A note on small defining sets for some SBIBD$(4t-1, 2t-1, t-1)$

Dinesh Sarvate
Department of Mathematics
College of Charleston
Charleston, SC,
USA

and

Jennifer Seberry*†
Department of Computer Science
The University of Wollongong
Wollongong, NSW, 2500
Australia

Abstract

We conjecture that p specified sets of p elements are enough to define an $SBIBD(2p+1, p, (p-1)/2)$ when $p \equiv 1 (mod\ 4)$ is a prime or prime power. This means in these cases p rows are enough to uniquely define the Hadamard matrix of order $2p+2$. We show that the p specified sets can be used to first find the residual $BIBD(p+1, 2p, p, (p+1)/2, (p-1)/2)$ for p prime or prime power. This can then be used to uniquely complete the $SBIBD$ for $p = 5, 9, 13$ and 17. This is another case where a residual design with $\lambda > 2$ is completable to an $SBIBD$, the first such case having been given by Seberry in "On small defining sets for some $SBIBD(4t-1, 2t-1, t-1)$", *Bull. ICA* 4:58-62, 1992.

We will refer to a design and its incidence matrix, with treatments as rows and blocks as columns, interchangeably.

Smallest defining sets have been studied by Gray [1, 2, 4] and minimal defining sets by Seberry [8]. Definitions are used from [9, 11, 12].

Let $D = \{d_1, d_2, \ldots, d_{2t}\}$ be the quadratic residues modulo $p = 4t+1 = q^r$ a prime power (we recall zero is neither a quadratic residue nor a quadratic nonresidue). Let

$$E = \{d_1, d_2, \ldots, d_{2t}, p, d_1+p, d_2+p, \ldots, d_{2t}+p\}.$$

Consider a Galois field $GF(q^r)$ with a primitive element x satisfying $g(x) = 0$. Now the elements of this field are integers or polynomials in x. The constant term in each element (polynomial) will be referred to as the *integer*. In the next description, in working with the first $2t$ elements of E, integers are reduced modulo q, $p = q^r$ so $q + i \equiv i (mod\ q)$, ie integers and coefficients remain in the range 0 to $q-1$.When working with the last $2t+1$ elements of E the integers (not coefficients) are reduced modulo q so $p + q + i \equiv p + i (mod\ q)$ and $p - j \equiv p + q - j (mod\ q)$ so coefficients remain in the range 0 to $q-1$ and integers in the range p to $p+q-1$.

We label the columns of a partial incidence matrix $0, 1, \ldots, q-1, x, x+1, \ldots, x+q-1, 2x, \ldots, 2x+q-1, \ldots, (q-1)(x^r-1)/(x-1), p, p+1, \ldots, p+q-$

*Written while on faculty at the Center for Communication and Information Science, the Department of Electrical Engineering and the Department of Computer Science and Engineering, University of Nebraska - Lincoln, NE 68588-0502, USA.

†Research funded by ARC grant A48830241 and an ATERB grant.

$1, p+x, \ldots, p+(q-1)(x^r-1)/(x-1)$, and the rows $0, 1, \ldots, q-1, x, \ldots, (q-1)(x^r-1)/(x-1)$.
Associate with each row label an index, g_i , $i = 0, 1, \ldots, q^r - 1$, and with each column label an index, f_j , $j = 0, 1, \ldots, 2q^r - 1$. We now define the sets $E_i, i = 0, 1, \ldots, q^r - 1$ by

$$E_i = \{f_j : (f_j - g_i)(mod\ g(x), mod\ p) \in E\},$$

as j runs from 0 to $2q^r - 1$.

1 The case p ≡ 1(mod 4)

Conjecture 1 *The $p = q^r, p \equiv 1(mod\ 4)$ a prime power, sets given by E_i, $i = 0, 1, \ldots, p-1$, are (minimal) defining sets for an $SBIBD(2p+1, p, (p-1)/2)$.*

We will show that the conjecture is true for $p = 5, 9, 13$ and 17.

Example. For $p = 5, D = \{1, 4\}$, there is no polynomial primitive element and $E = \{1, 4, 5, 6, 9\}$. Now $g_0 = 0, \ldots, g_4 = 4$, and $f_0 = 0, f_1 = 1, \ldots, f_9 = 9$. To find E_i we consider

$$f_0 - g_i, f_1 - g_i, \ldots, f_9 - g_i$$

and $f_j \in E_i$ if $f_j - g_i \in E$. Hence we have $E_0 = \{1, 4, 5, 6, 9\}$, $E_1 = \{2, 0, 6, 7, 5\}$, $E_2 = \{3, 1, 7, 8, 6\}$, $E_3 = \{4, 2, 8, 9, 7\}$, $E_4 = \{0, 3, 9, 5, 8\}$ where the first two elements are reduced modulo 5 to the range 0 to 4 and the last three elements are reduced modulo 5 to the range 5 to 9. □

Example.

For $p = 9 = 3^2$ and $x^2 = x + 1$ be the primitive polynomial, now $D = \{1, 2, x+1, 2x+2\}$ and $E = \{1, 2, x+1, 2x+2, 9, 10, 11, x+10, 2x+11\}$. Thus,

$g_0 = f_0 = 0$,	$g_6 = f_6 = 2x$,	$f_{12} = x + 9$,
$g_1 = f_1 = 1$,	$g_7 = f_7 = 2x + 1$,	$f_{13} = x + 10$,
$g_2 = f_2 = 2$,	$g_8 = f_8 = 2x + 2$,	$f_{14} = x + 11$,
$g_3 = f_3 = x$,	$f_9 = 9$,	$f_{15} = 2x + 9$,
$g_4 = f_4 = x + 1$,	$f_{10} = 10$,	$f_{16} = 2x + 10$,
$g_5 = f_5 = x + 2$,	$f_{11} = 11$,	$f_{17} = 2x + 11$.

To find E_i we consider

$$f_0 - g_i, f_1 - g_i, \ldots, f_{17} - g_i$$

and $f_j \in E_i$ if $f_j - g_i \in E$. Hence we have

$E_0 = \{1, 2, x+1, 2x+2, 9, 10, 11, x+10, 2x+11\}$,
$E_1 = \{2, 0, x+2, 2x, 10, 11, 9, x+11, 2x+9\}$,
$E_2 = \{0, 1, x, 2x+1, 11, 9, 10, x+9, 2x+10\}$,
$E_3 = \{x+1, x+2, 2x+1, 2, x+9, x+10, x+11, 2x+10, 11\}$,
$E_4 = \{x+2, x, 2x+2, 0, x+10, x+11, x+9, 2x+11, 9\}$,
$E_5 = \{x, x+1, 2x, 1, x+11, x+9, x+10, 2x+9, 10\}$,
$E_6 = \{2x+1, 2x+2, 1, x+2, 2x+9, 2x+10, 2x+11, 10, x+11\}$,
$E_7 = \{2x+2, 2x, 2, x, 2x+10, 2x+11, 2x+9, 11, x+9\}$,
$E_8 = \{2x, 2x+1, 0, x+1.2x+11, 2x+9, 2x+10, 9, x+12\}$.

where the first four elements are reduced modulo 3 to the range 0 to 2 and the last five elements have their coefficients in the range 0 to 2 and their integers in the range 9 to 11.

The incidence matrix is made using the labels $f_0, \ldots, f_{q^r-1}$. If $f_j \in E_i$, then the (i,j) element of the incidence matrix is 1, otherwise it is zero. Hence the incidence matrices for examples 1 and 2 are:

0	1	2	3	4	5	6	7	8	9
0	1	0	0	1	1	1	0	0	1
1	0	1	0	0	1	1	1	0	0
0	1	0	1	0	0	1	1	1	0
0	0	1	0	1	0	0	1	1	1
1	0	0	1	0	1	0	0	1	1

and, as the column labels are $0, 1, 2, x, x+1, x+2, \ldots$ the incidence matrix is:

0	1	2	x	x+1	x+2	$2x$			9	10	11	x+9			$2x$+9		
0	1	1	0	1	0	0	0	1	1	1	1	0	1	0	0	0	1
1	0	1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0
1	1	0	1	0	0	0	1	0	1	1	1	1	0	0	0	1	0
0	0	1	0	1	1	0	1	0	0	0	1	1	1	1	0	1	0
1	0	0	1	0	1	0	0	1	1	0	0	1	1	1	0	0	1
0	1	0	1	1	0	1	0	0	0	1	0	1	1	1	1	0	0
0	1	0	0	0	1	0	1	1	0	1	0	0	0	1	1	1	1
0	0	1	1	0	0	1	0	1	0	0	1	1	0	0	1	1	1
1	0	0	0	1	0	1	1	0	1	0	0	0	1	0	1	1	1

(note for space reasons not all the labels in the first row are given). □

Lemma 1 *The incidence matrix of* $E_0, \ldots, E_{p-1}$ *and* $E_p = \{0, 1, \ldots, q-1, x, \ldots, (q-1)(x^r-1)/(x-1)\}$ *is a* $BIBD(p+1, 2p, p, (p+1)/2, (p-1)/2)$.

Proof. The dimensions, the row sum and the column sum are by construction.

Now the nature of the construction shows that the first p columns of the incidence matrix will have $(p-1)/2 = 2t$ elements and the last $p+1$ columns will have $(p+1)/2 = 2t+1$ elements as the elements of a Galois field are an additive group and as we run through all g_i the number of times $f_j - g_i \in D$ for fixed j is $|D| = 2t$.

It remains to discuss the inner product of the rows. For the last row, from E_p, the intersection is correct by construction.

The first p rows can be divided into the first and last p columns. They are the incidence matrices of the quadratic residues (the matrix in the 0 to $(p-1)$st rows and the 0th to $(p-1)$st columns) and the quadratic residues with 0 in the pth to $(2p-1)$st columns. These sets are known [9] to give $2-\{p; (p-1)/2, (p+1)/2, (p-1)/2\}$ supplementary different sets and so we have the correct innerproduct. □

Conjecture 2 *The sets given in the last Lemma always form the residual design of an* $SBIBD(2p+1, p, (p-1)/2)$.

Lemma 2 *The sets for $p = 5$ can be uniquely extended to an $SBIBD(11,5,2)$.*

Proof. Straightforward use of the properties of an $SBIBD$.

Lemma 3 *The sets given for $p = 9$ can be uniquely extended to a symmetric $SBIBD(19,9,4)$.*

Proof. A search was made for all possible 11th rows to complete the design and exactly nine possibilities were found. These nine rows gave the following $SBIBD(19,9,4)$:

0	0	1	1	0	1	0	0	0	1	1	1	1	0	1	0	0	1
0	1	0	1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0
0	1	1	0	1	0	0	0	1	0	1	1	1	1	0	0	0	1	0
0	0	0	1	0	1	1	0	1	0	0	0	1	1	1	1	0	1	0
0	1	0	0	1	0	1	0	0	1	1	0	0	1	1	1	0	0	1
0	0	1	0	1	1	0	1	0	0	0	1	0	1	1	1	1	0	0
0	0	1	0	0	0	1	0	1	1	0	1	0	0	0	1	1	1	1
0	0	0	1	1	0	0	1	0	1	0	0	1	1	0	0	1	1	1
0	1	0	0	0	1	0	1	1	0	1	0	0	0	1	0	1	1	1
0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	1	0	1	1	1	0	1	0	0	0	1	0
1	0	0	0	1	0	1	1	1	0	0	1	1	0	1	0	0	0	1
1	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1	1	0	0
1	0	1	1	0	0	0	1	1	0	1	0	0	1	0	1	0	0	1
1	0	1	1	1	0	1	0	0	0	1	0	0	0	1	0	1	1	0
1	1	0	1	0	0	0	0	1	1	0	1	0	1	1	0	1	0	0
1	1	0	1	1	1	0	0	0	0	0	1	0	0	0	1	0	1	1
1	1	1	0	0	0	0	1	0	1	0	0	1	0	1	1	0	1	0
1	1	1	0	0	1	1	0	0	0	0	0	1	1	0	0	1	0	1

□

The expanded version of the incidence matrix of the $SBIBD(19,9,4)$ found during the construction is row and column permutation equivalent to:

0	e_3	e_3	e_3	0_3	0_3	0_3
0_3^T	J-I	I	I	J	I	I
0_3^T	I	J-I	I	I	J	I
0_3^T	I	I	J-I	I	I	J
e_3^T	0	J-I	J-I	J-I	I	I
e_3^T	J-I	0	J-I	I	J-I	I
e_3^T	J-I	J-I	0	I	I	J-I

or

0	0	1	1	1	0	0	1	0	0	1	1	1	1	0	0	1	0	0
0	1	0	1	0	1	0	0	1	0	1	1	1	0	1	0	0	1	0
0	1	1	0	0	0	1	0	0	1	1	1	1	0	0	1	0	0	1
0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	1	1	0	0
0	0	1	0	1	0	1	0	1	0	0	1	0	1	1	1	0	1	0
0	0	0	1	1	1	0	0	0	1	0	0	1	1	1	1	0	0	1
0	1	0	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	1
0	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0	1	1	1
0	0	0	1	0	0	1	1	1	0	0	0	1	0	0	1	1	1	1
0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	0	1	1	0	1	1	1	0	0	1	0	0
1	0	0	0	1	0	1	1	0	1	1	0	1	0	1	0	0	1	0
1	0	0	0	1	1	0	1	1	0	1	1	0	0	0	1	0	0	1
1	0	1	1	0	0	0	0	1	1	1	0	0	0	1	1	1	0	0
1	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	1	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	1
1	0	1	1	0	1	1	0	0	0	1	0	0	1	0	0	0	1	1
1	1	0	1	1	0	1	0	0	0	0	1	0	0	1	0	1	0	1
1	1	1	0	1	1	0	0	0	0	0	0	1	0	0	1	1	1	0

A similar computer search has verified that:

Lemma 4 *The sets given by the conjecture for $p = 13$ and 17 can be uniquely extended to symmetric $SBIBD(27,13,6)$ and $SBIBD(35,17,8)$.*

2 The case p ≡3(mod 4)

Seberry [8] gave a conjecture for primes $4t - 1 \equiv 3(mod\ 4)$ and showed the conjecture is true for $t = 2,3,5$. Subsequently Gower [7] showed the conjecture is true for $t = 6$. We now extend the conjecture of that paper to the case of prime powers.

Conjecture 3 *Let $D = \{d_1, d_2, \ldots, d_{2t-1}\}$ be the quadratic residues modulo $p = 4t - 1 \equiv 3(mod\ 4)$ a prime power. Let x satisfy a primitive polynomial. Write the elements of $GF(p)$ in additive notation as $g_1, g_2, \ldots, g_p$. Define $E_i = \{g_j : g_j - x^i \in D, i$ fixed, $j = 1, \ldots, p, x \in D\}$ for $i = 1, \ldots, 2t-1$. Then we claim the sets $E_1, \ldots, E_{2t-1}, D$ are the residual design of an $SBIBD(4t-1, 2t-1, t-1)$.*

Conjecture 4 *Suppose $4t-1$ is a prime power. Then the sets $E_1, \ldots, E_{2t-1}$ just defined can be extended, uniquely, up to permutation of treatments using the link property of blocks of an $SBIBD$ to form an $SBIBD(4t-1, 2t-1, t-1)$.*

Example. If $p \equiv 3(mod\ 4) = 3^3$ with primitive root x satisfying $x^3 = x + 2$ we have $D = \{1, 2x, 2x+1, 2x+2, x^2, x^2+2, x^2+x, x^2+x+1, x^2+2x, x^2+2x+1, 2x^2+2, 2x^2+x+1, 2x^2+2x+1\}$. With the elements of $GF(3^3)$ written as $g_1, \ldots, g_{27}$ for example $g_4 = x^4 = x^2 + 2x$, and $E_4 = \{g_j : g_j - x^4 \in D\} = \{g_j : g_j - x^2 - 2x \in D\} = \{x^2+2x+1, x^2+x, x^2+x+1, x^2+x+2, 2x^2+2x, 2x^2+2x+2, 2x^2, 2x^2+1, 2x^2+2, 2x^2+x, 2x^2+x+1, 2x+2, 1, x+1.\}$ Then we claim $E_1, \ldots, E_{13}, D$ give a residual design of the $SBIBD(27,13,6)$ and can be uniquely extended to that design.

We give another, simpler proof of Lemma 2 of [8]:

Lemma 5 *Suppose $4t-1$ is a prime power. Then the sets $E_1, E_2, \ldots, E_{2t-1}$ defined above can be completed to the residual design $BIBD(2t, 4t-1, 2t-1, t, t-1)$ of an $SBIBD(4t-1, 2t-1, t-1)$.*

Proof. Since $4t-1$ cannot be written as the sum of two squares, the sets $E_1, E_2, \ldots, E_{2t-1}$ do not contain the zero element and are therefore subsets of the set of $4t-2$ nonzero elements. We write down A, the $2t-1 \times 4t-2$ incidence matrix of the E_is.

From the construction of the $SBIBD(4t-1, 2t-1, t-1)$ based on the quadratic residues, we know that these sets form part of an $SBIBD$ generated from D. In this $SBIBD$, $| E_i \cap D | = t-1$ for each i, and the elements in this intersection must be quadratic residues as D contains only quadratic residues. Hence each E_i consists of $t-1$ quadratic residues and t quadratic non-residues. Thus in the incidence matrix A, in each column corresponding to a quadratic non-residue there will be t ones, and since there are $2t-1$ quadratic non-residues, these columns contain altogether $t(2t-1)$ ones in A. Similarly, in each column corresponding to a quadratic residue there will be $t-1$ ones, and since there are $2t-1$ quadratic residues, these columns contain altogether $(t-1)(2t-1)$ ones in A. This shows A contains $(2t-1)^2$ ones.

A may be interpreted in two ways: first, as the incidence matrix of the first $2t-1$ blocks of an $SBIBD(4t-1, 2t-1, t-1)$, where each row corresponds to a block; second, as the incidence matrix of the first $2t-1$ elements of a $BIBD(2t, 4t-1, 2t-1, t, t-1)$, where each column corresponds either to a block or to a block with one element missing.

Now if we wish to extend each block to form the $BIBD(2t, 4t-1, 2t-1, t, t-1)$, or in other words, to adjoin one extra row to the matrix A to form the incidence matrix B of such a design, we must place one extra one in each of the columns which corresponds to a quadratic residue. The number of ones in this additional row must be the difference between the number of ones in B and the number already present in A, that is $2t(2t-1) - (2t-1)^2 = 2t-1$ precisely.

Thus the extra row is simply the incidence vector of D, and as already noted D intersects each E_i in precisely $t-1$ elements. □

We see that a similar result is not true for twin prime power difference sets. Indeed Gray and Street [5] indicate that the smallest defining set for an $SBIBD(15, 7, 3)$ contains nine blocks. The next example shows why twin prime powers are radically different.

Example.

Consider the difference set $D = \{(0,0), (1,0), (2,0), (1,1), (1,4), (2,2), (2,3)\}$ to generate a $(15, 7, 3)$ design. As $(0,0)$ is in the difference set, $(0,0) + D$ is D again.

Acknowledgement. The authors would like to thank the referee for many useful comments.

References

[1] Ken Gray, Further results on smallest defining sets of well known designs, *Australas. J. Combinatorics* 1:91–100, 1990.

[2] Ken Gray, On the minimum number of blocks defining a design, *Bull. Austral. Math. Soc.* 41:97–112, 1990.

[3] Ken Gray, Defining sets of single-transposition-free designs, *Utilitas Math.* 38:97–103, 1990.

[4] Ken Gray, *Special Subsets of the Block Sets of Designs*, Ph.D. Thesis, University of Queensland, 1990.

[5] Ken Gray and Anne Penfold Street, e-mail communication to Jennifer Seberry, July 1992.

[6] A. V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel, 1979.

[7] Rebecca Gower, e-mail communication to Jennifer Seberry, Nov 1991.

[8] Jennifer Seberry, On small defining sets for some $SBIBD(4t-1, 2t-1, t-1)$, *Bull. ICA*, 4:58–62, 1992; corrigendum, *Bull. ICA*, 6:62, 1992.

[9] Jennifer Seberry Wallis, Hadamard matrices, Part IV, *Combinatorics: Room Squares, Sum free sets and Hadamard Matrices*, Lecture Notes in Mathematics, Vol 292, eds. W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[10] Jennifer Seberry Wallis, Some remarks on supplementary differences sets, *Coll. Math. Soc. Janos Bolyai*, B10:1503-1526, 1973.

[11] Thomas Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham, Chicago, 1967.

[12] T. Tsuzuku, *Finite Groups and Finite Geometries*, Cambridge University Press, Cambridge, 1982.