On small defining sets for some SBIBD$(4t-1, 2t-1, t-1)$

Jennifer Seberry

Department of Computer Science
The University of New South Wales
Australian Defence Force Academy
Canberra ACT 2600
AUSTRALIA

Abstract

We conjecture that $2t-1$ specified sets of $2t-1$ elements are enough to define an SBIBD$(4t-1, 2t-1, t-1)$ when $4t-1$ is a prime or product of twin primes. This means that in these cases $2t-1$ rows are enough to uniquely define the Hadamard matrix of order $4t$.

We show that the $2t-1$ specified sets can be used to first find the residual BIBD$(2t, 4t-2, 2t-1, t, t-1)$ for $4t-1$ prime. This can then be uniquely used to complete the SBIBD for $t = 1, 2, 3, 5$.

This is remarkable as formerly only residual designs with $\lambda = 1$ or 2 have been completable to SBIBD.

We note that not any set of elements will do as Marshall Hall Jr found 13 sets from 19 which could not be completed to an $(19, 9, 4)$.

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

Conjecture 1 *Let D be the quadratic residues modulo a prime power $4t-1$. Then the residual design with treatments given by the sets $D, D+d_1, \ldots, D+d_{2t-1}, d_i \in D, i = 1, \ldots, 2t-1$ can be extended, uniquely, up to permutation of treatments using the link property of blocks of an SBIBD (inner product of the columns) to form an SBIBD$(4t-1, 2t-1, t-1)$.*

Theorem 2 *The conjecture is true for $t = 2, 3, 5$.*

1 Properties of given sets

Write $E_i = D + d_i$, $i = 1, \ldots, 2t-1$ where D is the set of quadratic residues modulo $4t-1$.

Lemma 1 $0 \notin D_i$ *for any* $i = 1, \ldots, 2t-1$.

Proof. The elements of E_i are $d_j + d_i$ where $d_j, d_i \in D$ are both quadratic residues. If $d_j + d_i = 0$ for some j, i then $d_j = -d_i$, that is, a quadratic residue equals a quadratic non residue. This is not possible for primes $4t-1$. □

We note from cyclotomy, writing D for the set of quadratic residues, N for the set of quadratic non residues and ΔD, ΔN for the collection of distinct differences between elements of D and N respectively, that

$$\Delta D = \Delta N = (t-1)(V/\{0\})$$

where V is the elements of GF$(4t-1)$. $V = D \cup N \cup \{0\}$. Also

$$\begin{aligned} \Delta(D-N) &= (t-1)D + tN \\ \Delta(N-D) &= tD + (t-1)N \end{aligned} \qquad (1)$$

where $\Delta(A-B)$ is the collection of elements $[a-b : a \in A, b \in B]$. □

Lemma 2 $E_1, E_2, ..., E_{2t-1}$ *can be completed to be the residual design BIBD*$(2t, 4t-2, 2t-1, t, t-1)$ *of an SBIBD*$(4t-1, 2t-1, t-1)$.

Proof. Since the sets $E_i, i = 1, ..., 2t-1$ do not contain 0 they are defined on a set of size $4t-2$. Clearly they each contain $2t-1$ elements. We write down the 0,1 incidence matrix of the sets E_i and obtain a $(2t-1) \times (4t-2)$ matrix, A, with $2t-1$ ones per row. We will now show A has t or $t-1$ elements per column and inner product between its rows exactly $t-1$.

We first show that in those columns of A which represent a quadratic residue in some E_i there are $t-1$ ones and in those which represent a quadratic non residue there are t ones. Let d_h be a quadratic residue then we ask how many times is $d_i + d_j = d_h, d_i, d_j \in D$. That is, how many times is $d_j = d_h - d_i$ for fixed d_j. Since D is the set of quadratic residues the equation $d_j = d_h - d_i$ has $t-1$ solutions for fixed d_j. Hence the column of A which represents d_j has $t-1$ ones.

Next we consider the number of solutions of the equation $d_j = -d_h$ where $(-d_h)$ is a quadratic non residue. That is, how many solutions are there to the equation $d_j = (-d_h) - d_i$, that is, the differences between a non residue and a residue should be a residue. Equation (1) from the theory of cyclotomy shows there are t solutions.

We thus observe that if we add another row to A which is 1 in the columns representing the quadratic residues we will have added the representation of D and have a new matrix B which is $2t \times (4t-2)$, has $2t-1$ ones per row and t ones per column.

To show B is the required BIBD we need to show that $|E_j \cap E_h| = |E_j \cap D| = t-1$ for $j, h = 1, ..., 2t-1$. We first consider $|E_j \cap D|$. Thus we want to know how many times an element $d_j + d_h \in D_j$ equals $d_i \in D$, $i \neq h$. However, $d_i - d_h = d_j$ for fixed d_j and $d_i \in \{d_1, ..., d_{2t-1}\}$ has $t-1$ solutions. Hence $|E_j \cap D| = t-1$. For $|E_j \cap E_h|$ we need $d_x + d_j = d_y + d_h$, that is, the number of times $w = d_j - d_h = d_y - d_x$ has a solution for fixed d_j, d_h and this is again $t-1$.

Thus we have the required residual design BIBD$(2t, 4t-2, 2t-1, t, t-1)$. □

Example. The sets $D = \{0,1,2,4,5,8,10\}$, $D+1$, $D+2$, $D+4$, $D+5$, $D+8$, $D+10$ are defining sets for an SBIBD$(15,7,3)$.

Example. The 7 sets:

0	1	2	4	5	8	10
1	2	3	5	6	9	11
2	3	4	6	7	10	12
4	5	6	8	9	12	14
5	6	7	9	10	13	0
8	9	10	12	13	1	3
10	11	12	14	0	3	5

Example. Let $D = \{d_1, d_2, ..., d_{2t-1}\}$ be the quadratic residues. Then $D + d_i$, $i = 1, 2, ..., 2t-1$ are defining sets modulo $4t-1$, which can be uniquely completed to SBIBD$(4t-1, 2t-1, t-1)$ and an Hadamard matrix of order $4t$ (up to permutation of rows) for $t = 2, 3, 5$.

Case $t = 2$: The sets are $\{2,3,5\}$, $\{3,4,6\}$, $\{5,6,1\}$. Let us write them as a $(0,1)$ incidence matrix giving:

0	1	2	3	4	5	6
		1	1		1	
			1	1		1
	1				1	1

Using the fact that an SBIBD is a linked design, so each column has three ones and without loss of generality the first column is $(0,0,0,0,1,1,1)^T$, each other column has one 1 in the last three rows, we see we can uniquely complete the fourth row so in each column we have a total of $2t-1 = 3$ ones. So we have:

0	1	2	3	4	5	6
		1	1		1	
			1	1		1
	1				1	1
0	1	1		1		
1						
1						
1						

Note the fourth row is the incidence matrix of D the set of quadratic residues and the first $2t = 4$ rows and $4t-2 = 6$ columns is the incidence matrix of the residual BIBD$(4, 6, 3, 2, 1)$.

Without loss of generality we choose the $(5,1) = (6,2)$ elements one. The inner products of the rows and columns now uniquely complete the design.

Case $t = 3$: Let $D = \{1, 3, 4, 5, 9\}$ be the quadratic residues modulo 11. Then $D + d_i$, $d_i \in D$, $i = 1, ..., 5$ are defining sets giving, as before with D the residual design BIBD$(5,10,4,3,2) = H$:

$H =$

0	1	2	3	4	5	6	7	8	9	10
		1		1	1	1				1
	1			1		1	1	1		
		1			1		1	1	1	
			1			1		1	1	1
	1	1	1				1			1
	1		1	1	1				1	
1	1	1				1			1	0
1	1				1			1		1
1		1	1	1				1		0
1			1		1	1	1	0	0	0
1				1			1	0	1	1

The first three columns are easily completed (up to permutation of rows) and the inner product of the rows and columns, as well as the row and column sums, fix the remainder.

Case $t = 5$: Let D be the quadratic residues and as before use the sets $D + d_i$, $i = 1,...,9$, $d_i \in D$. Again form the incidence matrix and note that without loss of generality the first column can be written as $2t$ zeros and $2t - 1$ ones in the $2t + 1$ to $4t - 1$ places. The fact that the SBIBD$(19,9,4)$ is a linked design means each of the last $2t - 1$ rows has $t - 1 = 4$ ones per column means the $2t$th row can be uniquely completed to give a total of $2t - 1$ ones in each column of the design. Again the $2t$th column is the incidence matrix of D the set of quadratic residues.

Note the $2t \times (4t - 2)$ matrix, which is the first $2t$ rows and the last $4t - 2$ columns, is the residual BIBD$(2t, 4t - 2, 2t - 1, t, t - 1)$.

It now remains to show the design can be uniquely completed.

We have:

$H =$

0	1	2	3	4	5	6	7	8	9	A	B	C	E	F	G	H	I	J
		1			1	1	1	1		1		1					1	1
	1	1			1			1	1	1	1		1		1			
		1	1			1			1	1	1	1		1		1		
			1	1			1			1	1	1	1		1		1	
				1	1			1			1	1	1	1		1		1
	1					1	1			1			1	1	1	1		1
	1		1					1	1			1			1	1	1	1
	1	1	1	1		1		1					1	1			1	
		1	1	1	1		1		1					1	1			1
	1			1	1	1	1		1		1					1	1	

$K =$

0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*E*	*F*	*G*	*H*	*I*	*J*
1	1	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1
1	1	1	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0
1	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1
1	1	0	0	1	0	0	1	1	1	1	0	1	0	1	0	0	0	0
1		1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1	1
1		1	0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	0
1			0	0	1	1	0	0	1	0	0	1	1	1	1	0	1	0
1			1	1	1	1	0	1	0	1	0	0	0	0	1	1	0	0
1		0	1	0	0	1	1	1	1	0	1	0	1	0	0	0	0	1

Again we have unique completion up to permutation of rows.

References

[1] M. Hall Jr. Private communication, 1977.

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

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

[4] Ken Gray. *Special Subsets of the Block Sets of Designs.* PhD thesis, University of Queensland, 1990.

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

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

[7] J.S. Wallis. Hadamard matrices. In *Combinatorics: Room Squares, sum-free sets and Hadamard matrices*, volume 292 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin-Heidelberg-New York, 1972. Part IV of W.D. Wallis, Anne Penfold Street, and Jennifer Seberry Wallis.