On symmetric designs and binary 3-frameproof codes

Chuan Guo[1], Douglas R. Stinson[1⋆], and Tran van Trung[2]

[1] David R. Cheriton School of Computer Science, University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
[2] Institut für Experimentelle Mathematik, Universität Duisburg-Essen
Ellernstrasse 29, 45326 Essen, Germany

Abstract. In this paper, we study when the incidence matrix of a symmetric (v, k, λ)-BIBD is a 3-frameproof code. We show the existence of infinite families of symmetric BIBDs that are 3-frameproof codes, as well as infinite families of symmetric BIBDs that are not 3-frameproof codes.

1 Introduction

Frameproof codes were introduced by Boneh and Shaw [2] as a method for digital rights control. Given a finite set Q and a positive integer N, let $C \subseteq Q^N$ be a finite set of length N codewords from the alphabet set Q. C is called a (N, n, q) code if $|C| = n$ and $|Q| = q$. The elements of C are called codewords, with each codeword of the form $x = (x_1, x_2, \ldots, x_N)$ where $x_i \in Q$ for all i. C is called a w-frameproof code if no coalition of size at most w can construct a codeword not belonging to the coalition, and hence cannot frame the holder of the codeword.

Formally, the coalition is a subset $P \subseteq C$ of w codewords. To construct a new codeword, for $1 \leq i \leq N$, the coalition may select any available alphabet element a_i from a codeword $a \in P$ and insert it into position i of the new codeword. The set of possible new codewords is $\mathrm{desc}(P) = \{x \in Q^N : x_i \in \{a_i : a \in P\}, 1 \leq i \leq N\}$. Using this definition, a code C is w-frameproof if for any $P \subseteq C$, $|P| \leq w$, we have $\mathrm{desc}(P) \cap C = P$.

The condition for C to be a frameproof code has been shown to be equivalent to a certain type of separating hash families. Let X, Y be finite sets and let $\mathcal{H}$ be a set of functions from X to Y. For pairwise disjoint subsets $C_1, C_2, \ldots, C_t \subseteq X$, we say that $h \in \mathcal{H}$ separates $C_1, C_2, \ldots, C_t$ if $h(C_1), h(C_2), \ldots, h(C_t) \subseteq Y$ are also pairwise disjoint. If some $h \in \mathcal{H}$ separates $C_1, C_2, \ldots, C_t$ for every choice of $C_1, C_2, \ldots, C_t$ with $|C_i| = w_i$ for fixed integers w_i, $i = 1, \ldots, N$, we say that $\mathcal{H}$ is a $(N; n, q, \{w_1, w_2, \ldots, w_t\})$-separating hash family (denoted $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$), where $N = |\mathcal{H}|$, $n = |X|$, $q = |Y|$. (N, n, q)

⋆ D. Stinson's research is supported by NSERC discovery grant 203114-11.

w-frameproof codes are equivalent to $\mathsf{SHF}(N; n, q, \{1, w\})$ [13], and it is usually easier to study frameproof codes in terms of the equivalent separating hash family.

Given an $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$, we may represent it as an $N \times n$ matrix with entries $1, \ldots, q$. The rows are indexed by $\mathcal{H}$ and the columns are indexed by X. The value of $h(x)$ is the entry in the matrix at row h and column x. An $N \times n$ matrix A with entries $1, \ldots, q$ is the representation matrix of an $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$ if and only if for every pairwise disjoint set of columns $C_1, C_2, \ldots, C_t$ with $|C_i| = w_i$, $i = 1, \ldots, N$, there exists a row h such that $\{A(h, x) : x \in C_i\} \cap \{A(h, x) : x \in C_j\} = \emptyset$ for every $i \neq j$.

It is easy to see that a permutation matrix of order N always gives an $\mathsf{SHF}(N; N, 2, \{1, w\})$ for any w. In [9], it was shown that for $w \geq 3$, if $N \leq 3w$ then $\mathsf{SHF}(N; n, 2, \{1, w\})$ exists if and only if $n \leq N$ and permutation matrices are the only examples of $\mathsf{SHF}(N; N, 2, \{1, w\})$ up to exchanging 0s and 1s in each row independently. One interesting question is finding examples of $\mathsf{SHF}(N; N, 2, \{1, w\})$ with $N > 3w$ that are not permutation matrices. In this paper, we will explore the option of using symmetric BIBDs to provide such examples.

The rest of the paper is organized as follows. In Section 2, we mention some previous results. Section 3 contains our main results. First we give a parametric and structural characterization of symmetric BIBDs that are 3-frameproof codes. In Section 3.1, we study the case of Hadamard designs in detail, and Section 3.2 addresses designs with $k = 3\lambda$. We consider "small" designs in Section 3.3 and we construct a table of existence and nonexistence results. Finally, Section 4 contains a couple of additional results and some open problems.

2 Previous Results

Connections between BIBDs and SHFs have previously been discovered. Type $\{1, w\}$ SHFs can be derived from t-designs – a more general form of combinatorial designs. A t-(v, k, λ) design is a set system $(X, \mathcal{B})$ where X is a finite set and $\mathcal{B}$ is a set of subsets of X satisfying

(i) $|X| = v$,
(ii) $|B| = k$ for every $B \in \mathcal{B}$, and
(iii) for every $Y \subseteq X$, $|Y| = t$, there exist $B_1, B_2, \ldots, B_\lambda \in \mathcal{B}$ distinct such that $Y \subseteq B_i$ for $i = 1, \ldots, \lambda$.

The elements of X are called points and the elements of $\mathcal{B}$ are called blocks. In the special case that $t = 2$, we call the design a (v, k, λ)-BIBD (balanced incomplete block design). The number of blocks of the design is $b = |\mathcal{B}|$, and is related to the parameters of the design by $bk = vr$, where $r = \frac{\lambda(v-1)}{k-1}$ is the number of blocks each point is contained in. If $v = b$, the design is called a

symmetric BIBD. One family of symmetric BIBDs is the projective planes with $v = q^2 + q + 1$, $k = q + 1$ and $\lambda = 1$, where q is a prime power.

It is often useful to represent a t-design using a binary matrix. Given a t-(v, k, λ) design $(X, \mathcal{B})$, its *point-block incidence matrix* is the $v \times b$ binary matrix A with rows indexed by X and columns indexed by $\mathcal{B}$, with $\mathsf{A}(x, B) = 1$ if and only if $x \in B$. The *block-point incidence matrix* is the transpose of the point-block incidence matrix. The following theorem gives a construction for SHFs from t-designs.

Theorem 1. *[14] Let $(X, \mathcal{B})$ be a t-$(v, k, 1)$ design. The point-block incidence matrix of $(X, \mathcal{B})$ is an $\mathsf{SHF}(v; b, 2, \{1, w\})$ where $b = \binom{v}{t}/\binom{k}{t}$ is the number of blocks and $w = \lfloor \frac{k-1}{t-1} \rfloor$.*

For $t = 2$, this result shows that all members of the projective plane family of designs is an $\mathsf{SHF}(v; v, 2, \{1, w\})$ for $w = k - 1$.

3 Binary Frameproof Codes

In this section, we give a characterization of $\mathsf{SHF}(v; v, 2, \{1, 3\})$ for all symmetric (v, k, λ)-BIBDs.

Theorem 2. *Let $(X, \mathcal{B})$ be a symmetric (v, k, λ)-BIBD and let A be its block-point incidence matrix. If $k \geq 3\lambda+1$ or if $k-\lambda$ is odd then A is an $\mathsf{SHF}(v; v, 2, \{1, 3\})$.*

Proof. Suppose that A is not an $\mathsf{SHF}(v; v, 2, \{1, 3\})$, then there exists some column set pair $(\{\mathsf{x}\}, \{\mathsf{u}, \mathsf{v}, \mathsf{w}\})$ that cannot be separated. For each $Z \subseteq \{\mathsf{u}, \mathsf{v}, \mathsf{w}\}$, partition $\mathcal{B}$ into subsets $\mathcal{A}_Z$ where $\mathcal{A}_Z = \{B \in \mathcal{B} : B \cap \{\mathsf{u}, \mathsf{v}, \mathsf{w}\} = Z\}$, and let $a_Z = |\mathcal{A}_Z|$. We obtain the following set of equations from $(X, \mathcal{B})$ being a symmetric (v, k, λ)-BIBD:

$$a_\emptyset + a_\mathsf{u} + a_\mathsf{v} + a_\mathsf{w} + a_\mathsf{uv} + a_\mathsf{vw} + a_\mathsf{uw} + a_\mathsf{uvw} = v \tag{3.1}$$
$$a_\mathsf{u} + a_\mathsf{uv} + a_\mathsf{uw} + a_\mathsf{uvw} = k \tag{3.2}$$
$$a_\mathsf{v} + a_\mathsf{uv} + a_\mathsf{vw} + a_\mathsf{uvw} = k \tag{3.3}$$
$$a_\mathsf{w} + a_\mathsf{uw} + a_\mathsf{vw} + a_\mathsf{uvw} = k \tag{3.4}$$
$$a_\mathsf{uv} + a_\mathsf{uvw} = \lambda \tag{3.5}$$
$$a_\mathsf{vw} + a_\mathsf{uvw} = \lambda \tag{3.6}$$
$$a_\mathsf{uw} + a_\mathsf{uvw} = \lambda \tag{3.7}$$

Letting $\alpha = a_\mathsf{uvw}$, we get that

$$\begin{aligned} a_\mathsf{uv} = a_\mathsf{vw} = a_\mathsf{uw} &= \lambda - \alpha \\ a_\mathsf{u} = a_\mathsf{v} = a_\mathsf{w} &= k - 2(\lambda - \alpha) - \alpha \\ &= k + \alpha - 2\lambda. \end{aligned}$$

Next, define $\mathcal{B}_Z = \{B \in \mathcal{A}_Z : \mathsf{x} \in B\}$ and let $b_Z = |\mathcal{B}_Z|$. We obtain another set of equations:

$$b_\emptyset + b_\mathsf{u} + b_\mathsf{v} + b_\mathsf{w} + b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uw} + b_\mathsf{uvw} = k \tag{3.8}$$
$$b_\mathsf{u} + b_\mathsf{uv} + b_\mathsf{uw} + b_\mathsf{uvw} = \lambda \tag{3.9}$$
$$b_\mathsf{v} + b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uvw} = \lambda \tag{3.10}$$
$$b_\mathsf{w} + b_\mathsf{uw} + b_\mathsf{vw} + b_\mathsf{uvw} = \lambda \tag{3.11}$$

Note that for every Z, we get $0 \leq b_Z \leq a_Z$. It is clear that the column set pair $(\{\mathsf{x}\}, \{\mathsf{u}, \mathsf{v}, \mathsf{w}\})$ cannot be separated if and only if $b_\emptyset = 0$ and $b_\mathsf{uvw} = \alpha$. Thus equations (3.8) – (3.11) simplify to

$$b_\mathsf{u} + b_\mathsf{v} + b_\mathsf{w} + b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uw} = k - \alpha \tag{3.12}$$
$$b_\mathsf{u} + b_\mathsf{v} + b_\mathsf{w} + 2(b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uw}) = 3(\lambda - \alpha) \tag{3.13}$$

Subtracting (3.12) from (3.13) gives

$$b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uw} = 3\lambda - k - 2\alpha. \tag{3.14}$$

Since $b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uw} \geq 0$, (3.14) implies that

$$0 \leq 3\lambda - k - 2\alpha. \tag{3.15}$$

Now, since $\alpha \geq 0$, we see from (3.15) that $k \leq 3\lambda$. Therefore A is an $\mathsf{SHF}(v; v, 2, \{1, 3\})$ if $k \geq 3\lambda + 1$.

Next, we multiply (3.12) by 2 and subtract (3.13), giving

$$b_\mathsf{u} + b_\mathsf{v} + b_\mathsf{w} = \alpha + 2k - 3\lambda. \tag{3.16}$$

Then we have

$$3(k + \alpha - 2\lambda) = a_\mathsf{u} + a_\mathsf{v} + a_\mathsf{w} \geq b_\mathsf{u} + b_\mathsf{v} + b_\mathsf{w} = \alpha + 2k - 3\lambda. \tag{3.17}$$

Therefore, from (3.17), we have

$$3\lambda - k - 2\alpha \leq 0. \tag{3.18}$$

Now, (3.15) and (3.18) together show that $3\lambda - k = 2\alpha$. This implies that $3\lambda - k$ is even, and therefore $k - \lambda$ is also even. Therefore A is an $\mathsf{SHF}(v; v, 2, \{1, 3\})$ if $k - \lambda$ is odd. □

Corollary 1. *Let $(X, \mathcal{B})$ be a symmetric (v, k, λ)-BIBD and let A be its block-point incidence matrix. If $k \leq 3\lambda$ and $k - \lambda$ is even then A is an $\mathsf{SHF}(v; v, 2, \{1, 3\})$ if and only if the following substructure does not occur: there exist four points $\mathsf{u}, \mathsf{v}, \mathsf{w}, \mathsf{x}$ such that*

1. *$\alpha = \frac{3\lambda - k}{2}$ blocks contain all four points $\mathsf{u}, \mathsf{v}, \mathsf{w}, \mathsf{x}$,*

Table 1. Block intersections with $\{\mathsf{u},\mathsf{v},\mathsf{w},\mathsf{x}\}$

T	c_T	T	c_T
$\{\mathsf{x}\}$	$b_\emptyset = 0$	$\{\mathsf{u}\}$	$a_\mathsf{u} - b_\mathsf{u} = 0$
$\{\mathsf{v}\}$	$a_\mathsf{v} - b_\mathsf{v} = 0$	$\{\mathsf{w}\}$	$a_\mathsf{v} - b_\mathsf{v} = 0$
$\{\mathsf{u},\mathsf{x}\}$	$b_\mathsf{u} = \lambda - \alpha$	$\{\mathsf{u},\mathsf{v}\}$	$a_\mathsf{uv} - b_\mathsf{uv} = a_\mathsf{uv} = \lambda - \alpha$
$\{\mathsf{v},\mathsf{x}\}$	$b_\mathsf{v} = \lambda - \alpha$	$\{\mathsf{u},\mathsf{w}\}$	$a_\mathsf{uw} - b_\mathsf{uw} = a_\mathsf{uw} = \lambda - \alpha$
$\{\mathsf{w},\mathsf{x}\}$	$b_\mathsf{w} = \lambda - \alpha$	$\{\mathsf{v},\mathsf{w}\}$	$a_\mathsf{vw} - b_\mathsf{vw} = a_\mathsf{vw} = \lambda - \alpha$
$\{\mathsf{u},\mathsf{v},\mathsf{x}\}$	$b_\mathsf{uv} = 0$	$\{\mathsf{u},\mathsf{w},\mathsf{x}\}$	$b_\mathsf{uw} = 0$
$\{\mathsf{v},\mathsf{w},\mathsf{x}\}$	$b_\mathsf{vw} = 0$	$\{\mathsf{u},\mathsf{v},\mathsf{w}\}$	$a_\mathsf{uvw} - b_\mathsf{uvw} = \alpha - \alpha = 0$
$\{\mathsf{u},\mathsf{v},\mathsf{w},\mathsf{x}\}$	$b_\mathsf{uvw} = \alpha$		

2. *no block contains exactly one or three points from* $\{\mathsf{u},\mathsf{v},\mathsf{w},\mathsf{x}\}$*, and*
3. *for any subset of two points from* $\{\mathsf{u},\mathsf{v},\mathsf{w},\mathsf{x}\}$*, there are exactly* $\lambda - \alpha$ *blocks that contain these two points.*

Proof. It is clear that A is not a $\mathsf{SHF}(v; v, 2, \{1,3\})$ if the specified substructure exists. So we just need to prove the converse, namely, that the substructure exists if A is not a $\mathsf{SHF}(v; v, 2, \{1,3\})$. We use the same notation as in the proof of Theorem 2. The proof of that theorem established that $\alpha = (3\lambda - k)/2$.

For each $T \subseteq \{\mathsf{u},\mathsf{v},\mathsf{w},\mathsf{x}\}$, we will compute c_T, which denotes the number of blocks B such than $B \cap \{\mathsf{u},\mathsf{v},\mathsf{w},\mathsf{x}\} = T$. First, we note two relevant facts:

- The inequality in (3.17) must be an inequality, so $b_\mathsf{u} = a_\mathsf{u}$, $b_\mathsf{v} = a_\mathsf{v}$ and $b_\mathsf{w} = a_\mathsf{w}$. Now $a_\mathsf{u} = a_\mathsf{v} = a_\mathsf{w} = k + \alpha - 2\lambda = \lambda - \alpha$, so we obtain $b_\mathsf{u} = b_\mathsf{v} = b_\mathsf{w} = \lambda - \alpha$.
- From (3.14), we see that $b_\mathsf{uv} + b_\mathsf{vw} + b_\mathsf{uw} = 0$, so $b_\mathsf{uv} = b_\mathsf{vw} = b_\mathsf{uw} = 0$.

It is now straightforward to compute the values c_T using these facts. This is done in Table 1. □

3.1 Hadamard Designs

The following is an immediate corollary of Theorem 2. This result is in fact equivalent to a result of Kimura [11, Proposition 2.1].

Corollary 2. *The incidence matrix of a* $(4n-1, 2n-1, n-1)$*-BIBD is an* $\mathsf{SHF}(4n-1; 4n-1, 2, \{1,3\})$ *if* $n > 1$ *is odd.*

There is a useful classification of Hadamard matrices in terms of substructures involving four columns; see, for example, [10]. The notion of a *type* of a Hadamard matrix is defined in [10] as follows. Let H be a Hadamard matrix of order $4n$.

For any non-negative integer m, let j_m denote the all 1's column vector of length m. By permuting and/or and negating rows and columns, any four columns of H may be transformed uniquely to the following form:

j_a	j_a	j_a	j_a
j_b	j_b	j_b	$-j_b$
j_b	j_b	$-j_b$	j_b
j_a	j_a	$-j_a$	$-j_a$
j_b	$-j_b$	j_b	j_b
j_a	$-j_a$	j_a	$-j_a$
j_a	$-j_a$	$-j_a$	j_a
j_b	$-j_b$	$-j_b$	$-j_b$

where $a+b=n$ and $0 \leq b \leq \lfloor n/2 \rfloor$. A set of four columns which is transformed to the above form is said to be of *type b*. Any permutation and negation of rows and/or columns leaves the type unchanged. A Hadamard matrix is of *type b* ($0 \leq b \leq \lfloor n/2 \rfloor$) if it has a set of four columns of type b and no set of four columns of type less than b.

If a Hadamard matrix has a first row and first column consisting entirely of entries equal to 1, then we say that the matrix is *standardized*. Any Hadamard matrix can be transformed into a standardized Hadamard matrix by multiplying certain rows and columns by -1.

Lemma 1. *Suppose we construct an incidence matrix of a* $(4n-1, 2n-1, n-1)$*-BIBD from a standardized Hadamard matrix of order* $4n > 4$ *by deleting the first row and column and replacing all occurrences of* -1*'s by* 0*'s. Then this incidence matrix is a* 3*-frameproof code if and only if the Hadamard matrix is not of type 0.*

Proof. First, suppose that the Hadamard is of type 0. Then it is obvious in the incidence matrix of the associated design that the first of the four given columns cannot be separated from the other three given columns.

Conversely, suppose that we have an incidence matrix A (of a $(4n-1, 2n-1, n-1)$-BIBD) that is not a 3-frameproof code. From Corollary 2, n must be even for this to occur. By permuting columns of A, we can assume that column 1 cannot be separated from columns 2, 3, and 4. Now we apply Corollary 1. Looking at the first four columns of A, there must be $n/2-1$ occurrences of 1111 and $n/2$ occurrences of each of the other seven patterns containing an even number of 1's. When we convert A to a Hadamard matrix H of order $4n$, we change all 0's to -1's and we add an additional row of 1's. Now we multiply all rows of H that corresponded to patterns 0000, 0011, 0101 and 0110 in A by -1. We then see that these four columns in H are of type 0. □

Remark. Kimura's result that was mentioned above is in fact a proof that a Hadamard matrix of order congruent to 4 modulo 8 is not of type 0.

Table 2. Number of inequivalent Hadamard matrices of different types

Order	4	8	12	16	20	24	28
0	1	1	0	5	0	58	0
Type 1	0	0	1	0	3	1	486
2	0	0	0	0	0	1	1

A classification, according to type, of (inequivalent) Hadamard matrices of small orders is given in [10]. The following table is from [10]:

We now give a family of Hadamard BIBDs that contain the forbidden substructure from Corollary 1. Hence, these designs are not $\{1,3\}$-SHFs.

Theorem 3. *For $n \geq 4$, let H_n be a standardized Hadamard matrix of order n. Let*

$$H = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

and let A be the $(2n-1) \times (2n-1)$ submatrix of H by removing the first column and first row and replacing all -1's by 0's. Then A is the incidence matrix of a symmetric $(2n-1, n-1, \frac{n-2}{2})$-design which is not an $\mathsf{SHF}(2n-1; 2n-1, 2, \{1,3\})$.

Proof. A is a Hadamard design by construction. Let $n = 4m$, $m \geq 1$. Since H_n is a standard Hadamard matrix of order $4m$, deleting the first column gives a 2-$(2, 4m-1, m)$ orthogonal array. Hence columns 2 and 3 of H_n contain each of the pairs $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ m times. Thus columns $2, 3, 4m+2, 4m+3$ of H contain each of the quadruples $(0,0,0,0)$, $(0,1,0,1)$, $(1,0,1,0)$, $(1,1,1,1)$ m times in rows $1, \ldots, 4m$ of H. Similarly, columns $2, 3, 4m+2, 4m+3$ of H contain each of the quadruples $(0,0,1,1)$, $(0,1,1,0)$, $(1,0,0,1)$, $(1,1,0,0)$ m times in rows $4m+1, \ldots, 8m$ of H.

Recall that the first column of H is deleted to form A. Since the first row of H consists of only 1's, we have that columns $1, 2, 4m+1, 4m+2$ of A contain each of the quadruples $(0,0,0,0)$, $(0,1,0,1)$, $(1,0,1,0)$, $(0,0,1,1)$, $(0,1,1,0)$, $(1,0,0,1)$, $(1,1,0,0)$ m times and contains $(1,1,1,1)$ $m-1$ times. Together, the eight quadruples occupy all $8m-1$ rows of A. In particular, columns $1, 2, 4m+1, 4m+2$ of A do not contain the quadruple $(1,0,0,0)$ and $(0,1,1,1)$, so $(\{1\}, \{2, 4m+1, 4m+2\})$ cannot be separated by A. □

The quadratic residue difference sets (also known as *Paley difference sets*) give rise to Hadamard designs. For a prime power $q \equiv 3 \bmod 4$, the set of quadratic residues in $\mathbb{F}_q$, when developed through $\mathbb{F}_q$, yields a $(q, (q-1)/2, (q-3)/4)$-BIBD. When $q > 11$ is prime, we will show that the incidence matrices of these designs are $\{1,3\}$-SHFs. The proof is similar to the main theorem in [8]; it is based on a character-theoretic bound proven by Burgess [3].

Theorem 4. *For all primes $q \equiv 3 \bmod 4$, $q > 11$, there is a $(q, (q-1)/2, (q-3)/4)$-BIBD whose block-point incidence matrix is a $\{1,3\}$-SHF.*

Proof. Let $\chi : {\mathbb{Z}_q}^* \to \{1, -1\}$ be the quadratic character. Define $\chi(0) = 0$ and let $a_1, a_2, a_3, a_4 \in \mathbb{Z}_q$ be distinct. Define

$$S = \sum_{x \in \mathbb{Z}_q} \chi(x - a_1)\chi(x - a_2)\chi(x - a_3)\chi(x - a_4). \tag{3.19}$$

By [3, Lemma 1], it immediately follows that $S \leq 2\sqrt{q} + 1$. For any integer $q > 11$, it is easy to see that $2\sqrt{q} + 1 < q - 4$. Therefore, $S < q - 4$. Clearly the sum in (3.19) contains exactly four terms equal to 0. The remaining $q - 4$ terms in this sum are all equal to ± 1. Since $S < q - 4$, there must be a term in the sum equal to -1. That is, there exists $x \in \mathbb{Z}_q$ such that exactly one or three of the four (non-zero) values $\chi(x - a_1), \chi(x - a_2), \chi(x - a_3), \chi(x - a_4)$ are equal to 1. In the associated design, we have a block that contains an odd number of points from $\{a_1, a_2, a_3, a_4\}$. Applying Corollary 1, it follows that the incidence matrix of the design is a $\{1,3\}$-SHF. □

Remark. For all primes $q \equiv 3 \bmod 4$, $q > 1024$, it is noted in Colbourn and Kéri [5] that Paley difference sets yield covering arrays of strength four, which immediately implies that they are $\{1,3\}$-SHFs. This follows from a similar character-theoretic argument.

Theorem 5. *There is a $(39, 19, 9)$-BIBD whose incidence matrix is a $\{1,3\}$-SHF.*

Proof. The website [12] includes 22 (known to date) skew Hadamard matrices of order 40. We derived Hadamard designs (i.e., $(39, 19, 9)$-BIBDS) from all of them by standardizing with respect to a given row and column and then deleting the given row and column. Then we checked the resulting $(39, 19, 9)$-BIBDs by computer to see if they are $\{1,3\}$-SHF. It turned out that eight of these matrices, namely numbers 1, 5, 7, 10, 11, 13, 17 and 20, give rise to $(39, 19, 9)$-BIBDs which are $\{1,3\}$-SHF. Moreover, the transposes of the incidence matrices of these 22 $(39, 19, 9)$-BIBDs give rise to eight additional $(39, 19, 9)$-BIBDs which are $\{1,3\}$-SHF, namely numbers 2, 3, 8, 12, 14, 16, 18 and 21. It did not matter which row/column we chose for the standardization process. □

3.2 The Case $k = 3\lambda$

The case $k = 3\lambda$ is especially interesting because this corresponds to $\alpha = 0$ in Theorem 1. In this situation, the four-point substructure is an *oval*, using the terminology of Assmus and van Lint [1] (the paper [1] is a general study of ovals in symmetric BIBDs). Specializing Corollary 1 to this case, we obtain the following.

Corollary 3. *Let $(X, \mathcal{A})$ be a symmetric (v, k, λ)-BIBD with $k = 3\lambda$. Then $(X, \mathcal{A})$ is not an $\mathsf{SHF}(v; v, 2, \{1, 3\})$ if and only if $(X, \mathcal{A})$ contains an oval (of cardinalty 4).*

We next present some examples to show how Corollary 3 can be used to determine if a specific parameter set gives rise to $\{1, 3\}$-SHFs.

Example 1. There is a unique $(7, 3, 1)$-BIBD up to isomorphism. As is observed in [1], the complement of any block is an oval. Therefore the $(7, 3, 1)$-BIBD is not a $\{1, 3\}$-SHF.

Example 2. There are precisely three non isomorphic $(16, 6, 2)$-BIBDs. It is observed in [1] that all three of these designs contain ovals. Therefore, no $(16, 6, 2)$-BIBD is a $\{1, 3\}$-SHF.

Example 3. It is observed in [1] that there is a $(25, 9, 3)$-BIBD that contains an oval. Therefore this BIBD is not a $\{1, 3\}$-SHF. In fact, Denniston later showed in [7] that all 78 non isomorphic $(25, 9, 3)$-BIBDs contain an oval, so there are no $(25, 9, 3)$-BIBDs whose incidence matrices are $\{1, 3\}$-SHFs.

Finally, we present an infinite family of symmetric BIBDs with $k = 3\lambda$ whose incidence matrices are not $\{1, 3\}$-SHFs.

Theorem 6. *For all integers $h \geq 2$, there is a $(3^{h+1} - 2, 3^h, 3^{h-1})$-BIBD whose incidence matrix is not a $\{1, 3\}$-SHF.*

Proof. It is shown by Tran in [15] that the Mitchell-Rajkundlia designs with the above parameters all contain ovals. (Actually, Tran shows that the Mitchell-Rajkundlia designs constructed from the Desarguesian affine planes of order 2^n all contain *maximal 2^m-arcs* for $1 \leq m \leq n$. For the specific Mitchell-Rajkundlia designs with the indicated parameters, we have $m = 1$, and the maximal 2-arcs are in fact ovals.) □

3.3 Small Symmetric BIBDs

Table 3 lists parameters for 'small' symmetric BIBDs and constructions that give rise to $\{1, 3\}$-SHFs (or not). The case of $\lambda = 1$ for $k \geq 4$ is characterized by Theorem 1 and so these parameters are omitted from the table.

4 Additional Results and Comments

We have a simple result which shows that certain symmetric BIBDs are $\{1, w\}$-SHF.

Table 3. Small Symmetric BIBDs and $\{1,3\}$-SHF

v	k	λ	$\{1,3\}$-SHF	not $\{1,3\}$-SHF	Comment
7	3	1	None	All	Example 1
11	5	2	All	None	T_2
16	6	2	None	All	Example 2
15	7	3	None	All	Table 2
37	9	2	All	None	T_1
25	9	3	None	All	Example 3
19	9	4	All	None	T_2
31	10	3	All	None	T_1
56	11	2	All	None	T_1
23	11	5	$\mathsf{QR}(23)$	H	Table 2
45	12	3	All	None	T_1
79	13	2	All	None	T_1
40	13	4	All	None	T_1
27	13	6	All	None	T_2
71	15	3	All	None	T_1
36	15	6	All	None	T_2
31	15	7	$\mathsf{QR}(31)$	H	
61	16	4	All	None	T_1
49	16	5	All	None	T_1
41	16	6	[4, §II.6.9]	?	computer verified
69	17	4	All	None	T_1
35	17	8	All	None	T_2
39	19	9	Theorem 5	H	
96	20	4	All	None	T_1
85	21	5	All	None	T_1
71	21	6	All	None	T_1
43	21	10	All	None	T_2
78	22	6	All	None	T_1
47	23	11	$\mathsf{QR}(47)$	H	
70	24	8	[4, §II.6.9]	?	computer verified
121	25	5	All	None	T_1
101	25	6	All	None	T_1
61	25	10	All	None	T_2
51	25	12	All	None	T_2

Legend	Description
T_1	Guaranteed to be {1,3}-SHFs by Theorem 2 from $k \geq 3\lambda + 1$
T_2	Guaranteed to be {1,3}-SHFs by Theorem 2 from $k - \lambda$ odd
H	Construction from Theorem 3
$\mathsf{QR}(q)$	Quadratic residue difference set (Theorem 4)

Theorem 7. *Suppose there exists a symmetric (v, k, λ)-BIBD where $k > w\lambda$. Then the block-point incidence matrix of this BIBD is a $\{1, w\}$-SHF.*

Proof. Let A be the block-point incidence matrix of the hypothesized design. Let i be one column of A and let $j_1, \ldots, j_w$ be w additional columns of A . For $1 \leq \ell \leq w$, define

$$R_\ell = \{r : \mathsf{A}(r, i) = \mathsf{A}(r, j_\ell) = 1\}.$$

Clearly $|R_\ell| = \lambda$ for all ℓ, so

$$\left| \bigcup_{\ell=1}^{w} R_\ell \right| \leq w\lambda.$$

There are k rows of A having a 1 in column i. Since $k > w\lambda$, there exists at least one row of A having a 1 in column i and 0's in columns $j_1, \ldots, j_w$. □

Remark. In the case $w = 3$, Theorem 7 provides a simple proof of the first part of Theorem 2.

Define $\mathcal{F}_w$ to be the set of all parameter triples (v, k, λ) such that there exists a symmetric (v, k, λ)-BIBD whose incidence matrix is a $\{1, w\}$-SHF, and define $\overline{\mathcal{F}}_w$ to be the set of all parameter triples (v, k, λ) such that there exists a symmetric (v, k, λ)-BIBD whose incidence matrix is *not* a $\{1, w\}$-SHF. A parameter triple (v, k, λ) will be called a *Hadamard triple* if it has the form $(4t + 3, 2t + 1, t)$ for a positive integer t, and a *non-Hadamard triple* otherwise.

There are several parameter triples in Table 3 that are in $\mathcal{F}_3 \cap \overline{\mathcal{F}}_3$. However, all of these examples are Hadamard triples. We now provide an example of a non-Hadamard triple in $\mathcal{F}_3 \cap \overline{\mathcal{F}}_3$, namely $(64, 28, 12)$.

Theorem 8. *There exists a $(64, 28, 12)$-BIBD whose incidence matrix is a $\{1, 3\}$-SHF, as well as a $(64, 28, 12)$-BIBD whose incidence matrix is not a $\{1, 3\}$-SHF.*

Proof. We have verified by computer that the incidence matrix of the design D_1 in [6, p. 113] is a $\{1, 3\}$-SHF. Furthermore, the incidence matrix of the design constructed from the difference set in $\mathbb{Z}_4 \times \mathbb{Z}_{16}$ (see [4, p. 428]) is not a $\{1, 3\}$-SHF. □

We close the paper by mentioning three open problems.

1. From the results proven in this paper, we know that $\mathcal{F}_3$ contains an infinite number of Hadamard triples, and $\overline{\mathcal{F}}_3$ also contains an infinite number of Hadamard triples. We conjecture that $\mathcal{F}_3 \cap \overline{\mathcal{F}}_3$ also contains an infinite number of Hadamard triples.
2. Does $\mathcal{F}_3$ contain an infinite number of non-Hadamard triples which do not satisfy one of the hypotheses of Theorem 2?

3. It was proven in [9] that an $\mathsf{SHF}(v; v, 2, \{1, 3\})$ is "equivalent" to a $v \times v$ permutation matrix if $v \leq 9$. We have shown in this paper that an $\mathsf{SHF}(11; 11, 2, \{1, 3\})$ is obtained from the incidence matrix of an $(11, 5, 2)$-BIBD. The case $v = 10$ remains open.

Acknowledgements

Thanks to Charlie Colbourn, Hadi Kharaghani, William Orrick and Behruz Tayfeh-Rezaie for helpful comments and for making us aware of some relevant papers.

References

1. E.F Assmus Jr. and J.H. van Lint. Ovals in projective designs. *Journal of Combinatorial Theory A* **27** (1979), 307–324.
2. D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory* **44** (1998), 1897–1905.
3. D.A. Burgess. On character sums and primitive roots. *Proceedings of the London Math. Society* **12** (1962), 1798–'92.
4. C.J. Colbourn and J.H. Dinitz. *Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall/ CRC, 2006.
5. C.J. Colbourn and G. Kéri. Binary covering arrays and existentially closed graphs. *Lecture Notes in Computer Science* **5557** (2009), 22–33 (IWCC 2009 Proceedings).
6. D. Crnković and M.-O. Pavčević. Some new symmetric designs with parameters $(64, 28, 12)$. *Discrete Mathematics* **237** (2001), 109–118,
7. R.H.F. Denniston. Enumeration of symmetric designs (25,9,3). *Annals of Discrete Mathematics* **15** (1982) 111–127.
8. R.L. Graham and J.H. Spencer. A constructive solution to a tournament problem. *Canadian Mathematical Bulletin* **14** (1971), 45–47.
9. C. Guo, D.R. Stinson, and Tran van Trung. On tight bounds for binary frameproof codes. Preprint, 2014. `http://arxiv.org/abs/1406.6920`
10. H. Kharaghani and B. Tayfeh-Rezaie. On the classification of Hadamard matrices of order 32. *Journal of Combinatorial Designs* **18** (2010), 328–336.
11. H. Kimura. Classification of Hadamard matrices of order 28. *Discrete Mathematics* **133** (1994) 171–180.
12. Christos Koukouvinos. `www.math.ntua.gr/people/(ckoukouv2)/hadamard.htm`.
13. D.R. Stinson, Tran van Trung, and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *Journal of Statistical Planning and Inference* **86** (2000), 595–617.
14. D.R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM Journal on Discrete Mathematics* **11** (1998), 41–53.
15. Tran van Trung. Maximal arcs and related designs. *Journal of Combinatorial Theory A* **57** (1991), 294–301.