AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **85(2)** (2023), Pages 220–227

Constructions of new families for Supplementary Difference Sets

Tianbing Xia

School of Computing and Information Technology
University of Wollongong
NSW 2522, Australia
txia@uow.edu.au

Guoxin Zuo Mingyuan Xia

School of Mathematics and Statistics
Central China Normal University
Wuhan, Hubei 430079, P. R. China
zuogx@mail.ccnu.edu.cn xiamy@mail.ccnu.edu.cn

Jennifer Seberry

School of Computing and Information Technology
University of Wollongong
NSW 2522, Australia
jennie@uow.edu.au

Abstract

In this paper, we construct two new families of Supplementary Difference Sets (SDS), that is,
4-$\{q^2; (q^2-1)/8; (q^2-9)/16\}$ SDS and 4-$\{q^2; q(q-1)/2; q(q-2)\}$ SDS.

1 Introduction

Hadamard matrices play important roles in communication systems, image processing and computer security (see [4, 7]). Hadamard matrices can be constructed by using different methods. Baumert and Hall Jr. [1], Turyn [8], and Xia et al. [9, 12] constructed Hadamard matrices from Williamson matrices. Cooper and Seberry (Wallis) defined T-matrices in 1972 [3]. Xia proposed the C-partitions on an abelian group [10] and found an infinite family of C-partitions on $GF(q^2)$ with $q \equiv 3 \pmod 8$, q a prime power [14, 16]. Chen [2] constructed a partition on $GF(q^2)$, then M. Xia et al. [15] generalized the results from $GF(q^2)$ to $GF(q)$. See [6] for more details.

ISSN: 2202-3518

Supplementary difference sets (SDS) are very useful in the construction of Hadamard matrices [10, 11, 13]. Compared to the results in [16], we give different methods on the constructions of C-partitions and SDS in this paper. The construction is new and the 4-$\left\{q^2; \frac{(q^2-1)}{8}; \frac{(q^2-9)}{1}6\right\}$ SDS is new.

Let G be an abelian group of order v. We denote the group operation by multiplication. Subsets $D_1, \dots, D_r$ of G are called r-$\{v; |D_1|, \dots, |D_r|; \lambda\}$ SDS, if for every nonidentity element g in G, there are exactly λ elements $(d, d^{'})$ in $D_1 \times D_1$, or $D_2 \times D_2$, $\dots$, or $D_r \times D_r$ such that $gd^{'} = d$. It is convenient to use the group ring $Z[G]$ of the group G over the ring Z of rational integers with addition and multiplication. Here the elements of $Z[G]$ are of the form

$$a_1 g_1 + a_2 g_2 + \cdots + a_v g_v, a_i \in Z,\ g_i \in G.$$

In $Z[G]$, the addition $+$ is given by the rule

$$\left(\sum_g a(g)g\right) + \left(\sum_g b(g)g\right) = \sum_g \left(a(g) + b(g)\right) g.$$

The multiplication in $Z[G]$ is given by the rule

$$\left(\sum_g a(g)g\right)\left(\sum_h b(h)h\right) = \sum_k \left(\sum_{gh=k} a(g)b(h)\right) k.$$

For any subset A of G, we denote an element

$$\sum_{g \in A} g \in Z[G],$$

and by abusing the notation, we denote it by A.

Let A and B be subsets of G and let t be an integer. We define

$$B^{(t)} = \sum_{b \in B} b^t \in Z[G],$$
$$AB^{(-1)} = \sum_{a \in A, b \in B} ab^{-1} \in Z[G],$$

and denote

$$\Delta A = AA^{(-1)},\ \ \Delta(A, B) = AB^{(-1)} + BA^{(-1)}.$$

If $A = \emptyset$, we define

$$\Delta\emptyset = 0,\ \Delta(\emptyset, B) = 0.$$

With this convention, $D_1, \dots, D_r$ being r-$\{v; |D_1|, \dots, |D_r|; \lambda\}$ SDS, are equivalent to

$$\sum_{i=1}^{r} \Delta D_i = \left(\sum_{i=1}^{r} |D_i| - \lambda\right) + \lambda G.$$

If $r = 1$, the single SDS becomes a difference set (DS) in the usual sense. When $|D_1| = \cdots = |D_r| = k$, we denote r-$\{v; |D_1|, \ldots, |d_r|; \lambda\}$ by r-$\{v; k; \lambda\}$. It is well-known that 4-$\{q^2; \frac{q(q-1)}{2}; q(q-2)\}$ SDS have been constructed for prime powers $q \equiv 1$ and $3 \pmod 4$, except for $q \equiv 7 \pmod 8$. (See [2, 8, 9, 10, 11, 12, 13].)

In this paper we give two new families of SDS:

$$4-\left\{q^2; \frac{(q^2-1)}{8}; \frac{(q^2-9)}{16}\right\} \text{ and } 4-\left\{q^2; \frac{q(q-1)}{2}; q(q-2)\right\},$$

where q is a prime power congruent to 3 (mod 8). By using the second SDS we can construct Hadamard matrices of order $4q^2$.

2 Preliminaries

Let q be a prime power congruent to $3 \pmod 4$ and let g be a generator of the cyclic group of $G = GF(q^2)$. Set

$$c_i = \left\{g^{2(q+1)j+i} : j = 0, \ldots, \frac{(q-3)}{2}\right\}, \quad i = 0, 1, \ldots, 2q+1, \tag{2.1}$$

$$s_i = c_i \cup c_{i+q+1}, \quad i = 0, 1, \ldots, q. \tag{2.2}$$

Then the c_i and the s_i are partitions of $GF(q^2)$ into cosets of the quadratic residues of $GF(q)$ and the multiplicative group of $GF(q)$, respectively.

Denote

$$\Psi_0 = \Delta c_0, \quad \Psi_i = \Delta(c_0, c_i), \quad i = 1, \ldots, 2q+1,$$

and define

$$\Psi_i = \Psi_j \quad \text{as} \quad i \equiv j \pmod{2q+2}.$$

We have

$$\begin{aligned} \Delta c_i &= g^i \Psi_0, \quad i = 0, 1, \ldots, 2q+1, \\ \Delta(c_i, c_j) &= g^i \Psi_{j-i} = g^j \Psi_{i-j}\, i \quad \text{for } i \neq j. \end{aligned}$$

In particular,

$$\Psi_i = g^i \Psi_{-i} = g^i \Psi_{2q+2-i}, \quad i = 0, 1, \ldots, 2q+1.$$

From [10], we have the following lemma.

Lemma 2.1 *If $q \equiv 3 \pmod 4$ is a prime power, and $v = q^2$, then the following equations hold:*

(a) $\Psi_0 = \frac{(q-1)}{2} + \frac{(q-3)}{4} s_0$;

(b) $\Psi_{q+1} = \frac{(q-1)}{2} s_0$;

(c) $\Psi_i + \Psi_{i+q+1} = G^* - s_0 - s_i, \quad i = 1, \ldots, q,$

where $G^* = G \setminus \{0\}$.

Proof. From the definition of c_i in (2.1), c_0 is a Paley difference set and Ψ_{q+1} contains all non-quadratic residues in $GF(q)$. From [5] (page 178), it is easy to see that $\Psi_0 = \frac{(q-1)}{2} + \frac{(q-3)}{4}s_0$ and $\Psi_{q+1} = \frac{(q-1)}{2}s_0$. So (a) and (b) are proven.

Since $q \equiv 3 \pmod 4$ is a prime power, $f(x) = x^2+1$ is irreducible in $GF(q)$, and $ax+b \pmod{f(x)}$ is a finite field of $GF(v)$, where $a, b \in GF(q)$. Let $q = 4m+3$, and let h be a primitive element of $GF(q)$. We have

$$c_0 = \left\{h^{2i} : i = 0, \ldots, 2m\right\}, \quad c_{4m+4} = \left\{h^{2i+1} : i = 0, \ldots, 2m\right\}, \text{ and}$$
$$s_{2m+2} = c_{2m+2} \cup c_{6m+6} = \left\{h^i x : i = 0, \ldots, 4m+1\right\}.$$

When $i = 2m+2$,

$$\begin{aligned}
\Psi_{2m+2} + \Psi_{6m+6} &= \sum_{0\le k\le 2m,\ 0\le j\le 4m+1} \left(\left(h^{2k} - h^j x\right) + \left(h^j x - h^{2k}\right)\right) \\
&= \sum_{0\le k\le 2m,\ 0\le j\le 4m+1} \left(\left(h^j x + h^{2k}\right) + \left(h^j x + h^{2k+1}\right)\right) \\
&= \sum_{0\le j,k\le 4m+1} \left(h^j x + h^k\right) = G^* - s_0 - s_{2m+2}.
\end{aligned}$$

When $i \neq 2m+2,\ 1 \le i \le 4m+3$, denote $g^i = h^\alpha x + h^\beta$. Then we have

$$c_i + c_{i+4m+4} = s_i = \left\{h^{\alpha+j}x + h^{\beta+j} : j = 0, \ldots, 4m+1\right\},$$

and

$$\begin{aligned}
\Psi_i \quad &+ \quad \Psi_{i+4m+4} \\
&= \Delta(c_0, s_i) \\
&= \sum_{0\le k\le 2m,\ 0\le j\le 4m+1} \left(\left(h^{2k} - \left(h^{\alpha+j}x + h^{\beta+j}\right)\right) + \left(\left(h^{\alpha+j}x + h^{beta+j}\right) - h^{2k}\right)\right) \\
&= \sum_{0\le k\le 2m,\ 0\le j\le 4m+1} \left(\left(h^{\alpha+j}x + \left(\left(h^{\beta+j} + h^{2k}\right)\right) + \left(h^{\alpha+j}x + \left(h^{beta+j} + h^{2k+1}\right)\right)\right)\right) \\
&= \sum_{0\le j,k\le 4m+1} \left(h^{\alpha+j}x + \left(h^{\beta+j} + h^k\right)\right) \\
&= \sum_{0\le j\le 4m+1,\ c\in GF(q)} \left(h^{\alpha+j}x + c\right) - \sum_{0\le j\le 4m+1} \left(h^{\alpha+j}x + h^{\beta+j}\right) \\
&= G^* - s_0 - s_i.
\end{aligned}$$

So (c) is proven, and the proof is complete. □

It is easy to see that

$$\begin{aligned}
\sum_{i=0}^{q} g^i \Psi_0 &= \frac{q-1}{2}\sum_{i=0}^{q} g^i + \frac{q-3}{4}\sum_{i=0}^{q} g^i s_0 = \frac{(q^2-1)}{2} + \frac{(q-3)}{4}G^*, \text{ and} \\
\sum_{i=0}^{q} g^i \Psi_i &= \sum_{i=0}^{q} \Delta(c_0, c_i) = \frac{(q-1)}{2}G^*,\ i = 1, \ldots, q.
\end{aligned}$$

3 Two new families of SDS

From now on let $q \equiv 3 \pmod 8$ be a prime power. Set

$$A = \sum_{i=0}^{\frac{(q-3)}{4}} c_{8i}, \tag{3.1}$$

$$A_j = g^{\frac{(j-1)(q+1)}{4}} A = \sum_{i=0}^{\frac{(q-3)}{4}} c_{8i+\frac{(j-1)(q+1)}{4}},\ j = 1, 2, 3, 4. \tag{3.2}$$

Theorem 3.1 *There are* 4-$\{q^2; \frac{(q^2-1)}{8}; \frac{(q^2-9)}{16}\}$ *SDS for every prime power* q *with* $q \equiv 3 \pmod 8$.

Proof. If $q = 3$, we take $A_1 = A_2 = A_3 = A_4 = \{0\}$. Clearly, $A_1, \ldots, A_4$ are 4-$\{9; 1; 0\}$ SDS. Now suppose $q > 3$. We take $A_1, \ldots, A_4$ as defined in (3.1) and (3.2).

We prove that these are 4-$\{q^2; \frac{(q^2-1)}{8}; \frac{(q^2-9)}{16}\}$ SDS. First, from a simple calculation, we have

$$\Delta A = \sum_{i=0}^{\frac{(q-3)}{4}} g^{4i}(\Psi_0 + \sum_{j=1}^{\frac{(q-3)}{8}} \Psi_{8j}).$$

Then

$$\begin{aligned} \sum_{k=1}^{4} \Delta A_k &= \sum_{i=0}^{q} g^i(\Psi_0 + \sum_{j=1}^{\frac{(q-3)}{8}} \Psi_{8j}) \\ &= \frac{(7q^2+1)}{16} + \frac{(q^2-9)}{16} G. \end{aligned}$$

So the proof is complete. □

Let X and Y be two subsets of $\{0, 1, \ldots, 2q+1\}$, such that

$$X \cap \{i + q + 1 (\mathrm{mod}\ 2q+2) : i \in X\} = \emptyset, \tag{3.3}$$

$$\{i (\mathrm{mod}\ q+1) : i \in X\} \cap Y = \emptyset, \tag{3.4}$$

and

$$|X| + 2|Y| = q. \tag{3.5}$$

Write

$$D = \sum_{i \in X} c_i + \sum_{j \in Y} s_j. \tag{3.6}$$

It is well-known that

$$\Delta D = \frac{(q-1)(q-|X|)}{2} + \frac{(q-|X|)(q+|X|-2)}{4}G^* - \frac{(q-|X|)}{2}\sum_{i\in X} s_i + \Delta E, \quad (3.7)$$

where $E = \sum_{i\in X} c_i$. (See [11] for more details.) We see that the equation (3.7) is dependent on the set X only, but the set Y has nothing to do with it.

Theorem 3.2 *Let* $q \equiv 3 \pmod 8$ *be a prime power. Then there are* 4-$\{q^2; \frac{q(q-1)}{2}; q(q-2)\}$ *SDS.*

Proof. In (3.6), taking $X = \{8i : i = 0, \ldots, \frac{(q-3)}{4}\}$ and $D_k = g^{\frac{(k-1)(q+1)}{4}}D$, $k = 1, 2, 3, 4$, we have

$$\sum_{k=1}^{4} \Delta D_k = q^2 + q(q-2)G.$$

The proof is now complete. □

The proof of SDS here is different from that in [10]. Using these SDS obtained from Theorem 3.2, we can construct a Hadamard matrix of order $4q^2$.

Remark 3.1 In $GF(9)$, let $g = w+1 \pmod{w^2+1,\ \mathrm{mod}\ 3}$ be a generator of $GF(9)$, and set

$$D_i = \{0, g^{i-1}, g^{i+3}\}, \quad i = 1, 2, 3, 4.$$

Then they are 4-$\{9; 3; 3\}$ SDS and their $(1, -1)$ incidence matrices are of type 1; say A, B, C, D, are symmetric and satisfy

$$\begin{aligned} A^2 + B^2 + C^2 + D^2 &= 36I_9, \\ AB - CD = AC - BD = AD - BC &= 0. \end{aligned}$$

(See [14] for more details.)

Although we have not got a 4-$\{q^2; \frac{q(q-1)}{2}; q(q-2)\}$ SDS for prime powers q with $q \equiv 7 \pmod 8$, nevertheless here is an example below.

Example 3.1 In $GF(49)$, let $g = w + 2$ and

$$\begin{aligned} &c_i = \{g^{16j+i} (\mathrm{mod}\ w^2+1, \mathrm{mod}\ 7) : j = 0, 1, 2\},\ i = 0, 1, \ldots, 15, \\ &s_i = c_i + c_{i+8},\ i = 0, 1, \ldots, 7. \end{aligned}$$

Take $X = \{0, 3, 6\}$ and $Y = \{1, 2\}$; put

$$\begin{aligned} D &= \sum_{i\in X} c_i + \sum_{j\in Y} s_j, \\ D_k &= g^{2(k-1)}D, k = 1, 2, 3, 4. \end{aligned} \quad (3.8)$$

It is easy to verify that D_1, D_2, D_3, D_4 in (3.8) are 4-$\{49; 21; 35\}$ SDS. Take $X = \{0, 3, 6, 9, 12\}$ and $Y = \{2\}$; put

$$\begin{aligned} D &= \sum_{i\in X} c_i + s_2, \\ D_k &= g^{2(k-1)} D, k = 1, 2, 3, 4. \end{aligned} \tag{3.9}$$

It is easy to verify that D_1, D_2, D_3, D_4 in (3.9) are 4-$\{49; 21; 35\}$ SDS too. Take

$$X = \{0, 5, 10\} \text{ and } Y = \{1, 3\} \tag{3.10}$$

or

$$X = \{0, 4, 5, 10, 15\} \text{ and } Y = \{1\}, \tag{3.11}$$

and putting D_k, $k = 1, 2, 3, 4$, as in (3.8), (3.9) respectively, we can get 4-$\{49; 21; 35\}$ SDS again.

Example 3.2 In $GF(121)$, let $g = x + 4$ and

$$c_i = \left\{g^{24j+i} \pmod{x^2+1, \bmod 11} : j = 0, 1, 2, 3, 4\right\}, \ i = 0, \ldots, 23,$$
$$s_i = c_i \cup c_{i+12}, \quad T_i = \sum_{h\in s_i} h, \ i = 0, \ldots, 11.$$

Set

$$\begin{aligned} D_1 &= c_0 \cup c_8 \cup c_{16} \cup s_1 \cup s_2 \cup s_3 \cup s_5; \\ D_i &= g^{i-1} D_1, \quad i = 2, 3, 4. \end{aligned}$$

We have

$$\begin{aligned} \Delta D_1 = {} & 55 + 22(T_0 + T_4 + T_8) + 25(T_1 + T_5 + T_9) + 27(T_2 + T_6 + T_{10}) \\ & +25(T_3 + T_7 + T_{10}), \end{aligned}$$

so that

$$\sum_{i=1}^{4} \Delta D_i = 121 + 99G,$$

and we can get a 4-$\{121; 55; 99\}$ SDS.

Acknowledgments

The authors thank the editor and the anonymous reviewers for their helpful comments and useful suggestions.

References

[1] L. D. Baumert and M. Hall Jr., A new construction for hadamard matrices, *Bull. Amer. Math. Soc.* 71 (1965), 169–170.

[2] Y. Q. Chen, On the existence of Abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Applic'ns* 3 (1997), 234–256.

[3] J. Cooper and J. Seberry (Wallis), A construction for Hadamard arrays, *Bull. Aust. Math. Soc.* 7 (1972), 269–278.

[4] H. Evangelaras, C. Koukouvinos and J. Seberry, Applications of Hadamard matrices, *J. Telecommunications and Inf. Tech.* (2003), 3–10.

[5] M. Hall Jr., *Combinatorial Theory*, 2nd ed., John Wiley and Sons, New York, 1986.

[6] J. Seberry, *Orthogonal Designs, Hadamard Matrices, Quadratic Forms and Algebras*, Springer, 2017.

[7] J. Seberry, B. J. Wysocki and T. A. Wysocki, On some applications of Hadamard matrices. *Metrika* 62 (2005), 221–239; `https://doi.org/10.1007/s00184-005-0415-y`.

[8] R. J. Turyn, A special class of Williamson matrices and difference sets, *J. Combin. Theory Ser. A* 36 (1984), 111–115.

[9] M. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory Ser. A* 61 (1992), 230–242.

[10] M. Xia, On supplementary difference sets and Hadamard matrices, *Acta Mathematica Scientia* 4(1) (1984), 81–92.

[11] M. Xia, Some new families of SDS and Hadamard matrices, *Acta math. Sci.* 16 (1996), 153–161.

[12] M. Xia and G. Liu, An infinite class of supplementary differences sets and Williamson matrices, *J. Combin. Theory Ser. A* 58 (1991), 310–317.

[13] M. Xia and T. Xia, Hadamard matrices constructed from supplementary difference sets in the class H_1, *J. Combin. Des.* 2(5) (1994), 325–339.

[14] M. Xia and T. Xia, A family of C-partitions and T-matrices, *J. Combin. Des.* 7 (1999), 269–281.

[15] M. Xia, T. Xia and J. Seberry, A new method for constructing Williamson matrices, *Des. Codes Crypto.* 35 (2005), 191–209.

[16] M. Xia, T. Xia, J. Seberry and G. Zuo, A new method for constructing T-matrices, *Australas. J. Combin.* 32 (2005), 61–78.

(Received 24 Oct 2022)