n$ for every $k<n$ which is the sum of at most three squares of integers. In other words, the necessary condition for the existence of an orthogonal design of type ( $1, k$ ) in order $n, n \equiv 4(\bmod 8)$ is also sufficient);
(iv) for $n \equiv 0(\bmod 8)$ there is a skew-symmetric weighing matrix of order $n$ for every $k<n$ (equivalently there is an orthogonal design of type ( $1, k$ ) in order $n$ for every $k<n$ );
(v) for $n \equiv 2(\bmod 4)$ there is an orthogonal design of type ( $1, k$ ) in order $n$ for every $k<n-1$ such that $k$ is an integer square.

Conjecture (ii) above is an extension of the Hadamard conjecture (that is, for every $n \equiv 0$ (mod 4) there is a $\{1,-1\}$ matrix, $H$, of order $n$ satisfying $H H^{t}=n I_{n}$ ) while (iv) and (iii) generalize the conjecture that for every $n \equiv 0(\bmod 4)$ there is a Hadamard matrix, $H$, of order $n$, with the property that $H=I_{n}+S$ where $S=-S^{t}$.

Conjecture (ii) was established in [10] for $n \in\{4,8,12, \ldots, 32,40\}$ and in $[6]$ for $n=2^{t}$. Conjecture (iii) was established in [3, Theorem 17] for $n=2^{t}(t \geq 3)$.

Conjectures (iv) and (iii) (and as a consequence conjecture (ii)) were established for $n=2^{t+1} \cdot 3, n=2^{t+1} \cdot 5, t$ a positive integer, in [4] and in [11] for $n=2^{t+1} \cdot 9$. Also in [3] it was shown that only
$k=46,47$ in order 56 remain to be found and the conjectures will be settled for $n=2^{t+1} \cdot 7$.

It has been established [5] that given a square $k$ there exists an $N(k)$ such that $W(n, k)$ exists for every $n>N$. Consequently an orthogonal design ( $1, k$ ) exists in every order $2 n, n>N$.

Here we give some results which allow $N(k)$ to be lowered when $k$ has a factor of 4 .

Let $R$ be the back diagonal matrix. Then an orthogonal design or weighing matrix is said to be constructed from two circulant matrices $A$ and $B$ if it is of the form

$$
\left[\begin{array}{cc}
A & B R \\
B R & -A
\end{array}\right]
$$

and to be of Goethals-Seidel type if it is of the form

$$
\left[\begin{array}{cccc}
A & B R & C R & D R \\
-B R & A & D^{t} R & -C^{t} R \\
-C R & -D^{t} R & A & B^{t} R \\
-D R & C^{t} R & -B^{t} R & A
\end{array}\right]
$$

where $A, B, C, D$ are circulant matrices.
Let $S_{1}, S_{2}, \ldots, S_{n}$ be subsets of $V$, a finite abelian group, containing $k_{1}, k_{2}, \ldots, k_{n}$ elements respectively. Write $T_{i}$ for the totality of all differences between elements of $S_{i}$ (with repetitions), and $T$ for the totality of elements of all the $T_{i}$. If $T$ contains each non-zero element of $V$ a fixed number of times, $\lambda$ say, then the sets $S_{1}, S_{2}, \ldots, S_{n}$ will be called $n-\left\{v ; k_{1}, k_{2}, \ldots, k_{n} ; \lambda\right\}$ supplementary difference sets.
2. Weighing matrices of odd order

If $A$ is a $W(n, k)$, then $(\operatorname{det} A)^{2}=k^{n}$. Thus if $n$ is odd and a $W(n, k)$ exists, then $k$ must be a perfect square.

In [2] where they are first discussed it is shown that

$$
(n-k)^{2}-(n-k)+2>n
$$

must also hold. It is noted there that the "boundary" values of this condition are of special interest; that is, if

$$
(n-k)^{2}-(n-k)+1=n,
$$

for in this case the zeros of $A$ occur such that the incidence between any pair of rows is exactly one. So if we let $B=J-A^{*} A, B$ satisfies

$$
B B^{t}=(n-k-1) I_{n}+J_{n}, \quad B J=(n-k) J_{n} ;
$$

that is, $B$ is the incidence matrix of the projective plane of order $n-k-1$.

Thus, the Bruck-Ryser Theorem on the non-existence of projective planes of various orders implied the non-existence of the appropriate $W(n, k)$.

We shall prove in this paper that if $q$ is a prime power, then a circulant weighing matrix of the form

$$
w\left(q^{2}+q+1, q^{2}\right)
$$

can be constructed. Our method makes use of near difference sets.
In [8] Ryser has given the following definition of a near difference set.

Let $m \geq 4$ be an even integer, and let $k$ and $\lambda$ be positive integers. A near difference set

$$
D=\left\{d_{1}, d_{2}, \ldots, d_{k}\right\}
$$

is a set of $k$ residues modulo $m$ with the property that, for any residue $a \neq 0, \frac{m}{2}(\bmod m)$, the congruence

$$
d_{i}-d_{j} \equiv a(\bmod m)
$$

has exactly $\lambda$ solution pairs $\left(d_{i}, d_{j}\right)$ with $d_{i}$ and $d_{j}$ in $D$ and no solution pairs for $a \equiv \frac{m}{2}(\bmod m)$.

A necessary condition for the existence of a near difference set with
parameters $m, k, \lambda$ is that

$$
k(k-1)=\lambda(m-2)
$$

Let us put

$$
m=2 v
$$

Then the necessary condition becomes

$$
k(k-1)=2 \lambda(v-1) .
$$

Examples of near difference sets are:-

$$
\begin{equation*}
v=7, \quad k=4, \quad \lambda=1, \quad m=14, \tag{i}
\end{equation*}
$$

| 0 | 1 | 4 | 6 |
| :--- | :--- | :--- | :--- |

$$
\begin{equation*}
v=13, \quad k=9, \quad \lambda=3, \quad m=26, \tag{ii}
\end{equation*}
$$

| 0 | 1 | 6 | 8 | 10 | 11 | 12 | 15 | 18 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |

$$
\begin{equation*}
v=21, \quad k=16, \quad \lambda=6, \quad m=42, \tag{iii}
\end{equation*}
$$

| 0 | 1 | 10 | 11 | 18 | 20 | 23 | 25 | 26 | 29 | 30 | 34 | 36 | 37 | 38 | 40 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |

In [1] Elliott and Butson proved that if $q$ is an odd prime power, then we can construct a near difference set with parameters

$$
m=2\left(1+q+q^{2}\right), \quad k=q^{2}, \quad \lambda=\frac{1}{2} q(q-1)
$$

Spence [9] showed that the construction of Elliott and Butson is also valid when $q$ is a power of 2 .

The three examples of near difference sets that we have given illustrate the cases $q=2,3,4$ of the Elliott-Butson-Spence result.

Suppose that we are given a near difference set

$$
D=\left\{d_{1}, d_{2}, \ldots, d_{k}\right\}
$$

with parameters $m, k, \lambda$. Then the polynomial

$$
\alpha(x)=\sum_{d \in D} x^{d}
$$

is the Hall polynomial associated with $D$. Since $D$ is a near difference set we have
$\alpha(x) \alpha\left(x^{-1}\right) \equiv k+\lambda\left(x+x^{2}+\ldots+x^{v-1}+x^{v+1}+\ldots+x^{2 v-1}\right)\left(\bmod x^{2 v}-1\right)$. If we write $T_{r}(x)=1+x+x^{2}+\ldots+x^{2-1}$ this takes the form

$$
\alpha(x) \alpha\left(x^{-1}\right) \equiv k+\lambda\left(T_{2 v}(x)-T_{2}\left(x^{v}\right)\right)\left(\bmod x^{2 v}-1\right):
$$

In the rest of this discussion let $D$ denote the near difference set of Flliott-Butson-Spence. The parameters of $D$ are given by

$$
m=2\left(q^{2}+q+1\right), \quad k=q^{2}, \quad \lambda=\frac{q(q-1)}{2} .
$$

If $\alpha(x)=\sum_{d \in D} x^{d}$, then we have
$\alpha(x) \alpha\left(x^{-1}\right) \equiv q^{2}+\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}+x^{v+1}+\ldots+x^{2 v-1}\right)$
$\left(\bmod x^{2 v}-1\right)$,
where $v=1+q+q^{2}$. Let $k_{1}$ be the number of odd integers in $D$, and $k_{2}$ the number of even integers in $D$. Since a translate of $D$ is also a near difference set with the same parameters we may assume without loss of generality that

$$
k_{2} \geq k_{1}
$$

For $x=-1$ we have

$$
\alpha(-1)=k_{2}-k_{1}, \quad \alpha^{2}(-1)=q^{2} .
$$

## Hence

$$
\alpha(-1)=q .
$$

The two equations

$$
-k_{1}+k_{2}=q,
$$

$$
k_{1}+k_{2}=q^{2}
$$

yield

$$
k_{1}=\frac{q^{2}-q}{2}, \quad k_{2}=\frac{q^{2}+q}{2}
$$

Let us now put

$$
F(x)=\sum_{\substack{d \in D \\ d \text { odd }}} x^{d}, G(x)=\sum_{\substack{d \in D \\ d \text { even }}} x^{d}
$$

Then we have

$$
\begin{aligned}
\alpha(x) & =F(x)+G(x) \\
\alpha\left(x^{-1}\right) & =F\left(x^{-1}\right)+G\left(x^{-1}\right)
\end{aligned}
$$

so that

$$
\alpha(x) \alpha\left(x^{-1}\right)=F(x) F\left(x^{-1}\right)+G(x) G\left(x^{-1}\right)+F(x) G\left(x^{-1}\right)+F\left(x^{-1}\right) G(x)
$$

It is clear that
(1) $\quad F(x) F\left(x^{-1}\right)+G(x) G\left(x^{-1}\right) \equiv$

$$
\equiv q^{2}+\frac{q(q-1)}{2}\left(x^{2}+x^{4}+\ldots+x^{2 v-2}\right)\left(\bmod x^{2 v}-1\right),
$$

(2) $\quad F(x) G\left(x^{-1}\right)+F\left(x^{-1}\right) G(x) \equiv$

$$
\equiv \frac{q(q-1)}{2}\left(x+x^{3}+\ldots+x^{v-2}+x^{v+2}+\ldots+x^{2 v-1}\right)\left(\bmod x^{2 v}-1\right) .
$$

We next put

$$
\alpha_{1}(x)=\sum_{\substack{d \in D \\ d \text { odd }}} x^{(d+v) / 2}, \alpha_{2}(x)=\sum_{\substack{d \in D \\ d \text { even }}} x^{d / 2}
$$

Then the reduction of (1) mod $x^{v}-1$ yields
(3) $\alpha_{1}(x) \alpha_{1}\left(x^{-1}\right)+\alpha_{2}(x) \alpha_{2}\left(x^{-1}\right) \equiv q^{2}+\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right)$

$$
\left(\bmod x^{v}-1\right)
$$

The reduction of (2) $\bmod x^{v}-1$ yields
(4) $\quad \alpha_{1}(x) \alpha_{2}\left(x^{-1}\right)+\alpha_{2}(x) \alpha_{1}\left(x^{-1}\right) \equiv \frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right)$

$$
\left(\bmod x^{v}-1\right)
$$

We shall prove the following theorem.
THEOREM 1. Let $q$ be a prime power. Then a circulant weighing matrix of the form

$$
w\left(q^{2}+q+1, q^{2}\right)
$$

can be constructed.
Proof. Let $D=\left\{d_{1}, d_{2}, \ldots, d_{k}\right\}$ be an Elliott-Butson-Spence near difference set with parameters

$$
m=2\left(q^{2}+q+1\right), \quad k=q^{2}, \quad \lambda=\frac{q(q-1)}{2}
$$

We again put $v=q^{2}+q+1$. Let $S$ be the set of $v$ integers: $0,1,2, \ldots, v-1$. We partition $S$ into three subsets as follows:

$$
S=T_{1} \cup T_{2} \cup T_{3}
$$

where

$$
\begin{aligned}
& T_{1}=\left\{\frac{d+v}{2}(\bmod v), d \in D, d \text { odd }\right\}, \\
& T_{2}=\left\{\frac{d}{2}(\bmod v), d \in D, d \text { even }\right\}, \\
& T_{3}=\left\{s \in S, s \notin T_{1}, s \notin T_{2}\right\}
\end{aligned}
$$

There are $k_{1}$ integers in $T_{1}, k_{2}$ integers in $T_{2}$, and $v-k_{1}-k_{2}$ integers in $T_{3}$.

The sets $T_{1}$ and $T_{2}$ are disjoint. For if

$$
\frac{d_{i}+v}{2} \equiv \frac{d_{j}}{2}(\bmod v)
$$

then

$$
d_{i}-d_{j} \equiv v(\bmod 2 v), \quad\left(d_{i}, d_{j} \in D\right)
$$

in violation of the definition of a near difference set.

The initial row

$$
a_{0}, a_{1}, \ldots, a_{v-1}
$$

of the circulant $W\left(q^{2}+q+1, q^{2}\right)$ is now constructed as follows:

$$
a_{i}= \begin{cases}-1 & \text { if } i \in T_{1} \\ 1 & \text { if } i \in T_{2} \\ 0 & \text { if } i \in T_{3}\end{cases}
$$

Define $\psi(x)=\sum_{i=0}^{v-1} a_{i} x^{i}$. Then we have

$$
\begin{aligned}
\psi(x) & =\alpha_{2}(x)-\alpha_{1}(x) \\
\psi\left(x^{-1}\right) & =\alpha_{2}\left(x^{-1}\right)-\alpha_{1}\left(x^{-1}\right)
\end{aligned}
$$

so that

$$
\begin{aligned}
& \psi(x) \psi\left(x^{-1}\right)=\alpha_{1}(x) \alpha_{1}\left(x^{-1}\right)+\alpha_{2}(x) \alpha_{2}\left(x^{-1}\right)-\alpha_{1}(x) \alpha_{2}\left(x^{-1}\right)-\alpha_{1}\left(x^{-1}\right) \alpha_{2}(x) \\
& \equiv q^{2}+\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right)-\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right) \\
& \equiv q^{2}\left(\bmod x^{v-1}\right) \cdot \\
& \text { (mod } x^{v-1)} \\
&\text { Replacing } \left.x \text { by } \zeta \text { (where } \zeta^{v}=1\right) \text { we obtain }
\end{aligned}
$$

$$
\psi(\zeta) \psi\left(\zeta^{-1}\right)=q^{2}
$$

The last relation is valid for each $v$ th root of unity $\zeta$ including $\zeta=1$. For $\zeta=1$ we have

$$
\psi(1)=k_{2}-k_{1}=\frac{q(q+1)}{2}-\frac{q(q-1)}{2}=q
$$

We next apply the finite Parseval relation:

$$
\sum_{i=0}^{v-1} a_{i} a_{i+r}=\frac{1}{v} \sum_{j=0}^{v-1}\left|\psi\left(\zeta^{j}\right)\right|^{2} \zeta^{j r}
$$

For $r=0$ we have

$$
\sum_{i=0}^{v-1} a_{i}^{2}=\frac{1}{v} v q^{2}=q^{2}
$$

For $l \leq r \leq v-1$ we get

$$
\sum_{i=0}^{v-1} a_{i} a_{i+p}=\frac{1}{v} \cdot q^{2} \cdot 0=0
$$

This completes the proof of the orthogonality of the circulant $W\left(q^{2}+q+1, q^{2}\right)$.

## 3. Other observations

We next note that the sets $T_{1}, T_{2}$ constitute

$$
2-\left\{v ; k_{1}, k_{2} ; k_{1}+k_{2}-\frac{v-1}{2}\right\}
$$

supplementary difference sets. Since $k_{1}=\frac{q(q-1)}{2}, k_{2}=\frac{q(q+1)}{2}$, we have

$$
\lambda=k_{1}+k_{2}-\frac{v-1}{2}=k_{1} .
$$

The result follows at once from

$$
\alpha_{1}(x) \alpha_{1}\left(x^{-1}\right)+\alpha_{2}(x) \alpha_{2}\left(x^{-1}\right) \equiv q^{2}+\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right)
$$

$$
\left(\bmod x^{v}-1\right)
$$

We are now in the position to construct the Hadamard matrix, $H_{292}$, of Spence. We use the following well-known result.

Let $p=2 n+1$ be a prime. Let $U$ be the set of quadratic residues of $p$, and $V$ the set of quadratic non-residues of $p$. Then $U$ and $V$ constitute

$$
2-\left\{v ; k_{3}, k_{4} ; k_{3}+k_{4}-\frac{v+1}{2}\right\}
$$

supplementary difference sets. Here we have

$$
v=p=2 n+1 ; \quad k_{3}=k_{4}=n ; \lambda=n-1 .
$$

Combining our results we find that if $v=q^{2}+q+1$ is a prime, then we construct

$$
2-\left\{v ; k_{1}, k_{2} ; k_{1}+k_{2}-\frac{v-1}{2}\right\}
$$

supplementary difference sets, and also

$$
2-\left\{v ; k_{3}, k_{4} ; k_{3}+k_{4}-\frac{v+1}{2}\right\}
$$

supplementary difference sets. It follows that we have

$$
4-\left\{v ; k_{1}, k_{2}, k_{3}, k_{4} ; k_{1}+k_{2}+k_{3}+k_{4}-v\right\}
$$

supplementary difference sets, which may be used to construct an Hadamard matrix $H_{4 v}$ of Williamson type.

In particular for $q=8$ we have $v=73$. Therefore we can construct $H_{292}$.

Our next objective is to show that the $k_{1}+k_{2}$ numbers in $T_{1} \cup T_{2}$ constitute an ordinary difference set with parameters

$$
v=q^{2}+q+1, \quad k=q^{2}, \quad \lambda=q^{2}-q
$$

For this purpose we form the polynomial

$$
A(x)=\alpha_{1}(x)+\alpha_{2}(x)
$$

so that

$$
A\left(x^{-1}\right)=\alpha_{1}\left(x^{-1}\right)+\alpha_{2}\left(x^{-1}\right)
$$

Then we have

$$
\begin{aligned}
& A(x) A\left(x^{-1}\right)=\alpha_{1}(x) \alpha_{1}\left(x^{-1}\right)+\alpha_{2}(x) \alpha_{2}\left(x^{-1}\right)+\alpha_{1}(x) \alpha_{2}\left(x^{-1}\right)+\alpha_{1}\left(x^{-1}\right) \alpha_{2}(x) \\
& \equiv q^{2}+\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right)+\frac{q(q-1)}{2}\left(x+x^{2}+\ldots+x^{v-1}\right)
\end{aligned}
$$

$$
\left(\bmod x^{v}-1\right)
$$

$$
\equiv q^{2}+q(q-1)\left(x+x^{2}+\ldots+x^{v-1}\right)\left(\bmod x^{v}-1\right)
$$

The set $T_{3}$ is the complement of $T_{1} \cup T_{2}$. Therefore the integers
in $T_{3}$ constitute a difference set with parameters

$$
v^{*}=v, \quad k^{*}=v-k=q+1, \quad \lambda^{*}=v-2 k+\lambda=1
$$

## 4. Applications to weighing matrices and orthogonal designs

 The existence of the $W(21,16)$ allows us to make the following statements.THEOREM 2. There exists a $W(n, 16)$ for every
$n \in\{16,18,20,21,22,24,26, \ldots, 36$, and all orders $\geq 36\}$.
Proof. In [5] it was noted that a $W(n, 16)$ exists for $n \in\{16,18,20, \ldots, 64$, and all orders $\geq 64\}$. Thus the existence of a $W(21,16)$ allows this set to be replaced by that of the enunciation.

THEOREM 3. There exist orthogonal designs (1,9) and (1, 16) in every order $2 n, n \geq 21$.

Proof. These results follow using the $W(21,16)$ to obtain a ( 1,16 ) in order 42 and then noting from Tables 1 and 2 of [4] that each order $2 n, n \geq 2 l$ can be written as $2 m_{1}+2 m_{2}$ where $(1,9)$ and (1, 16) exist for both orders $2 m_{1}$ and $2 m_{2}$.

THEOREM 4. There exists $a \quad W\left(42, a^{2}+b^{2}\right)$ for integers $a, b$ except possibly for $a^{2}+b^{2} \in\{18,25,29,36,37\}$.

Proof. Since a $W(22, k)$ and $W(20, k)$ exist for $k \in\left\{a^{2}+b^{2}: a^{2}+b^{2} \leq 20, a^{2}+b^{2} \neq 18\right\} \quad[4 ;$ Table 2] we have $W(42, k)=W(22, k) \oplus W(20, k)$ for the same $k$.

There is a $W(42, k)$ for $k \in\{26,32,40\}$ by [4; Proposition 13]. Writing $A=W(21,16)$ we see

$$
\left[\begin{array}{ll}
A+I & A-I \\
A^{t}-I & -A^{t}-I
\end{array}\right]
$$

is a $W(42,34)$. Finally since 41 is a prime the construction of Goethals and Seidel [7] gives a $W(42,41)$ and we have the result.

THEOREM 5. Since there exists a $W=W\left(q^{2}+q+1, q^{2}\right)$ for every prime power $q$ there exist orthogonal designs
(i) $\left(1, q^{2}\right)$ and $\left(q^{2}, q^{2}\right)$ in order $2\left(q^{2}+q+1\right)$;
(ii) $\left(1,1,1, q^{2}\right),\left(1,1, q^{2}, q^{2}\right),\left(1, q^{2}, q^{2}, q^{2}\right)$, $\left(q^{2}, q^{2}, q^{2}, q^{2}\right),\left(1,4, q^{2}\right),\left(1,1,2\left(q^{2}+1\right)\right)$, $\left(1, q^{2}, 2\left(q^{2}+1\right)\right),\left(q^{2}, q^{2}, 2\left(q^{2}+1\right)\right),\left(2\left(q^{2}+1\right), 2\left(q^{2}+1\right)\right)$ in every order $4\left(q^{2}+q+1\right)$;
(iii) ( $1,1,2, q^{2}, q^{2}, q^{4}$ ) (at least) in every order $8\left(q^{2}+q+1\right)$;
(iv) $\left(2 q^{2}, 2\left(q^{2}+2 q+2\right)\right)$ in order $4\left(q^{2}+q+1\right)$ with $q^{2}+q+1$ a prime.

Proof. Use $I, W$ in various combinations in the Geothals-Seidel array for (i), (ii), (iii).

For (iv) we note that $W^{*} A=0$ where $A$ is the incidence matrix of the $\left(q^{2}+q+1, q+1,1\right)$ configuration satisfying

$$
A A^{t}=q I+J
$$

and * is the Hadamard product. For every prime order, $p$, there exist circulant matrices $X, Y$ satisfying

$$
X X^{t}+Y Y^{t}=2(p+1) I-2 J .
$$

Then

$$
a W+b A, a W-b A, b X, b Y
$$

may be used in the Goethals-Seidel array to give the required result.
THEOREM 6. Since there exists a $W\left(q^{2}+q+1, q^{2}\right)$ for every prime power $q$ there exist
(i) $W\left(2\left(q^{2}+q+1\right), 2\left(q^{2}+1\right)\right)$;
(ii) $W\left(4\left(q^{2}+q+1\right), 4\left(q^{2}+2\right)\right)$.

## References

[1] J.E.H. Elliott and A.T. Butson, "Relative difference sets", Illinois J. Math. 10 (1966), 517-531.
[2] Anthony V. Geramita, Joan Murphy Geramita, Jennifer Seberry Wallis, "Orthogonal designs", J. Lin. Multilin. Algebra (to appear).
[3] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs II", Aequationes Math. (to appear).
[4] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs III: weighing matrices", Utilitas Math. 6 (1974), 209-236.
[5] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs IV: existence questions", J. Combinatorial Theory Ser. A (to appear).
[6] Anthony V. Geramita, Norman S. Pullman, and Jennifer S. Wallis, "Families of weighing matrices", Bull. Austral. Math. Soc. 10 (1974), 119-122.
[7] J.M. Goethals and J.J. Seidel, "Orthogonal matrices with zero diagonal", Canad. J. Math. 19 (1967), 1001-1010.
[8] H.J. Ryser, "Variants of cyclic difference sets", Proc. Amer. Math. Soc. 41 (1973), 45-50.
[9] Edward Spence, "Skew-Hadamard matrices of the Goethals-Seidel type", Canad. J. Math. (to appear).
[10] Jennifer Wallis, "Orthogonal ( $0,1,-1$ ) matrices", Proc. First Austral. Conf. Combinatorial Math., Newcastle, 1972, 61-84 (TUNRA, Newcestle, 1972).
[11] Jennifer Seberry Wallis, "Orthogonal designs V: orders divisible by eight", Utilitas Math. (to appear).

| Department of Mathematics, | Department of Mathematics, |
| :--- | :--- |
| Institute of Advanced Studies, | University of Southern California, |
| Australian National University, | Los Angeles, |
| Canberra, | California, |
| ACT. | USA. |

