# Some new results of regular Hadamard matrices and SBIBD II\*

# TIANBING XIA

CCSR, School of ITACS
University of Wollongong
NSW 2522
Australia
txia@uow.edu.au

# MINGYUAN XIA

School of Mathematics & Statistics
Central China Normal University
Wuhan, Hubei 430079
China
xiamy@mail.ccnu.edu.cn

#### JENNIFER SEBERRY

CCSR, School of ITACS University of Wollongong NSW 2522 Australia j.seberry@uow.edu.au

#### Abstract

In this paper we prove that there exist  $4 - \{k^2; \frac{1}{2}k(k-1); k(k-2)\}$  SDS, regular Hadamard matrices of order  $4k^2$ , and SBIBD( $4k^2, 2k^2 + k, k^2 + k$ ) for  $k = 47, 71, 151, 167, 199, 263, 359, 439, 599, 631, 727, 919, <math>5q_1, 5q_2N, 7q_3$ , where  $q_1, q_2$  and  $q_3$  are prime powers such that  $q_1 \equiv 1 \pmod{4}$ ,  $q_2 \equiv 5 \pmod{8}$  and  $q_3 \equiv 3 \pmod{8}$ ,  $N = 2^a 3^b t^2$ , a, b = 0 or  $1, t \neq 0$  is an arbitrary integer. We find new SBIBD( $4k^2, 2k^2 + k, k^2 + k$ ) for 43 values of k less than 1000.

<sup>\*</sup> The research supported by the ARC (No. LX0560185).

# 1 Preliminaries

An  $n \times n$  matrix H is called an Hadamard matrix (or H-matrix) if every entry of the matrix is 1 or -1, and

$$HH^T = nI_n$$

where  $I_n$  is an  $n \times n$  identity matrix. In this paper we use  $H^T$  to denote the transpose of a matrix H.

We denote the excess of a Hadamard matrix  $H = [a_{ij}]$  by  $\sigma(H)$ , where

$$\sigma(H) = \sum_{1 \le i, j \le n} a_{ij}.$$

Let  $\sigma(n) = \max\{\sigma(H)\}$ . The weight of a Hadamard matrix H, denoted by W(H), is the number of ones in the H. We define  $W(n) = \max\{W(H)\}$ . Note that the maxima are taken over all Hadamard matrices H of order n. It is obvious that  $\sigma(H) = 2W(H) - n^2$  and  $\sigma(n) = 2W(n) - n^2$  (see [3, 4, 5, 6] for details).

M. R. Best [1] proved that

$$\sigma(n) \le n\sqrt{n}.\tag{1}$$

**Definition 1** (Regular Hadamard Matrix) A regular Hadamard matrix has the sum of each column of the matrix and the sum of each row of the matrix constant.

**Definition 2** (SBIBD) A symmetric balanced incomplete block design, called as  $SBIBD(v,k,\lambda)$ , is defined by a  $v \times v$  matrix M, which has every entry 0 or 1. The sum of each column and the sum of each row of the matrix is k. For any two columns  $c_i$ ,  $c_j$  (and two rows  $r_i$ ,  $r_j$ ),  $1 \le i \ne j \le v$ , the inner product of  $c_i$  and  $c_j$  ( $r_i$  and  $r_j$ ) is  $\lambda$  (see [8]).

In 1989 J. Seberry proved the following theorem which is very useful for constructing SBIBD( $4k^2$ ,  $2k^2 + k$ ,  $k^2 + k$ ).

**Theorem 1** (J. Seberry [6]) The following conditions are equivalent:

- (i) There exists a Hadamard matrix of order  $4k^2$  with maximum excess  $8k^3$ .
- (ii) There exists a regular Hadamard matrix of order  $4k^2$ .
- (iii) There exists an  $SBIBD(4k^2, 2k^2 + k, k^2 + k)$ .

Many regular Hadamard matrices of order  $4k^2$  and SBIBD $(4k^2, 2k^2 + k, k^2 + k)$  were given in [3, 7, 11]. In particular, there were 169 values of k less than 1000 for which the existence of SBIBD $(4k^2, 2k^2 + k, k^2 + k)$  was still undetermined (see the list of [11]).

# 2 Construct SBIBD from SDS

**Definition 3** (SDS) 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  $r-\{v; |D_1|, \dots, |D_r|; \lambda\}$  supplementary difference sets (SDS), if for every nonidentity element g in G there are exactly  $\lambda$  ordered pairs (d, d') in  $D_1 \times D_1$ , or  $D_2 \times D_2$ , ..., or  $D_r \times D_r$ , such that qd' = 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

$$a_1g_1 + a_2g_2 + \dots + a_vg_v, \ a_i \in Z, \ g_i \in G.$$

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

$$\sum_{g \in G} a(g)g + \sum_{g \in G} b(g)g = \sum_{g \in G} (a(g) + b(g))g.$$

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

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

For any subset A of G we define

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

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

For any two subsets  $A, B \subset G$ , 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

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

If  $A = \emptyset$ , then we have

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

It is obviously that  $\Delta(A, A) = 2\Delta A$ .

With this convention  $D_1, D_2, \cdots, D_r$  being  $r - \{v; |D_1|, \cdots, |D_r|; \lambda\}$  SDS are equivalent to

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

If  $k_1 = \cdots = k_r = k$ , we simplify  $D_1, \cdots, D_r$  to  $r - \{v; k; \lambda\}$  SDS. When r = 1, the single SDS becomes a difference set (DS) in the usual sense. When r = 4 and  $\lambda = \sum_{i=1}^4 k_i - v$ , we call  $D_1, D_2, D_3, D_4$  type H-SDS.

In this paper special interest is devoted to the case:  $v=q^2$ ,  $k_1=k_2=k_3=k_4=\frac{1}{2}q(q-1)$  and  $\lambda=q(q-2)$  (see [6]).

To construct SBIBD from SDS we need the following theorem.

**Theorem 2** (T. Xia, M.Y. Xia and J. Seberry [11]) If there exists a  $4 - \{q^2; \frac{1}{2}q(q-1); q(q-2)\}$  SDS on an abelian group G of order  $q^2$ , then there exists an  $SBIBD(4q^2, 2q^2 + q, q^2 + q)$ .

In the following we assume p is an odd prime, r > 0, and

$$q = p^r = 4m + 3.$$

Let g be a generator of  $GF(q^2)^*$ . Put

$$E_i = \{g^{8(m+1)j+i} : j = 0, \dots, 2m\}, \quad i = 0, \dots, 8m+7.$$
 (2)

**Lemma 1** (M.Y. Xia and G. Liu [9]) In  $GF(q^2)$  the following equations hold:

(i) 
$$\Delta E_i = (2m+1) + m(E_i + E_i^{-1}),$$

(ii) 
$$\Delta(E_i, E_i^{-1}) = (2m+1)(E_i + E_i^{-1}),$$

(iii) 
$$\Delta(E_i, E_j + E_j^{-1}) = GF(q^2)^* - (E_i + E_i^{-1} + E_j + E_j^{-1}),$$

where  $0 \le i \ne j \le 8m + 7$ ,  $GF(q^2)^*$  is the set of all nonzero elements of  $GF(q^2)$ .

Let

$$U = \{a_i: 0 \le a_i \le 8m + 7, i = 0, \dots, 2t\},\$$

$$V = \{b_i: 0 \le b_i \le 4m + 4, j = 1, \dots, 2m + 1 - t\},\$$

where  $0 \le t \le 2m + 1$ , such that

$$|\{a \pmod{4m+4}: a \in U\} \cup V| = 2m+2+t. \tag{3}$$

The equation (3) means that  $a_i \not\equiv a_j \pmod{4m+4}$  for  $i \neq j$  and  $a_i \not\equiv b_j \pmod{4m+4}$  for any i, j. Write

$$A = \bigcup_{a \in U} E_a, \ B = \bigcup_{b \in V} (E_b \cup E_{b+4m+4})$$
 (4)

and set

$$D = A \cup B. \tag{5}$$

**Lemma 2** Under the condition (3) we have

$$\Delta D = 2(2m+1-t)(2m+1) + ((2m+1)^2 - t^2)GF(q^2)^* - (2m+1-t)(A+A^{-1}) + \Delta A.$$
 (6)

**Proof.** (6) follows from Lemma 1 by direct calculation.

From (6) we can see that  $\triangle D$  only depends on A and does not depend on the particular choice of B. This is a very useful property in searching SDS.

Put

$$D_i = g^{(m+1)i}D, \quad i = 0, 1, 2, 3.$$
 (7)

We investigate when  $D_0$ ,  $D_1$ ,  $D_2$  and  $D_3$  defined as above can form  $4 - \{q^2; \frac{1}{2}q(q-1); q(q-2)\}$  SDS for some appropriate set A, i.e.,

$$\sum_{i=1}^{3} \Delta D_i = q^2 + q(q-2)GF(q^2). \tag{8}$$

When  $q \equiv 3 \pmod{8}$ , many subsets in  $GF(q^2)$  can be taken as the A that makes (8) true [9, 10]. In other cases we know of no general answer so far. Fortunately, when  $q \equiv 7 \pmod{16}$ , we find many positive results.

**Lemma 3** For q = 71, 151, 167, 199, 263, 359, 439, 599, 631, 727 and 919, there exist subsets A of  $GF(q^2)$  that make (8) true.

Concrete constructions for A in the above cases are given in the Appendix of the paper. Using Lemma 1 and Lemma 2 one can check they satisfy (8). We leave verification to the reader.

Lemma 3 is an attempt to search for  $4-\{q^2;\ \frac{1}{2}q(q-1);\ q(q-2)\}$  SDS when  $q\equiv 7\pmod 8$ . From Lemma 3 it follows

Corollary 1 There exist  $SBIBD(4k^2; 2k^2 + k; k^2 + k)$  for k = 71, 151, 167, 199, 263, 359, 439, 599, 631, 727 and 919, respectively.

For  $q \equiv 7 \pmod{16}$  the first three gaps of k are 103, 311 and 487. The regular Hadamard matrices of corresponding orders are unknown as yet. This means that we cannot use the method given to find solutions for all cases.

# 3 Construct SBIBD from SDS and T-matrices

**Definition 4** (T-matrix) Let  $T_1, T_2, T_3, T_4$  be  $n \times n$  matrices with entries  $(0, \pm 1)$ . Then we call  $T_1, T_2, T_3, T_4$  T-matrices if

(i) 
$$T_i T_j = T_j T_i, \ 1 \le i, j \le 4,$$

- (ii) there exists an  $n \times n$  monomial matrix R with  $R^T = R$ ,  $R^2 = I_n$ , such that  $(T_iR)^T = T_iR$ , i = 1, 2, 3, 4,
- (iii) if  $T_i = (t_{jk}^{(i)})$ ,  $1 \le j, k \le n$ , i = 1, 2, 3, 4, then  $\sum_{i=1}^4 |t_{jk}^{(i)}| = 1$ ,  $i \le j, k \le n$ ,
- $(iv) \sum_{i=1}^4 T_i T_i^T = nI_n.$

We use conditions (i) and (ii) to replace the condition of circulant T-matrices. More details of T-matrices are discussed in [2]. In this paper we refer to the paper [10]. The following theorem will be useful for constructing SBIBD.

**Theorem 3** ([11]) If there exist  $4 - \{q^2; \frac{1}{2}q(q-1); q(q-2)\}$  SDS  $D_1$ ,  $D_2$ ,  $D_3$ ,  $D_4$  of order  $q^2$  in an abelian group G of order  $q^2$ , and every element of G appears an even number of times in  $D_1$ ,  $D_2$ ,  $D_3$ ,  $D_4$ , then there exist T-matrices  $T_1$ ,  $T_2$ ,  $T_3$ ,  $T_4$  that satisfy

$$\sigma(T_1) = q^3, \quad \sigma(T_2) = \sigma(T_3) = \sigma(T_4) = 0.$$
 (9)

For convenience we write the prime power  $q \equiv 4m+3=16n+7$ . Since the polynomial  $x^2+1$  is irreducible over GF(q), the set of all elements  $\alpha x+\beta$ ,  $\alpha$ ,  $\beta \in GF(q)$  modulo  $x^2+1$  is a finite field  $GF(q^2)$ . In the following we will employ this concrete representation of  $GF(q^2)$ .

We know that there exist T-matrices  $T_1$ ,  $T_2$ ,  $T_3$  and  $T_4$  of order  $q^2$  which satisfy (9) when  $q \equiv 3 \pmod{8}$  [10]. Another example of T-matrices satisfying (9) is as follows:

**Example 1** Let g = x + 1 in  $GF(5^2)$  and

$$C_i = \{g^{8j+i} \pmod{x^2 - 3, \mod 5} : j = 0, 1, 2\}, i = 0, 1, \dots, 7.$$

Take

$$\begin{array}{ll} D_1 = \{0\} \cup C_0 \cup C_1 \cup C_2, & D_2 = \{0\} \cup C_0 \cup C_1 \cup C_3, \\ D_3 = \{0\} \cup C_0 \cup C_2 \cup C_6, & D_4 = \{0\} \cup C_0 \cup C_3 \cup C_6. \end{array}$$

It is easy to verify that  $D_1$ ,  $D_2$ ,  $D_3$  and  $D_4$  defined above are  $4-\{25; 10; 15\}$  SDS and Theorem 3 holds for q=5. Consequently, there exist T-matrices of order 25 that satisfy (9).

**Theorem 4** Suppose  $D_1$ ,  $D_2$ ,  $D_3$  and  $D_4$  are  $4-\{k^2; \frac{1}{2}k(k-1); k(k-2)\}$  SDS such that

$$D_i = D_i^{-1}, \quad i = 1, 2, 3, 4.$$
 (10)

Then there exist  $SBIBD(4(kt)^2, 2(kt)^2 + kt, (kt)^2 + kt)$  where  $t^2$  is an order of T- matrices satisfying (9).

**Proof.** From Theorem 3 of [11] the theorem holds.

**Example 2** In  $GF(7^2)$  let g = x + 2 and set

$$S_i = \{g^{12j+i} \pmod{x^2+1}, \mod 7\}: j = 0, 1, 2, 3\}, i = 0, 1, \dots, 11.$$

Take

$$D_i = \{0\} \cup S_{3+3i} \cup S_{5+3i} \cup S_{6+3i} \cup S_{7+3i} \cup S_{9+3i}, \quad i = 0, 1, 2, 3.$$

It is easy to verify that  $D_0$ ,  $D_1$ ,  $D_2$  and  $D_3$  are 4-{49; 21; 35} SDS and  $D_i^{-1} = D_i$ , i = 0, 1, 2, 3.

From Theorem 3, Theorem 4, Example 1, and Example 2, we have the following corollaries.

**Corollary 2** There exist  $SBIBD(4k^2, 2k^2+k, k^2+k)$  for  $k=35, 5q_1$  and  $5q_2N$ , where  $q_1, q_2$  are prime powers, such that  $q_1 \equiv 1 \pmod{4}$ ,  $q_2 \equiv 5 \pmod{8}$ ,  $N=2^a 3^b t^2$ , where a, b=0 or 1 and  $t \neq 0$  any integer.

**Corollary 3** There exist  $SBIBD(4k^2, 2k^2 + k, k^2 + k)$  for  $k = 7q_3$  where  $q_3 = 3 \pmod{8}$  is a prime power.

# 4 Summary

# 4.1 Numerical results

**Example 3** In  $GF(47^2)$ , let g = x + 2 and set

$$C_i = \{g^{32j+i}: j = 0, \dots, 68\}, i = 0, \dots, 31,$$
  
 $E_i = \{g^{96j+i}: j = 0, \dots, 22\}, i = 0, \dots, 95.$ 

Write  $I_1 = \{0, 1, 3, 6, 8, 13, 15, 18, 28\}, I_2 = \{3, 5, 11, 12, 14, 15, 24, 25, 26\}$  and put

$$A_i = \bigcup_{j \in I_i} C_j, \quad B_i = \bigcup_j (E_j \cup E_{j+48}),$$

such that

$$A_i \cap B_i = \emptyset$$
 and  $|A_i| + |B_i| = 1081$ ,  $i = 1, 2$ .

Take  $D_i = A_i \cup B_i$  and  $D_{i+2} = g^8 D_i$ , i = 1, 2. Then  $D_1$ ,  $D_2$ ,  $D_3$  and  $D_4$  are 4- $\{2209; 1081; 2115\}$  SDS. Thus we can construct a regular Hadamard matrix of order 8836.

From Example 3, Corollary 1, 2 and 3, one can assert that there are 43 new values of k < 1000 for which there exist SBIBD( $4k^2, 2k^2 + k, k^2 + k$ ). They are 47, 71, 151, 167, 199, 263, 359, 439, 599, 631, 727, 919 (Corollary 1); 77(7 · 11), 133(7 · 19), 301(7 · 43), 413(7 · 59), 469(7 · 67), 581(7 · 83), 749(7 · 107), 917(7 · 131), 973(7 · 139) (Corollary 3); 265(5 · 53), 305(5 · 61), 365(5 · 73), 435(5 · 29 · 3), 445(5 · 89), 485(5 · 97), 505(5 · 101), 545(5 · 109), 555(5 · 37 · 3), 565(5 · 113), 585(5 · 13 · 9), 685(5 · 137), 745(5 · 149), 785(5 · 157), 795(5 · 53 · 3), 905(5 · 181), 915(5 · 61 · 3), 965(5 · 193), 985(5 · 197) (Corollary 2); 459(3^3 · 17) (Theorem 3 of [11]); 681(227 · 3), 825(11 · 3 · 5^2) (Proposition 6 of [11]).

The last three values of k were missed from the list of [11].

#### 4.2 Unknown cases

There are at most 126 values of k < 1000 for which the existence of SBIBD( $4k^2$ ,  $2k^2 + k$ ,  $k^2 + k$ ) is undetermined. These values are:

 $79,\ 103,\ 127,\ 141,\ 191,\ 209,\ 213,\ 217,\ 223,\ 231,\ 237,\ 239,\ 253,\ 255,\ 271,279,\ 309,\ 311,\ 329,\ 341,\ 355,\ 357,\ 367,\ 369,\ 377,\ 381,\ 383,\ 385,\ 395,\ 399,\ 403,\ 423,\ 425,\ 431,\ 437,\ 453,\ 455,\ 463,\ 465,\ 473,\ 479,\ 481,\ 483,\ 487,\ 493,\ 497,\ 501,\ 503,\ 515,\ 517,\ 527,\ 553,\ 561,\ 573,\ 589,\ 595,\ 597,\ 607,\ 611,\ 615,\ 627,\ 629,\ 635,\ 639,\ 647,\ 649,\ 651,\ 657,\ 663,\ 665,\ 669,\ 689,\ 693,\ 697,\ 705,\ 711,\ 713,\ 715,\ 717,\ 719,\ 721,\ 737,\ 743,\ 751,\ 755,\ 759,\ 765,\ 775,\ 781,\ 789,\ 793,\ 799,\ 801,\ 805,\ 813,\ 817,\ 823,\ 833,\ 835,\ 837,\ 839,\ 861,\ 863,\ 869,\ 873,\ 887,\ 889,\ 893,\ 899,\ 901,\ 903,\ 911,\ 913,\ 923,\ 927,\ 933,\ 935,\ 949,\ 955,\ 967,\ 969,\ 983,\ 987,\ 989,\ 991,\ 995.$ 

# Appendix

Although D in (5) contains A and B, the expression of  $\Delta D$  only depends on A and does not depend on the particular choice of B. So at first we can ignore B and just search A satisfying (8); then we can take B as in (4) satisfying (3).

Now put

$$C_i = \{g^{16j+i}: j = 0, 1, \cdots, (2n+1)(8n+3) - 1\}, i = 0, 1, \cdots, 15.$$

where g is a generator of  $GF(q^2)$ . It is clear that

$$C_i = \bigcup_{i=0}^{2n} E_{16j+i}, \quad i = 0, \dots, 15,$$

where  $E_i$  is defined in (2). The list of A is as follows:

 $q = 71, \ A = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_7, \ \text{where} \ g = x + 8.$ 

q = 151,  $A = C_0 \cup C_1 \cup C_2 \cup C_6 \cup C_{13}$ , where g = x + 9.

 $q = 167, A = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_7, \text{ where } g = x + 2.$ 

q = 199,  $A = C_0 \cup C_1 \cup C_5 \cup C_6 \cup C_{11}$ , where g = x + 13. q = 263,  $A = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_{12}$ , where q = x + 2.

q = 359,  $A = C_0 \cup C_1 \cup C_3 \cup C_6 \cup C_{13}$ , where q = x + 11.

q = 439,  $A = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_6 \cup C_7$ , where q = x + 9.

q = 599,  $A = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_7$ , where q = x + 11.

q = 631,  $A = C_0 \cup C_1 \cup C_3 \cup C_6 \cup C_{13}$ , where g = x + 5.

 $q = 727, \ \ A = C_0 \cup C_1 \cup C_2 \cup C_4 \cup C_7 \cup C_{13} \cup C_{14}, \ \text{where} \ g = x+2.$ 

q = 919,  $A = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_{12}$ , where g = x + 6.

Introducing cyclotomic classes  $C_i$ ,  $0 \le i < 16$  simplifies the procedure of searching for A in (5) satisfying (8) considerably. Further research will show this method is suitable to obtain more values of q which would lead to more new results.

# References

- [1] M. R. Best, The excess of a Hadamard matrix, Ind. Math. 39 (1977), 357–361.
- [2] G. Cohen, D. Rubie, C. Kouhouvinos, J. Seberry and M. Yamada, A survey of base sequences, disjoint complementary sequences and OD(4t; t, t, t, t), J. Combin. Math. Combin. Comp. 5 (1989), 69–104.
- [3] C. Koukouvinos, S. Koumias and J. Seberry, Further Hadamard matrices with maximal excess and new  $SBIBD(4k^2, 2k^2 + k, k^2 + k)$ , Utilitas Mathematica 36 (1989), 135–150.
- [4] S. Kounias and N. Farmakis, On the existence of Hadamard matrices with maximum excess, *Discrete Math.* 68 (1988), 59–69.
- [5] K. W. Schmidt, The weight of Hadamard matrices, J. Combin. Theory Ser. A 23 (1977), 257–263.
- [6] J. Seberry,  $SBIBD(4k^2, 2k^2 + k, k^2 + k)$  and Hadamard matrices of order  $4k^2$  with maximal excess are equivalent, Graphs and Combinatorics 5 (1989), 373–383.
- [7] J. Seberry, Existence of  $SBIBD(4k^2, 2k^2 \pm k, k^2 \pm k)$  and Hadamard matrices with maximal excess, Australas. J. Combin. 4 (1991), 87–91.
- [8] A. P. Street and D. J. Street, Combinatorics of Experimental Design, Oxford University Press, Oxford, 1987.
- [9] M. Xia and G. Liu, A new family of supplementary difference sets and Hadamard matrices, J. Statist. Plann. Inference 51 (1996), 283–291.
- [10] M. Xia and T. Xia, A family of C-partitions and T-matrices, J. Combin. Designs 7 (1999), 269–281.
- [11] Tianbing Xia, Mingyuan Xia and Jennifer Seberry, Regular Hadamard matrix, maximum excess and SBIBD, Australas. J. Combin. 27 (2003), 263–275.

(Received 25 Aug 2005)