New Results on Binary Frameproof Codes

Douglas R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo

ADTHM 2014
July 9, 2014

This talk is based on joint work with Chuan Guo and Tran van Trung.

Outline

1. Introduction to frameproof codes and separating hash families.
2. Existence of small $\{1, w\}$-separating hash families over binary alphabets.
3. Symmetric BIBDs and $\{1, 3\}$-separating hash families over binary alphabets.

Frameproof Codes

- Let Q be a finite alphabet of size q and let $N > 0$.
- A subset $C \subseteq Q^N$ with $|C| = n$ is called C an (N, n, q)-code and the members of C are called codewords.
- Each codeword $x \in C$ is of the form $x = (x_1, \ldots, x_N)$, where $x_i \in Q$, $1 \leq i \leq N$.
- For any subset of codewords $P \subseteq C$, the set of descendants of P, denoted $desc(P)$, is defined by

$$desc(P) = \{x \in Q^N : x_i \in \{a_i : a \in P\},\ 1 \leq i \leq N\}.$$

- Let C be an (N, n, q) code and let $w \geq 2$ be an integer. C is called a w-frameproof code (or w-FPC) if, for all $P \subseteq C$ with $|P| \leq w$, we have that $desc(P) \cap C = P$.

Example

- Let $Q = \{1, 2, 3\}$, $N = 3$, and

$$C = \{(1, 1, 2), (2, 3, 2), (2, 1, 2), (2, 2, 2)\}.$$

- C is a $(3, 4, 3)$-code.
- Let $P = \{(1, 1, 2), (2, 3, 2)\} \subseteq C$.
- Then

$$desc(P) = \{(1, 1, 2), (2, 3, 2), (1, 3, 2), (2, 1, 2)\}$$

- Since $(2, 1, 2) \in desc(P) \cap C$ but $(2, 1, 2) \notin C$, it follows that C is not a 2-frameproof code.

Separating Hash Families

Definition 1

An $(N; n, q)$-hash family is a set of N functions say $\mathcal{F}$, such that $|X| = n$, $|Y| = q$, and $f : X \to Y$ for each $f \in \mathcal{F}$.

Definition 2

An SHF$(N; n, q, \{w_1, w_2, \cdots, w_t\})$ is an $(N; n, q)$-hash family, say $\mathcal{F}$, that satisfies the following property:

> For any $C_1, C_2, \cdots, C_t \subseteq \{1, 2, \ldots, n\}$ such that $|C_1| = w_1$, $|C_2| = w_2$, $\cdots$, $|C_t| = w_t$ and $C_i \cap C_j = \emptyset$ for any $i \neq j$, there exists at least one function $f \in \mathcal{F}$ such that
>
> $$\{f(x) : x \in C_i\} \cap \{f(x) : x \in C_j\} = \emptyset$$
>
> for any $i \neq j$.

The type of the *SHF* is the multiset $\{w_1, w_2, \cdots, w_t\}$.

Matrix Representation

- An $(N; n, q)$-hash family can be depicted as an $N \times n$ matrix *A* on q symbols.
- The rows of *A* correspond to the hash functions in the family, the columns correspond to the elements in the domain, X, and the entry in row *f* and column x is just *f*(x).
- We call *A* the matrix representation of the hash family.
- It is well known that a w-frameproof (N, n, q)-code is equivalent to an *SHF*$(N; n, q, \{1, w\})$.
- The codewords are just the columns of the matrix representation of the *SHF*.

Some Examples of Binary Frameproof Codes

- We will concentrate on binary frameproof codes defined over the alphabet $\{0,1\}$.
- A permutation matrix of degree N is an $N \times N$ 0-1 matrix with exactly one 1 in each row and each column
- It is obvious that a permutation matrix of degree N is a *SHF*$(N; N, 2, \{1, w\})$ for any $w \leq N-1$.
- As another example, the incidence matrix of the $(7,3,1)$-*BIBD* is an *SHF*$(7; 7, 2, \{1, 2\})$.
- Suppose we want to separate x from y and z.
  1. If x, y, z occur in a block A, then let B be any other block that contains x.
  2. If x, y, z do not occur in a block, then let B be the unique block that contains y and z.
- One more example: the incidence matrix of the $(11,5,1)$-*BIBD* is an *SHF*$(11; 11, 2, \{1, 3\})$.

The $(7,3,1)$-BIBD

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ \color{red}{0} & \color{red}{1} & \color{red}{1} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \color{red}{1} & \color{red}{0} & 0 & \color{red}{0} & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- 1 is separated from $2,4$ by row 5 (i.e., the block $\{1,5,6\}$)
- 1 is separated from $2,3$ by row 2 (i.e., the block $\{2,3,5\}$)

Sample General Bounds for Frameproof Codes

Theorem 3 (SSW, 2001)

If there exists an SHF$(N; n, q, \{1, w\})$, *then*

$$n \leq w \left(q^{\lceil \frac{N}{w} \rceil} - 1 \right).$$

Comment: Stronger (and more complicated bounds) exist.

Theorem 4 (SZ, 2008)

There exists an SHF$(N; n, 2, \{1, w\})$ *if*

$$n \leq \left(1 - \frac{1}{w!} \right) \left(\frac{2^w}{2^w - 1} \right)^{\frac{N}{w}}.$$

Comment: This existence result uses the probabilistic method. It is a special case of a more general bound.

Small $\{1, w\}$-SHF

Here is our Main Theorem, which characterizes $\{1, w\}$-*SHF* having a "small" number of functions.

Theorem 5

For all $w \geq 3$, and for $w + 1 \leq N \leq 3w$, an SHF$(N; n, 2, \{1, w\})$ exists only if $n \leq N$.
Furthermore, for these parameter values, an SHF$(N; N, 2, \{1, w\})$ in standard form must be a permutation matrix of degree N.

Standard Form of $\{1, w\}$-SHF Over Binary Alphabets

- Suppose we have an *SHF*$(N; n, 2, \{1, w\})$ over the alphabet $Q = \{0, 1\}$.
- A row is said to be of type i if it contains exactly i entries equal to 1.
- If we interchange the 0 and 1 entries in any row of an *SHF*$(N; n, 2, \{1, w\})$, the result is still an *SHF*$(N; n, 2, \{1, w\})$.
- An *SHF*$(N; n, 2, \{1, w\})$ is said to be in standard form if every row has type $i \leq n/2$.
- The standard form of an *SHF*$(N; n, 2, \{1, w\})$ is unique if n is odd, or if n is even and there are no rows of type $n/2$.

A Useful Lemma

Lemma 6

Let A be an SHF$(N; n, 2, 1, w)$*. Suppose row* r *of A is of type* $i \le n/2$*.*

1. *If* $i < w$*, then row* r *separates exactly*

   $$i\binom{n-i}{w}$$

   column pairs (C_1, C_2)*, where* $|C_1| = 1$ *and* $|C_2| = w$*.*

2. *If* $i \geq w$*, then row* r *separates exactly*

   $$i\binom{n-i}{w} + \binom{i}{w}(n-i)$$

   column pairs (C_1, C_2)*.*

Another Useful Lemma

Lemma 7

Let w, n be positive integers such that $n \geq w + 1$. Then for $i = 1, 2, \ldots, n - w - 1$, we have

$$i\binom{n-i}{w} > (i+1)\binom{n-i-1}{w}$$

if and only if

$$(i+1)(w+1) > n + 1.$$

In particular, we have

$$\binom{n-1}{w} > 2\binom{n-2}{w} > 3\binom{n-3}{w} > \cdots > j\binom{n-j}{w} \qquad (1)$$

for $j \leq n - w$, whenever $n \leq 2w$.

The Easiest Cases: $w+1 \le N \le 2w-1$

Theorem 8

Suppose $w \ge 3$, $w+1 \le N \le 2w-1$, and there exists an SHF$(N; n, 2, \{1, w\})$. Then $n \le N$.

Proof.

Suppose there is an *SHF*$(N; n = N+1, 2, \{1, w\})$. Let *A* be its $N \times (N+1)$ matrix representation. There are $T = n\binom{n-1}{w}$ pairs of column sets (C_1, C_2) to be separated, where $|C_1| = 1$, $|C_2| = w$. Using Lemma 7, we see that

$$\binom{n-1}{w} > 2\binom{n-2}{w} > 3\binom{n-3}{w} > \cdots > (w-1)\binom{n-(w-1)}{w}.$$

A row of type 1 separates the largest number of column pairs, namely $\binom{n-1}{w} = \binom{N}{w}$. Since *A* has N rows, the maximum number of column pairs that can be separated is
$N\binom{N}{w} = (n-1)\binom{n-1}{w} < T$, which is a contradiction. $\square$

The Next Case: $N = 2w$

Theorem 9

Suppose $w \geq 3$, $N = 2w$, and there exists an SHF$(N; n, 2, \{1, w\})$. Then $n \leq N$.

Proof.

Suppose there is an *SHF*$(N = 2w; n = N + 1, 2, \{1, w\})$. We have

$$\begin{aligned}\binom{n-1}{w} &= 2\binom{n-2}{w} > \cdots > (w-1)\binom{n-(w-1)}{w} \\ &> w\binom{n-w}{w} + n - w.\end{aligned}$$

The last inequality can be easily checked, while all other inequalities follow from Lemma 7. The last term is given by Lemma 6; it corresponds to the case of a row of type w. A row of type 1 or type 2 separates the largest number of column pairs, namely $\binom{n-1}{w} = \binom{N}{w}$. The rest of the proof is as before. □

The Case $w = 3$

- For $w = 3$, $N \leq 9$, we have that an *SHF*$(N; n, 2, \{1, 3\})$ exists only if $n \leq N$ and any *SHF*$(N; N, 2, \{1, 3\})$ in standard from is a permutation matrix (Main Theorem).
- There exists an *SHF*$(11; 11, 2, \{1, 3\})$ (in standard form) that is not a permutation matrix, namely, the incidence matrix of an $(11, 5, 2)$-*BIBD*. (We will prove this a bit later.)
- What about $N = 10$? (This is an open problem.)

SBIBDs and $\{1,3\}$-SHF

Theorem 10

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

Theorem 11

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

1. *$\alpha = \frac{3\lambda - k}{2}$ blocks contain all four points u, v, w, x,*
2. *no block in $\mathcal{C}$ contains exactly one or three points from $\{u, v, w, x\}$, and*
3. *for any subset of two points from $\{u, v, w, x\}$, there are exactly $\lambda - \alpha$ blocks in $\mathcal{C}$ that intersect $\{u, v, w, x\}$ in the specified two points.*

SBIBDs and $\{1,3\}$-SHF (cont.)

We give an outline of the proof. First, we fix three columns u, v, w and classify the rows of the incidence matrix as follows:

# of rows	u	v	w
$a_\emptyset$	0	0	0
a_w	0	0	1
a_v	0	1	0
a_{vw}	0	1	1
a_u	1	0	0
a_{uw}	1	0	1
a_{uv}	1	1	0
a_{uvw}	1	1	1

If we denote $\alpha = a_{uvw}$, then it is easy to see that

$$a_{uv} = a_{vw} = a_{uw} = \lambda - \alpha$$
$$a_u = a_v = a_w = k + \alpha - 2\lambda$$

SBIBDs and $\{1,3\}$-SHF (cont.)

Now consider a fourth column, say x. We want to separate $\{x\}$ from $\{u,v,w\}$. We extend our classification of the rows of the incidence matrix as follows:

# of rows	u	v	w	x
$b_\emptyset$	0	0	0	1
b_w	0	0	1	1
b_v	0	1	0	1
b_{vw}	0	1	1	1
b_u	1	0	0	1
b_{uw}	1	0	1	1
b_{uv}	1	1	0	1
b_{uvw}	1	1	1	1

# of rows	u	v	w	x
$a_\emptyset - b_\emptyset$	0	0	0	0
$a_w - b_w$	0	0	1	0
$a_v - b_v$	0	1	0	0
$a_{vw} - b_{vw}$	0	1	1	0
$a_u - b_u$	1	0	0	0
$a_{uw} - b_{uw}$	1	0	1	0
$a_{uv} - b_{uv}$	1	1	0	0
$a_{uvw} - b_{uvw}$	1	1	1	0

Observation: We cannot separate $\{x\}$ from $\{u,v,w\}$ if and only if $b_\emptyset = 0$ and $a_{uvw} = b_{uvw}$.

SBIBDs and $\{1,3\}$-SHF (cont.)

Assume $b_\emptyset = 0$ and $a_{uvw} = b_{uvw}$. We have

$$\begin{aligned} b_\emptyset + b_u + b_v + b_w + b_{uv} + b_{vw} + b_{uw} + b_{uvw} &= k \\ b_u + b_{uv} + b_{uw} + b_{uvw} &= \lambda \\ b_v + b_{uv} + b_{vw} + b_{uvw} &= \lambda \\ b_w + b_{uw} + b_{vw} + b_{uvw} &= \lambda. \end{aligned}$$

Therefore

$$\begin{aligned} \boxed{b_u + b_v + b_w} + \boxed{b_{uv} + b_{vw} + b_{uw}} &= k - \alpha \\ \boxed{b_u + b_v + b_w} + 2(\boxed{b_{uv} + b_{vw} + b_{uw}}) &= 3(\lambda - \alpha). \end{aligned}$$

Let $B_1 = b_u + b_v + b_w$ and $B_2 = b_{uv} + b_{vw} + b_{uw}$. Then

$$\begin{aligned} B_1 &= \alpha + 2k - 3\lambda \\ B_2 &= 3\lambda - k - 2\alpha. \end{aligned}$$

SBIBDs and $\{1,3\}$-SHF (cont.)

Using the facts that

$$B_2 \geq 0$$

and

$$B_1 \leq a_u + a_v + a_w = 3(k + \alpha - 2\lambda),$$

it turns out that

$$\alpha = \frac{3\lambda - k}{2}.$$

Since α is a non-negative integer, this proves Theorem 9. Theorem 10 follows from further examination of the equations relating the a's and b's.

Comment: Theorem 9 immediately shows that the incidence matrix of an $(11,5,2)$-*BIBD* is an *SHF*$(11;11,2,\{1,3\})$, because $3\lambda - k = 1$ is odd.

The Case $k = 3\lambda$

- When $k = 3\lambda$, we have that $\alpha = 0$ and the substructure consists of four points.
- In this case, every block meets the substructure in 0 or two points.
- The substructure is in fact an oval in the *SBIBD*, as defined by Assmus and van Lint (1979).
- Theorem 11 says that an *SBIBD* with $k = 3\lambda$ is a $\{1, 3\}$-*SHF* if and only if the *BIBD* does not contain an oval.

Some Examples when $k = 3\lambda$

- There is a unique $(7, 3, 1)$-*BIBD* up to isomorphism. The complement of any block is an oval. Therefore the $(7, 3, 1)$-*BIBD* is not a $\{1, 3\}$-*SHF*. (Comment: this also follows from our Main Theorem.)
- There are precisely three nonisomorphic $(16, 6, 2)$-*BIBD*s. It is observed in Assmus and van Lint (1979) that all three of these designs contain ovals. Therefore, no $(16, 6, 2)$-*BIBD* is a $\{1, 3\}$-*SHF*.
- It is observed in Assmus and van Lint (1979) that there is a $(25, 9, 3)$-*BIBD* that contains an oval. Therefore this *BIBD* is not a $\{1, 3\}$-*SHF*.

Hadamard Designs and $\{1, 3\}$-SHF

We use the doubling construction for Hadamard matrices to construct Hadamard designs that are not $\{1, 3\}$-frameproof codes.

Theorem 12

Let H_n be a standardized Hadamard matrix of order n. Let

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

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

More About Hadamard Designs and $\{1,3\}$-SHF

- We have verified by computer that the Hadamard designs obtained from the quadratic residues in $\mathbb{F}_q$ are $\{1,3\}$-*SHF* when $q = 23, 27, 31$ and 47.
- The doubling construction from the previous slide yields Hadamard designs (for some of these parameters) that are not $\{1,3\}$-*SHF*.
- These are currently the only parameter cases for which we know that there exist *SBIBD*s that are $\{1,3\}$-*SHF* as well as *SBIBD*s that are not $\{1,3\}$-*SHF*.

Open Problems

- Can our Main Theorem be extended so it holds for some values $N > 3w$?
- For which parameter sets do there exist symmetric (v, k, λ)-*BIBD*s that are $\{1, 3\}$-*SHF* as well as symmetric *BIBD*s that are not $\{1, 3\}$-*SHF*?
- Find examples of symmetric (v, k, λ)-*BIBD*s that are $\{1, w\}$-*SHF*, where $w > 3$.
- What can we say about non-symmetric *BIBD*s?
- Can we give nice bounds and characterizations of small *SHF* for other types, e.g., $\{2, w\}$-*SHF*?
- Do any of these results generalize in a nice way to non-binary alphabets?

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] Chuan Guo, Douglas R. Stinson and Tran van Trung. On tight bounds for binary frameproof codes. Preprint, 2014, http://arxiv.org/abs/1406.6920.

[3] Chuan Guo, Douglas R. Stinson and Tran van Trung. On symmetric designs and binary frameproof codes. In preparation.

Thank You For Your Attention and Happy 70th Birthday to Hadi!