ELSEVIER

Journal of Statistical Planning and Inference 62 (1997) 81–90

journal of statistical planning and inference

Optimal designs, supplementary difference sets and multipliers

C. Koukouvinos[a], Jennifer Seberry[b,*], A.L. Whiteman[c], Ming-yuan Xia[d]

[a]*Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece*
[b]*Department of Computer Science, University of Wollongong, Wollongong, NSW 2522, Australia*
[c]*Department of Mathematics, University of Southern California, Los Angeles, CA 90089, USA*
[d]*Department of Mathematics, Huazhong Normal University, Wuhan, 430070, China*

Received 6 July 1994; revised 19 June 1995

Abstract

We investigate multipliers of $2-\{v;q^2,q^2;\lambda\}$ supplementary difference sets where cyclotomy has been used to construct D-optimal designs.

AMS classification: primary 62K05; 05B10, secondary 11T22

Keywords: Cyclotomy; Multiplier; D-optimal designs; Supplementary difference sets

1. Introduction

Let $S_1, S_2, \ldots, S_u$ be subsets of V, a finite abelian group of order v written in additive notation containing $k_1, k_2, \ldots, k_u$ 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 λ, say, then $S_1, S_2, \ldots, S_u$ will be called $u-\{v;k_1,k_2,\ldots,k_u;\lambda\}$ *supplementary difference sets.* Throughout this paper as in Wallis (1972), where they were first defined, and Seberry Wallis (1973), Wallis et al. (1972) and Wallis (1974) this will be abbreviated as sds.

The parameters of $u-\{v;k_1,k_2,\ldots,k_u;\lambda\}$ supplementary difference sets satisfy

$$\lambda(v-1)=\sum_{i=1}^{u}k_i(k_i-1). \tag{1}$$

* Corresponding author.

PII S0378-3758(96)00171-1

If $k_1 = k_2 = \cdots = k_u$ we will write $u - \{v; k; \lambda\}$ to denote the u supplementary difference sets and (1) becomes

$$\lambda(v-1) = uk(k-1). \tag{2}$$

We shall be concerned with collections defined on a fixed group V of order v in which repeated elements are counted multiply, rather than as with sets. If T_1 and T_2 are two collections then T_1 and T_2 will denote the result of adjoining the elements of T_1 to T_2 with total multiplicities retained.

Notation 1. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a k-set then we will use the notation

$$\Delta A = [a_i - a_j\colon\ i \neq j,\ 1 \leqslant i,\ j \leqslant k].$$

We refer to Seberry Wallis (1973) for the elementary theory of cyclotomy.

Let x be a primitive root of GF(v) where $v = p^r = ef + 1$ is a prime power. Write GF(v) $\setminus \{0\}$. The *cyclotomic classes* C_i in GF(v) are

$$C_i = \{x^{es+i}\colon\ 0 \leqslant s \leqslant f-1\}, \quad 0 \leqslant i \leqslant e-1.$$

We note that C_i are pairwise disjoint and their union is GF(v) $\setminus \{0\}$.

If $n \equiv 2 \pmod 4$, $v = \frac{1}{2}n$ and M, N are $v \times v$ commuting matrices, with elements ± 1, such that

$$MM^{\mathrm{T}} + NN^{\mathrm{T}} = (2v-2)I_v + 2J_v, \tag{3}$$

then the $n \times n$ matrix

$$R = \begin{bmatrix} M & N \\ -N^{\mathrm{T}} & M^{\mathrm{T}} \end{bmatrix}$$

has the maximum determinant (see Cohn, 1989; Ehlich, 1964) among all $n \times n \pm 1$ matrices. Such matrices are called D-optimal designs of order n.

Now form the two sets $A = \{a_1, a_2, \ldots, a_{k_1}\}$ and $B = \{b_1, b_2, \ldots, b_{k_2}\}$ where a_i, b_j denote the positions of the -1's in the first row of M, N, respectively. If the matrices M, N are circulant, then they satisfy (3) if and only if (see Chadjipantelis and Kounias, 1985) they are sds

$$2 - \{v; k_1, k_2; \lambda\}, \quad \lambda = k_1 + k_2 - \tfrac{1}{4}(n-2) \text{ and } k_1 \geqslant k_2 \geqslant 0$$

are found from

$$(v - 2k_1)^2 + (v - 2k_2)^2 = 2n - 2.$$

Hence the construction of the circulant matrices M and N satisfying (3) is equivalent to the construction of the corresponding sds. A similar result holds for group developed matrices and prime power orders.

2. Main theorems

Koukouvinos et al. (1991) proved the following theorem.

Theorem 1. *There exist D-optimal designs of order* $n \equiv 2 \pmod 4$ *where*

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

and q *is a prime power.*

Whiteman (1990) proved the following theorem.

Theorem 2. *There exist D-optimal designs of order* $n \equiv 2 \pmod 4$, *where*

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

and q *is an odd prime power.*

The proof of Theorem 1 is based on supplementary difference sets whereas the proof of Theorem 2 is based on a remarkable construction of symmetric block designs due to Brouwer (1983).

It is natural to ask if Theorem 2 can be established alternatively by means of a supplementary difference set construction.

The problem reduces to finding for each odd prime power q a pair of supplementary difference sets with parameters

$$v = 2q^2 + 2q + 1, \qquad k_1 = k_2 = q^2, \qquad \lambda = q(q-1).$$

The possibility that these supplementary difference sets also exist for q even is not precluded.

Theorem 3. *Let* g *be a generator of the cyclic group* $\mathrm{GF}(v) \setminus \{0\}$. *Suppose*

(i) $v = 2q^2 + 2q + 1$ *is a prime power,*

(ii) A *and* B *are* $2 - \{v; q^2, q^2; \lambda\}$ *sds such that* $2q + 1$ *is a multiplier i.e.* $B = (2q+1)A$, *and* $2q + 1 \in C_i$,

(iii) A *and* B *are unions of cyclotomic classes.*

Then every $\alpha \in C_i$ *or* $\alpha \in C_i^{-1}$ *is also a multiplier i.e.* $B = \alpha A$.

Proof. If q is even let

$$C_i = \{g^{4mj+i}\colon\ 0 \leqslant j \leqslant q\}, \quad 0 \leqslant i \leqslant 4m-1,\ q = 2m.$$

We have $2q + 1 \in C_m$ or $C_{3m} = C_m^{-1}$

$$A = \{0\} \cup C_{i_1} \cup C_{i_2} \cup \cdots \cup C_{i_{2m-1}}$$

and

$$B = \{0\} \cup C_{i_1+m} \cup C_{i_2+m} \cup \cdots \cup C_{i_{2m-1}+m},$$

for all $\alpha \in C_m$, $\alpha A = \{0\} \cup \alpha C_{i_1} \cup \alpha C_{i_2} \cup \cdots \cup \alpha C_{i_{2m-1}}$, $\alpha = g^{4mj+m}$ for some j and $2q+1 = g^{4mj_0+m}$ for some j_0.

$$\begin{aligned}\alpha C_{i_1} &= \{g^{4mj+m} \cdot g^{4mk+i_1}\colon\ 0 \leqslant k \leqslant q\} = \{g^{4m(j+k)+i_1+m}\colon\ 0 \leqslant k \leqslant q\} \\ &= \{g^{4m\ell+i_1+m}\colon\ 0 \leqslant \ell \leqslant q\} = C_{i_1+m}.\end{aligned}$$

Also if $\alpha \in C_{3m}$ we proceed similarly with m replaced by $3m$.

If q is odd let

$$C_i = \{g^{4mj+i}\colon\ 0 \leqslant j \leqslant q-1\}, \quad 0 \leqslant i \leqslant 4m-1,\ q = 2m-1$$

and the same proof follows. □

Theorem 4. *Suppose g is a generator of* GF(v) *where $v = 4m+1$, m odd. If $(A, g^{\alpha}A)$ are 2-sds for some α then so are $(A, g^{\beta}A)$ for $\beta = 4m-\alpha,\ 2m+\alpha,\ 2m-\alpha$.*

Proof. *Case $\beta = 4m-\alpha$:*

$$\begin{aligned}\Delta A + \Delta g^{4m-\alpha}A &= \Delta A + g^{4m-\alpha}\Delta A = g^{4m}\Delta A + g^{4m-\alpha}\Delta A \\ &= g^{4m-\alpha}(g^{\alpha}\Delta A + \Delta A) = g^{4m-\alpha}(\Delta A + \Delta g^{\alpha}A).\end{aligned}$$

Case $\beta = 2m+\alpha$:

$$\Delta A + \Delta g^{2m+\alpha}A = \Delta A + \Delta g^{\alpha}A.$$

Case $\beta = 2m-\alpha$:

$$\Delta A + \Delta g^{2m-\alpha}A = g^{2m}\Delta A + \Delta g^{2m-\alpha}A = g^{2m-\alpha}(\Delta A + g^{\alpha}\Delta A). \qquad \square$$

3. Results

3.1. The case $q = 2$

Here $v = 13$ and we find $2 - \{13; 4, 4; 2\}$ sds by using 2 as a generator of GF(13) and the cyclotomic classes

$$C_0 = \{1, 3, 9\}, \qquad C_i = 2^i C_0, \quad i = 1, 2, 3.$$

Then

$$A = \{0\} \cup C_0, \qquad B = \{0\} \cup C_1 = 5A$$

are $2-\{13;4,4;2\}$ sds, now $2q+1=5\in C_1$ and

$$\text{for all } a\in C_1\cup C_3, \quad \text{we have } B(\omega)=A(\omega^a),$$

where $\omega=e^{2\pi i/v}$ is a primitive vth root of unity.

3.2. The case $q = 3$

Here $v=25$ (a prime power) and we find $2-\{25;9,9;6\}$ sds by using the solution x of $x^2=x+3$ as a generator of GF(5^2) and the cyclotomic classes

$$C_0=\{1,2x+1,3x+3\}, \qquad C_i=x^iC_0, \quad i=1,2,\ldots,7.$$

Then

$$A=C_0\cup C_1\cup C_4, \qquad B=x^2A$$

are $2-\{25;9,9;6\}$ sds and every element in C_2 or C_6 is a multiplier so

$$\text{for all } a\in C_2\cup C_6, \quad \text{we have } B=aA.$$

3.3. The case $q = 4$

Here $v=41$ and we find $2-\{41;16,16;12\}$ sds by using 6 as a generator of GF(41) and the cyclotomic classes

$$C_0=\{1,10,16,18,37\}, \qquad C_i=6^iC_0, \quad i=1,2,\ldots,7.$$

Then

$$A=\{0\}\cup C_1\cup C_5\cup C_6, \qquad B=6^6A$$

are $2-\{41;16,16;12\}$ sds and every element in C_2 or C_6 is a multiplier. We note $2q+1=9\in C_6$ and

$$\text{for all } a\in C_2\cup C_6, \text{ we have } B(\omega)=A(\omega^a),$$

where $\omega=e^{2\pi i/v}$ is a primitive vth root of unity.

3.4. The case $q = 5$

Here $v=61$ and we find $2-\{61;25,25;20\}$ sds by using 2 as a generator of GF(61) and the cyclotomic classes

$$C_0=\{1,9,20,34,58\}, \qquad C_i=2^iC_0, \quad i=1,2,\ldots,11.$$

Then

$$A=C_0\cup C_2\cup C_3\cup C_5\cup C_6, \qquad B=2^3A$$

are $2-\{61;25,25;20\}$ sds. We note $2q+1 = 11 \in C_3$ and

for all $a \in C_3 \cup C_9$, we have $B(\omega) = A(\omega^a)$,

where $\omega = e^{2\pi i/v}$ is a primitive vth root of unity.

3.5. The case $q = 7$

Here $v = 113$ and we find $2-\{113;49,49;42\}$ sds by using 3 as a generator of GF(113) and the cyclotomic classes

$$C_0 = \{1,16,28,30,49,100,109\}, \qquad C_i = 3^i C_0, \quad i = 1,2,\ldots,15.$$

Then

$$A = C_0 \cup C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_8 \cup C_{12}, \qquad B = 3^4 A$$

are $2-\{113;49,49;42\}$ sds. We note $2q+1 = 15 \in C_4$ and

for all $a \in C_4 \cup C_{12}$, $\quad B(\omega) = A(\omega^a)$,

where $\omega = e^{2\pi i/v}$ is a primitive vth root of unity.

3.6. The case $q = 9$

Here $v = 181$ and we find $2-\{181;81,81;72\}$ sds by using 2 as a generator of GF(181) and the cyclotomic classes

$$C_0 = \{1,39,43,48,62,65,73,80,132\}, \qquad C_i = 2^i C_0, \quad i = 1,2,\ldots,19.$$

Then

$$A = C_0 \cup C_1 \cup C_7 \cup C_{10} \cup C_{11} \cup C_{13} \cup C_{14} \cup C_{16} \cup C_{19}, \qquad B = 2^5 A$$

are $2-\{181;81,81;72\}$ sds. We note $2q+1 = 19 \in C_{15}$ and

for all $a \in C_5 \cup C_{15}$, we have $B(\omega) = A(\omega^a)$,

where $\omega = e^{2\pi i/v}$ is a primitive vth root of unity.

Conjecture 1. *For each prime power q there exists a pair of supplementary difference sets A and B with parameters*

$$v = 2q^2 + 2q + 1, \qquad k_1 = k_2 = q^2, \qquad \lambda = q(q-1),$$

where v is a prime power and the relation

$$B(\omega) = A(\omega^{2q+1})$$

holds where $\omega = e^{2\pi i/v}$ is a primitive vth root of unity.

4. Some remarks on results of Dokovic

We note that if $C_a \cup C_b \cup \cdots \cup C_c$ and $C_d \cup C_e \cup \cdots \cup C_f$ are two sds then $C_{a+j} \cup C_{b+j} \cup \cdots \cup C_{c+j}$ and $C_{d+j} \cup C_{e+j} \cup \cdots \cup C_{f+j}$ are also two sds.

4.1. The case $q = 4$

The primitive element 6 was used to generate GF(41). Then the cyclotomic classes

$$C_i = \{6^{8j+i}: 0 \leqslant j \leqslant 5\}, \quad 0 \leqslant i \leqslant 8$$

were formed.

Then using Dokovic (1991, p. 374), where he uses the α_k notation for the cosets and we use the C_i notation for our cyclotomic classes, we have the correspondence

α_k	0	1	2	3	4	5	6	7
C_i	0	4	2	6	7	3	1	5

The sds given in Dokovic (1991) were transformed using the mapping $\alpha_{k_x} \to C_{i_x}$ and then multiplied as indicated.

Case	Map	2^xP	2^xQ
(a)	6^0	$A = C_0 \cup C_2 \cup C_3 \cup C_4 \cup C_7$	$6^6A = C_0 \cup C_1 \cup C_2 \cup C_5 \cup C_6$
(b)	6^6	$6^3A = C_2 \cup C_3 \cup C_5 \cup C_6 \cup C_7$	$B = C_0 \cup C_1 \cup C_2 \cup C_4 \cup C_5$
(c)	6^0	$B = C_0 \cup C_1 \cup C_2 \cup C_4 \cup C_5$	$6^1B = C_1 \cup C_2 \cup C_3 \cup C_5 \cup C_6$
(d)	6^0	$C = C_0 \cup C_2 \cup C_3 \cup C_4 \cup C_6$	$D = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_6$

For case (a) we have $B(\omega) = A(\omega^9)$ where $2q+1 = 9 \in C_6$. We note that $-6^4A = B$. So case (a) is $(A, 6^6A)$, case (b) is $(6^3A, B)$, and case (c) is $(B, 6^1B)$. We showed in our Theorem 3 that any element of $C_2 \cup C_6$ is a multiplier for A. By Theorem 4 if g^α is a multiplier then so are $g^{40-\alpha}$, $g^{20+\alpha}$ and $g^{20-\alpha}$. Using our notation these are inequivalent $2 - \{41; 25, 25; 30\}$.

The inequivalent $2 - \{41; 16, 16; 12\}$ are given below:

Case	Map	2^xP	2^xQ
(a)	6^0	$A' = \{0\} \cup C_1 \cup C_5 \cup C_6$	$6^6A' = \{0\} \cup C_3 \cup C_4 \cup C_7$
(b)	6^6	$6^3A' = \{0\} \cup C_0 \cup C_1 \cup C_4$	$B' = \{0\} \cup C_3 \cup C_6 \cup C_7$
(c)	6^0	$B' = \{0\} \cup C_3 \cup C_6 \cup C_7$	$6^1B' = \{0\} \cup C_0 \cup C_4 \cup C_7$
(d)	6^0	$C' = \{0\} \cup C_1 \cup C_5 \cup C_7$	$D' = \{0\} \cup C_4 \cup C_5 \cup C_7$

4.2. The case q = 5

The primitive element 2 was used to generate GF(61). Then the cyclotomic classes

$$C_i = \{2^{12j+i}: 0 \leqslant j \leqslant 5\}, \quad 0 \leqslant i \leqslant 11$$

were formed.

Then using Dokovic (1991, p. 375); where he uses the α_k notation for the cosets and we use the C_i notation for our cyclotomic classes, we have the correspondence

α_k	0	1	2	3	4	5	6	7	8	9	10	11
C_i	0	6	1	7	2	8	10	4	3	9	11	5

The sds given in Dokovic (1991, p. 375) were transformed using the mapping $\alpha_{k_x} \to C_{i_x}$ and then multiplied as indicated.

Case	Map	2^xP	2^xQ
(a)	2^7	$A = C_0 \cup C_4 \cup C_7 \cup C_9 \cup C_{10}$	$B = C_0 \cup C_1 \cup C_2 \cup C_6 \cup C_{10}$
(h)	2^3	$2^6A = C_1 \cup C_3 \cup C_4 \cup C_6 \cup C_{10}$	$B = C_0 \cup C_1 \cup C_2 \cup C_6 \cup C_{10}$
(j)	2^7	$B = C_0 \cup C_1 \cup C_2 \cup C_6 \cup C_{10}$	$2^6A = C_1 \cup C_3 \cup C_4 \cup C_6 \cup C_{10}$
(b)	2^1	$E = C_1 \cup C_3 \cup C_6 \cup C_7 \cup C_{11}$	$D = C_0 \cup C_1 \cup C_4 \cup C_6 \cup C_8$
(c)	2^{10}	$D = C_0 \cup C_1 \cup C_4 \cup C_6 \cup C_8$	$2^6E = C_0 \cup C_1 \cup C_5 \cup C_7 \cup C_9$
(e)	2^2	$2^3E = C_2 \cup C_4 \cup C_6 \cup C_9 \cup C_{10}$	$D = C_0 \cup C_1 \cup C_4 \cup C_6 \cup C_8$
(i)	2^9	$2^9E = C_0 \cup C_3 \cup C_4 \cup C_8 \cup C_{10}$	$D = C_0 \cup C_1 \cup C_4 \cup C_6 \cup C_8$
(d)	2^4	$F = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_{10}$	$G = C_0 \cup C_5 \cup C_8 \cup C_{10} \cup C_{11}$
(g)	2^7	$2^9F = C_0 \cup C_1 \cup C_7 \cup C_9 \cup C_{10}$	$F = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_{10}$
(f)	2^3	$H = C_1 \cup C_3 \cup C_6 \cup C_7 \cup C_{10}$	$I = C_0 \cup C_1 \cup C_2 \cup C_5 \cup C_6$

One of these is $11 \cdot P = Q$. We will show that $\Delta(C_i) = \Delta(-C_i) = \Delta(2^{12j}C_i) = \Delta(2^{12j+6}C_i)$. This means that since $2^9 \in C_9$ any element of C_9 or C_3 can act as a multiplier and, noting $11 \in C_3$, we have for case (g) that $B(\omega) = A(\omega^{11})$ and $B(\omega) = A(-\omega^{11})$.

We note that

$$\Delta(A) = \{x - y: x \in A, y \in A\}.$$

Suppose $d = x - y$ has δ_{x-y} solutions in $\Delta(A)$ then $-d = y - x$ has the same number of solutions δ_{x-y}. This means that in $\Delta(-A)$ we have $-d = -x - (-y)$ and $d = -y - (-x)$ also have δ_{x-y} solutions. Hence $\Delta(A) = \Delta(-A) = 2^{60}\Delta(A) = a\Delta(A)$ for every $a \in C_0$ or C_6.

This means cases (a), (h) and (j) are equivalent. Cases (b) and (c) are equivalent; cases (e) and (i) are equivalent; and the cases (d), (g) and (f) are inequivalent to all

of these. Hence there are six equivalence classes when group multipliers are taken into account.

Case	2^xP	2^xQ
(a)	$A = C_0 \cup C_4 \cup C_7 \cup C_9 \cup C_{10}$	$B = C_0 \cup C_1 \cup C_2 \cup C_6 \cup C_{10}$
(b)	$E = C_1 \cup C_3 \cup C_6 \cup C_7 \cup C_{11}$	$D = C_0 \cup C_1 \cup C_4 \cup C_6 \cup C_8$
(e)	$D = C_0 \cup C_1 \cup C_4 \cup C_6 \cup C_8$	$2^3E = C_2 \cup C_4 \cup C_6 \cup C_9 \cup C_{10}$
(d)	$F = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_{10}$	$G = C_0 \cup C_5 \cup C_8 \cup C_{10} \cup C_{11}$
(g)	$F = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_{10}$	$2^3F = C_1 \cup C_3 \cup C_4 \cup C_6 \cup C_7$
(f)	$H = C_1 \cup C_3 \cup C_6 \cup C_7 \cup C_{10}$	$I = C_0 \cup C_1 \cup C_2 \cup C_5 \cup C_6$

5. More results in the cyclic groups

5.1. The case $q = 3$

We have also found the following example which is inequivalent to those mentioned above:

$$A = \{0, 1, 2, 6, 8, 10, 11, 14, 15\}, \qquad B = 7A.$$

These are $2 - \{25; 9, 9; 6\}$ sds.

5.2. The case $q = 4$

We have also found the following example which is inequivalent to those mentioned above:

$$A = \{0, 1, 7, 14, 17, 20, 21, 22, 25, 26, 27, 29, 31, 37, 39, 40\}, \qquad B = 9A.$$

These are $2 - \{41; 16, 16; 12\}$ sds.

References

Brouwer, A.E. (1983). An infinite series of symmetric designs. Math. Centrum Amsterdam Report ZW 202/83.

Chadjipantelis, T. and S. Kounias (1985). Supplementary difference sets and D-optimal designs for $n \equiv 2 \pmod 4$. *Discrete Math.* **57**, 211–216.

Cohn, J.H.E. (1989). On determinants with elements ± 1, II. *Bull. London Math. Soc.* **21**, 36–42.

Dokovic, D.Z. (1991). On maximal $(1, -1)$-matrices of order $2n$, n odd. *Radovi Matematicki* **7**, 371–378.

Ehlich, H. (1964). Determinantenabschatzungen fur binare matrizen. *Math. Z.* **83**, 123–132.

Koukouvinos, C., S. Kounias and J. Seberry (1991). Supplementary difference sets and optimal designs. *Discrete Math.* **88**, 49–58.

Wallis, J. (1972). On supplementary difference sets. *Aequationes Math.* **8**, 242–257.

Seberry Wallis, J. (1973). Some remarks on supplementary difference sets. *Coll. Math. Soc. Janos Bolyai* **10**, 1503–1526.

Wallis, J. (1974). A note on supplementary difference sets, *Aequationes Math.* **10**, 46–49.
Wallis, W.D., A.P. Street and J. Seberry Wallis (1972). *Combinatorics: room Squares, sum-free sets, Hadamard Matrices*, Lecture Notes in Mathematics, Vol. 292, Springer, Berlin.
Whiteman, A.L. (1990). A family of D-optimal designs. *Ars Combin.* **30**, 23–26.
Yang, C.H. (1969). On designs of maximal $(1,-1)$-matrices of order $n \equiv 2 \pmod 4$ II. *Math. Comp.* **23**, 201–205.