1991

Supplementary difference sets and optimal designs

Christos Koukouvinos

Stratis Kounias

Jennifer Seberry

University of Wollongong, jennie@uow.edu.au

Publication Details

Supplementary difference sets and optimal designs

Abstract
D-optimal designs of order $n = 2v \equiv 2 \pmod{4}$, where $q$ is a prime power and $v = q^2 + q + 1$ are constructed using two methods, one with supplementary difference sets and the other using projective planes more directly.

An infinite family of Hadamard matrices of order $n = 4v$ with maximum excess

$\lambda(n) = n\sqrt{n} - 3$ where $q$ is a prime power and $v = q^2 + q + 1$ is a prime, is also constructed.

Disciplines
Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/1052
Supplementary difference sets and optimal designs

Christos Koukouvinos
Department of Mathematics, University of Thessaloniki, Thessaloniki, 54006, Greece

Stratis Kounias
Department of Statistics, University of Athens, Athens, 15784, Greece

Jennifer Seberry
Department of Computer Science, University College, University of New South Wales, Australian Defence Force Academy, A.C.T. 2600, Australia

Received 31 October 1988

Abstract
Koukouvinos, C., S. Kounias and J. Seberry, Supplementary difference sets and optimal designs, Discrete Mathematics 49–58.

D-optimal designs of order $n = 2v = 2 \pmod{4}$, where $q$ is a prime power and $v = q^2 + q + 1$ are constructed using two methods, one with supplementary difference sets and the other using projective planes more directly.

An infinite family of Hadamard matrices of order $n = 4v$ with maximum excess $\sigma(n) = n\sqrt{n} - 3$ where $q$ is a prime power and $v = q^2 + q + 1$ is a prime, is also constructed.

1. Introduction

In [17–18] (Seberry) Wallis has given the following definition of supplementary difference sets:

If $B = \{b_1, b_2, \ldots, b_k\}$, $D = \{d_1, d_2, \ldots, d_k\}$ are two collections of $k_1, k_2$ residues mod $v$ such that the congruence

$$b_i - b_j = a \pmod{v}, \quad d_i - d_j = a \pmod{v}$$

has exactly $\lambda$ solutions for any $a \not\equiv 0 \pmod{v}$ then $B, D$ are called supplementary difference sets (abbreviated as SDS), denoted by $2^{-\{v; k_1, k_2; \lambda\}}$.

In [5] Elliott and Butson have given the following definition of a relative difference set:

A set $D$ of $k$ elements in a group $G$ of order $vm$ is a difference set of $G$ relative to a normal subgroup $F$ of order $m \not= vm$ if the collection of differences
r - s, r, s ∈ D, r ≠ s contains only the elements of G which are not in F, and contains every such element exactly λ times. This relative difference set (abbreviated as RDS) will be denoted by R(v, m, k, λ).

In this paper we consider the case m = 2, i.e. R(v, 2, k, λ). These RDS are called also near difference sets (see Ryser [13]). In [5] Elliott and Butson proved that if q is an odd prime power, then we can construct cyclic relative difference sets R(v, 2, k, λ), where

\[ n = 2v = 2(q^2 + q + 1), \quad k = q^2, \quad \lambda = \frac{1}{2}q(q - 1) \]  

Spence [16] showed that the construction of Elliott and Butson is also valid when q is a power of 2. For the construction of these R(v, 2, k, λ) see also [11–12].

If n = 2 (mod 4), v = n/2 and R₁, R₂ are \( v \times v \) commuting matrices, with elements ±1, such that

\[ R₁R₁^T + R₂R₂^T = (2v - 2)I_v + qJ_v \]  

then the \( n \times n \) matrix

\[ R = \begin{bmatrix} R₁ & R₂ \\ -R₂^T & R₁^T \end{bmatrix} \]  

has the maximum determinant (Ehlich [4]) among all \( n \times n \pm 1 \) matrices.

Such matrices R are called D-optimal designs of order n and their construction is known for the following values of n: 2, 6, 10, 14, 18, 26, 30, 38, 42, 46, 50, 54, 62, 66, 82, 86 (Ehlich [4], Yang [20–24], Chadjipantelis and Kounias [2], Chadjipantelis, Kounias and Moyssiadis [3]).

If R₁, R₂ are circulant, then pre- and post-multiplying both sides of (2) by \( e^T \) and \( e \) respectively we obtain

\[ (v - 2k₁)^2 + (v - 2k₂)^2 = 4v - 2 \]  

where e is the \( v \times 1 \) matrix of 1’s and \( k₁, k₂ \) is the number of -1’s in every row of R₁, R₂ respectively.

If R₁, R₂ satisfy (2) so do \( ±R₁, ±R₂ \), i.e. we can always take \( 1 ≤ k₁ ≤ k₂ ≤ (v - 1)/2 \). In [2] Chadjipantelis and Kounias proved that the existence of 2-\{v; k₁, k₂; λ\} SDS, where \( k₁, k₂ \) satisfy (4) and \( λ = k₁ + k₂ - (v - 1)/2 \) is equivalent to the existence of D-optimal designs of order \( n = 2v = 2 \ (\text{mod} \ 4) \). In this paper we construct D-optimal designs for \( n = 2 \ (\text{mod} \ 4) \) by using SDS.

Now we give some basic definitions.

An Hadamard matrix, called H-matrix, of order n is an \( n \times n \) matrix H with elements +1, -1 satisfying

\[ H^TH = HH^T = nI_n. \]

The sum of the elements of H, denoted by \( σ(H) \), is called excess of H. The
maximum excess of $H$, over all $H$-matrices of order $n$, is denoted by $\sigma(n)$, i.e.

$$\sigma(n) = \max \sigma(H) \text{ for all } H\text{-matrices of order } n$$  \hspace{1cm} (5)

An equivalent notion is the weight $w(H)$ which is the number of 1's in $H$, then

$$\sigma(H) = 2w(H) - n^2$$

and

$$\sigma(n) = 2w(n) - n^2,$$

see [9–10].

Kounias and Farmakis [10] proved that $\sigma(n) = n\sqrt{n}$ when $n = 4(2m + 1)^2$ and a regular $H$-matrix exists thus satisfying the equality of Best's [1] inequality,

$$\sigma(n) \leq n\sqrt{n}.$$

Infinite families of $H$-matrices satisfying this bound have been found by Seberry [14] and Yamada [19].

Also, Kounias and Farmakis [10] proved that $\sigma(n) = n\sqrt{n} - 3$ can be attained when $n = (2m + 1)^2 + 3$ thus satisfying the equality of the Hammer–Levingston–Seberry [9] bound,

$$\sigma(n) \leq n\sqrt{n} - 3$$

for this bound. This is discussed further in Section 3.

In this paper we also construct an infinite family of $H$-matrices of order $n = 4v$ with maximum excess $\sigma(n) = n\sqrt{n} - 3$, where $q$ is a prime power and $v = q^2 + q + 1$ is a prime.

2. On $D$-optimal designs of order $n = 2 \pmod{4}$

Spence [16] proved the following theorem.

**Theorem 1** (Spence). If there exists a cyclic projective plane of order $q^2$ then there exist two $\pm 1$ matrices $R_1, R_2$, both circulant and of order $1 + q + q^2$, such that

$$R_1R_1^T + R_2R_2^T = 2(q + 1)I + 2J$$

(6)

where $I$ is the identity matrix of order $1 + q + q^2$ and $J$ is the square matrix of order $1 + q + q^2$, all the entries of which are $+1$.

Now, by using the circulant matrices $R_1, R_2$ constructed by Spence in Theorem 1, and the matrix $R$ in (3), we note the following theorem.

**Theorem 2.** There exist $D$-optimal designs of order $n = 2 \pmod{4}$, where $q$ is a prime power and

$$n = 2v = 2(q^2 + q + 1).$$

**Proof.** Let $D = \{d_1, d_2, \ldots, d_k\}$ be a $R(v, 2, k, \lambda)$ as in (1) and $v = q^2 + q + 1$.

The following two sets

$$D_1 = \{(d + v)/2 \pmod{v} \mid d \in D, \text{ d odd}\}$$

and

$$D_2 = \{d/2 \pmod{v} \mid d \in D, \text{ d even}\}$$

(7)
constitute $2\{-v, k_1, k_2; \lambda = k_1 + k_2 - (v - 1)/2\}$ SDS, where

\[
v = q^2 + q + 1, \quad k_1 = \frac{q(q - 1)}{2}, \quad k_2 = \frac{q(q + 1)}{2},
\]

satisfying (4) (see Spence [16], Seberry Wallis and Whiteman [15]).

Since a $R(v, 2, k, \lambda)$ exists when $q$ is a prime power, this completes the proof of Theorem 2. □

The matrices $R_1, R_2$ are the incidence circulant matrices of SDS described in (7) and are constructed by setting $-1$ in the positions indicated in $D_1, D_2$ respectively and $+1$ in the remaining positions. The following examples which are given in Table 1 illustrate the cases $q = 2, 3, 4, 5, 7$ of Theorem 2.

We give another proof of the above result which indicates possibilities for inequivalences and has less restrictions on the underlying structures.

First we note that a matrix, $W$, of order $n$ with entries $0, 1, -1$, exactly $k$ nonzero entries in each row and column and inner product of distinct rows zero is called a \textit{weighing matrix} denoted $W = W(n, k)$. In fact

\[WW^T = kI_n,\]

and a $W(n, n)$ is an Hadamard matrix.

\textbf{Theorem 3.} Let $Q$ and $P$ be the incidence matrices of $(q^2 + q + 1, q + 1, 1)$ difference sets. Further suppose $QP$ has elements $0, 1, 2$. Then $W = QP - J$ is a weighing matrix of order $q^2 + q + 1$ and weight $q^2$ that is $WW^T = q^2I$ and $W$ has entries $0, 1, -1$. Furthermore if $W = X - Y$, where $X$ and $Y$ have entries $0, 1$ then $R = J - X - Y$ satisfies $RR^T = qI + J$, $RJ = (q + 1)J$.

\textbf{Proof.} Since $P$ and $Q$ are incidence matrices of $(q^2 + q + 1, q + 1, 1)$ difference sets

\[PP^T = QQ^T = qI + J, \quad PJ = QJ = (q + 1)J\]

where $P, Q, I, J$ are of order $q^2 + q + 1$. Now

\[WW^T = (QP - J)(P^TQ^T - J) = QPP^TQ^T - JP^TQ^T - QPJ + J^2 = Q(qI + J)Q^T - 2(q + 1)^2 + J^2 = qQQ^T - (q + 1)^2J + J^2 = qI + qJ - (q^2 + 2q + 1 - q^2 - q - 1)J = q^2I.\]

Since $PQ$ had entries $0, 1, 2$ $PQ - J$ must have entries $0, 1, -1$.

Now $WJ = QPJ - J^2 = (q + 1)^2J - J^2 = qJ$. So $WJ = (X - Y)J = qJ$. $WW^T = q^2I$.
### Table 1

<table>
<thead>
<tr>
<th>$n$</th>
<th>$q$</th>
<th>$v$</th>
<th>$k$</th>
<th>$k_1$</th>
<th>$k_2$</th>
<th>$\lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>2</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>26</td>
<td>3</td>
<td>13</td>
<td>9</td>
<td>3</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>42</td>
<td>4</td>
<td>21</td>
<td>16</td>
<td>6</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>62</td>
<td>5</td>
<td>31</td>
<td>25</td>
<td>10</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>114</td>
<td>7</td>
<td>57</td>
<td>49</td>
<td>21</td>
<td>52</td>
<td>28</td>
</tr>
</tbody>
</table>

(i) $D = \{0, 1, 4, 6\}$
(ii) $D = \{0, 1, 4, 6, 9\} $
C. Koukouvinos et al.

says $W$ has $q^2$ entries $1$ or $-1$ in each row, say $x$ ones and $y$ minus ones. Then

$$x - y = q, \quad x + y = q^2$$

and thus

$$x = \frac{1}{2}q(q + 1), \quad y = \frac{1}{2}q(q - 1).$$

Now any row of $W$ has $x = \frac{1}{2}(q^2 + q)$ ones, $y = \frac{1}{2}(q^2 - q)$ minus ones and $q + 1$ zeros.

Write any two rows of $W$ as

$$\begin{array}{cccccccccccc}
1 & \cdots & 1 & - & \cdots & 0 & \cdots & 0 & 1 & \cdots & 1 & - & \cdots & 0 & \cdots & 0 \\
a & c & e & b & d & f & x - a - b & y - c - d & q + 1 - e - f
\end{array}$$

where there are, for example $a$ columns ($\binom{1}{1}$) and $f$ columns ($\binom{1}{0}$).

Now the number of columns ($\binom{6}{0}$) is $q + 1 - e - f$. Furthermore the inner product of each pair of rows is zero so $a + b - c - d = 0$. Also

$$a + c + e = x \quad \text{(number of ones in first row)}$$

$$b + d + f = y \quad \text{(number of minus ones in first row)}.$$ 

Hence

$$q + 1 - e - f = q + 1 + a + c - x + b + d - y = -q^2 + q + 1 + a + c + b + d$$

$$= -q^2 + q + 1 + 2c + 2d \quad \text{(using } a + b - c - d = 0)$$

$$\leq -q^2 + q + 1 + q^2 - q \quad \text{(number of minus ones in second row)}$$

$$\leq 1.$$ 

Now $1 \geq q + 1 - e - f \geq 0$. Suppose $q + 1 - e - f = 0$ then using

$$a + b + c + d + e + f = q^2$$

$$a + b - c - d = 0$$

$$e + f = q + 1$$

We have

$$2a + 2b = q^2 + q + 1.$$ 

But $q^2 + q + 1$ is always odd. So we have a contradiction and $q + 1 - e - f = 1$. In other words each row of $W$ has $q + 1$ zeros and in each pair of rows of $W$ exactly one zero is underneath a zero. Thus if $R = J - X - Y$ is the matrix with ones where $W$ had zeros $R$ is the incidence matrix of a $(q^2 + 1 + 1, q + 1, 1)$ configuration. So

$$RR^T = qI + J \quad \text{and} \quad RJ = (q + 1)J.$$ 

Furthermore if $P$ and $q$ were defined on a cyclic (abelian) group, $R$ is defined on the same group.
**Theorem 4.** There exist two matrices $A$ and $B$ of order $q^2 + q + 1$ which satisfy
\[ AA^T + BB^T = 2(q^2 + q)I + 2J. \]

**Proof.** Let $A = W + R$ and $B = W - R$ be defined as above. \(\square\)

**Corollary 5.** There is a D-optimal design of order $2(q^2 + q + 1)$ whenever there is a $(q^2 + q + 1, q + 1, 1)$ difference set.

**Proof.** Use
\[ \begin{bmatrix} A & B \\ -B^T & A^T \end{bmatrix} \]
as before. \(\square\)

**Remark 1.** This construction does not require the difference set to be defined on a cyclic group. Glynn [7], Geramita and Seberry [6, p. 152] have shown the conditions of the theorem can be met, for example if $P = Q$ in theorem.

**Remark 2.** We note that the sets $D_1$ and $D_2$ of $2 - \{v; k_1, k_2; \lambda\}$ SDS described in (7) are disjoint.

For if
\[ \frac{d_i + v}{2} = \frac{d_j}{2} \pmod{v} \]
then $d_i - d_j = v \pmod{2v}$, $(d_i, d_j \in D)$ in violation of the definition of a RDS. (see Seberry Wallis and Whitman [15]).

D-optimal designs have been constructed for $n = 14, n = 26$ by Ehlich [4] and Yang [22] and for $n = 42, n = 62$ by Yang [20,23] and Chadjipantelis and Kounias [2]. All the other orders of D-optimal designs which are constructed by the above method are new.

3. The maximum excess of Hadamard matrices of order $n = 4v$

First we show that the Hammer–Levingston–Seberry [9, p. 246] bound for $n = (2m + 1)^2 + 3$ is the same as that found by Kounias and Farmakis [10, section 4].

Hammer, Levingston and Seberry [9, p. 217] show that for H-matrices of order $n$, writing $x$ for the greatest even integer $<\sqrt{n}$, $t = x$ if $|n - x^2| < (x + 2)^2 - n$ and $t = x - 2$ otherwise, i the integer part of $n((t + 4)^2 - n)/8(t + 2)$, the excess of the H-matrices is bounded by
\[ \sigma(n) = n(t + 4) - 4i. \]
Write \( n = (2m + 1)^2 + 3 = 4(m^2 + m + 1) \). Now \( x \), even, is the greatest even integer \( < \sqrt{n} \).

Let \( x = 2a \), then \( 2a < \sqrt{n} \) and
\[
4m^2 \leq 4a^2 < 4(m^2 + m + 1) < 4(m + 1)^2
\]

Hence \( m \leq a < m + 1 \).

Thus we can write
\[
x = 2a = 2m, \quad t = x - 2 = 2m - 2 \quad \text{and} \quad i = m^2 + m + 1.
\]

Hence
\[
\sigma(n) \leq (2m + 2) - 4i = n(2m + 2) - n = n(2m + 1) = n\sqrt{n - 3}
\]

This was the result given in Kounias and Farmakis [10]. We summarize this as the following lemma.

**Lemma 6.** The Hammer-Levingston-Seberry bound is equivalent to \( \sigma(n) \leq n(2m + 1) = n\sqrt{n - 3} \) when \( n = (2m + 1)^2 + 3 \).

Kounias and Farmakis [10] proved that \( \sigma(n) = n\sqrt{n - 3} \) can be attained when \( n = (2m + 1)^2 + 3 \) thus satisfying the equality of the above bound.

Spence [16] proved the following theorem.

**Theorem 7** (Spence). If there exists a cyclic projective plane of order \( q^2 \) and two supplementary difference sets in a cyclic group of order \( 1 + q + q^2 \), then there exists a Hadamard matrix of the Goethals-Seidel type of order \( 4(1 + q + q^2) \).

Now, from this theorem of Spence we note the following theorem.

**Theorem 8.** There exist \( H \)-matrices of order \( n = (2q + 1)^2 + 3 \), with maximum excess \( \sigma(n) = n\sqrt{n - 3} \), where \( q \) is a prime power and \( v = q^2 + q + 1 \) is a prime.

**Proof.** It is easy to see (Spence [16], Seberry Wallis and Whiteman [15]) that if \( v = q^2 + q + 1 \) is a prime, then we can construct two sets \( D_3 \) and \( D_4 \) as
\[
2 - \left\{ v; k_3, k_4; k_3 + k_4 - \frac{v + 1}{2} \right\}
\]
SDS, where \( D_3 \) is the set of quadratic residues of \( v \), and \( D_4 \) is the set of quadratic nonresidues of \( v \), \( k_3 = k_4 = q(q + 1)/2 \), \( \lambda = k_3 + k_4 - (v + 1)/2 = q(q + 1)/2 - 1 \).

By using (7) and (9) SDS, we can construct a
\[
4 - \left\{ v; k_1, k_2, k_3, k_4; \lambda = \sum_{i=1}^{4} k_i - v \right\}
\]
which may be used to construct \( H \)-matrices \( (H_{n}) \) of the Goethals-Seidel type.
Now, it is obvious that $n = 4v = 4(q^2 + q + 1) = (2q + 1)^2 + 3$, and from Lemma 3 and the result of Kounias and Farmakis [10], we note that these H-matrices have maximum excess $\sigma(n) = n\sqrt{n} - 3$. □

If we construct the $R_3$, $R_4$ incidence circulant matrices of (9) SDS, we have

$$R_3R_4^T + R_4R_3^T = 2(q^2 + q + 2)I_v - 2J_v. \tag{10}$$

Hence from (6) and (10) we obtain:

$$R_1R_4^T + R_2R_3^T + R_4R_1^T + R_3R_4^T = 4(q^2 + q + 1)I_v = 4vJ_v. \tag{11}$$

The following matrix $G$, whose construction is due to Goethals and Seidel [8], is an H-matrix of order $4(q^2 + q + 1)$:

$$G = \begin{bmatrix}
R_1 & R_2W & R_3W & R_4W \\
-R_2W & R_1 & -R_3W & R_4W \\
-R_3W & R_2W & R_1 & -R_4W \\
-R_4W & R_3W & R_2W & R_1
\end{bmatrix} \tag{12}$$

where $W = [w_{ij}]$ is the permutation matrix of order $v = q^2 + q + 1$ defined by

$$w_{ij} = \begin{cases} 
1, & \text{if } i + j = 1 \pmod{v}, \\
0, & \text{otherwise}.
\end{cases}$$

The circulant $(1, -1)$ matrices $R_1, R_2, R_3, R_4$ of order $v$, have row sums $2q + 1, 1, 1, 1$ respectively, then $G$ gives the row-sum vector $(2q^2e_1, 2q^2 + 4)e_n^T$ where $re_s^T$ denotes the $1 \times s$ vector $(r, r, \ldots, r)$.

**Example.** From Theorem 8 we obtain the following orders of H-matrices with maximum excess:

- $n = 28$ \quad $(q = 2, v = 7)$,
- $n = 52$ \quad $(q = 3, v = 13)$,
- $n = 124$ \quad $(q = 5, v = 31)$,
- $n = 292$ \quad $(q = 8, v = 73)$,
- $n = 1228$ \quad $(q = 17, v = 307)$,
- $n = 3028$ \quad $(q = 27, v = 757)$,
- $n = 6892$ \quad $(q = 41, v = 1723)$,
- $n = 14164$ \quad $(q = 59, v = 3541)$, \quad etc.

H-matrices with maximum excess have been constructed for $n = 28, n = 52, n = 124$ from the results of Hammer, Levingston and Seberry [9] using Williamson-type matrices alone, or from the results of Kounias and Farmakis [10]. All the other orders of H-matrices with maximum excess are new.
References

[14] J. Seberry, SBIBD \((4k^2, 2k^2 + k, k^2 + k)\) and Hadamard matrices of order \(4k^2\) with maximal excess are equivalent, Graphs Combin. 5 (1989) 373–383.