Constructions of 2-Cover-Free Families and Related Separating Hash Families

P.C. Li and G.H.J. van Rees
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada

R. Wei*
Department of Computer Science
Lakehead University
Thunder Bay, Ontario P7B 5E1, Canada

September 29, 2005

Abstract

Cover-free families (CFF) were considered from different subjects by numerous researchers. In this paper we mainly consider explicit constructions of $(2; d)$-cover-free families. We also determine the size of optimal 2-cover-free-families on 9, 10 and 11 points. Related separating hash families, which can be used to construct CFFs, are also discussed.

Key words: cover-free family, separating hash families, superimposed codes, combinatorial design, cryptography

1 Introduction

Cover-free families were considered from different subjects such as information theory, combinatorics and group testing. Cover-free families were first introduced in 1964 by Kautz and Singleton [16] to investigate nonrandom superimposed binary codes. These codes may be used for file retrieval, data communication and magnetic memories. In 1985, Erdös, Frankl and Füredi [12] considered cover-free families as combinatorial objects which generalized Sperner systems. In 1987, Hwang and Śos [15] defined cover-free families for non-adaptive group testing. Recently, cover-free families have been considered for many cryptographic problems such as frameproof codes and traceability schemes ([2, 5, 6, 13, 20, 21, 22]), broadcast encryption ([14, 17, 23], key storage ([9, 18]), multi-receiver authentication ([19]), etc. For these applications, various generalized definitions of cover-free families were adapted. A summary of cover-free families can be found in [24]. In this paper, we use a definition adapted in [10], which is a slightly generalized version of the definition found in [12].

*Corresponding author(wei@ccc.cs.lakeheadu.ca)

We now provide some definitions.

Definition 1.1 *A* set system *is a pair* $(X, \mathcal{B})$ *that satisfies the following properties:*

1. X *is a finite set of* points*,*
2. $\mathcal{B}$ *is a collection of subsets of* X*, called* blocks*.*

Definition 1.2 *A set system* $(X, \mathcal{F})$ *is called a* $(r; d)$-cover-free family *(or* $(r; d)$-CFF*) provided that, for any* r *distinct blocks* $A_1, \cdots, A_r \in \mathcal{F}$ *and any other block* $B_0 \in \mathcal{F}$*, we have*

$$\left| B_0 \setminus \left(\bigcup_{j=1}^{r} A_j \right) \right| > d,$$

When $|X| = v$ and $|\mathcal{F}| = b$, we will denote it as $(r; d)$-CFF(v, b). If every block of the CFF is of size k, then we call it a k-uniform cover-free family and denote it as $(r; d)$-CFF$_k(v, b)$. When $d = 0$, we will omit d and call it r-CFF.

In this paper, we mainly consider constructions of $(2; d)$-cover-free families. Erdös et al. [11] first discussed 2-cover-free families in detail. Let $T(r, v)$ denote the maximum number of blocks in an r-CFF of v points and $T_k(r, v)$ denote the maximum number of blocks in an r-CFF$_k$ of v points. The following results were proved in [11].

Theorem 1.1

$$\begin{aligned} T_{2t-1}(2, v) &\leq \binom{v}{t} \Big/ \binom{2t-1}{t}, \\ T_{2t}(2, v) &\leq \binom{v-1}{t} \Big/ \binom{2t-1}{t}. \end{aligned}$$

Theorem 1.2

$$1.134^v < T(2, v) < 1.25^v.$$

Remark The bounds in Theorem 1.2 are quite good. However, the upper bound is asymptotic and useless for small values of v. Further, the proof of $T(2, v) > 1.134^v$ used a probabilistic argument and hence is non-constructive. For an explicit construction, the authors of [11] provided a method for constructing a 2-CFF$_k \left(v, \binom{v}{\lfloor k/2 \rfloor} \Big/ \binom{k}{\lfloor k/2 \rfloor}^2 \right)$. For purposes of applicability to areas of cryptography, better explicit constructions of CFFs are needed.

There is little known about explicit constructions of $(2; d)$-CFF for $d > 0$. In this paper, we will give some new constructions for these kinds of CFFs. In Section 2, we will give an overview of some known results on cover-free families. In Section 3, we will provide some new recursive constructions for $(2, d)$-cover-free families. A study of separating hash families is given in Section 4. In Section 5, we consider a slight generalization of the algorithm in [11] for constructing $(2, d)$-cover-free families with uniform block sizes. Finally, in Section 6, we state some results for $T(r, v)$, study $T(2, v)$ for $v = 9, 10$ and 11 and provide a table of lower and upper bounds for $T(2, v)$.

2 Known Constructions

In [4, 12, 16, 21, 22], combinatorial designs were used to construct r-CFF. For the details of combinatorial designs used in this paper, readers are referred to [7]. The following construction of $(r;d)$-CFF using t-designs can be found in [12, 16, 22]. First we give the definition of a t-packing design as follows.

Definition 2.1 *A t-(v,k,λ)* packing design *is a set system $(X,\mathcal{B})$, where $|X| = v$,$|B| = k$ for every $B \in \mathcal{B}$,and every t-subset of X occurs in at most λ blocks in $\mathcal{B}$.*

A t-packing design is an $(r;d)$-CFF for certain values of r, d. We have the following construction from [24].

Theorem 2.1 *If there exists a t-$(v,k,1)$ packing design having b blocks, then there exists a $(r;d)$-CFF$_k(v,b)$, where $r = \lfloor (k-d-1)/(t-1) \rfloor$.*

In [22], orthogonal arrays were used to obtain t-packing designs. An *orthogonal array* $\mathrm{OA}(t,k,s)$ is a $k \times s^t$ array, with entries from a set of $s \geq 2$ symbols, such that in any t rows, every $t \times 1$ column vector appears exactly once. Suppose a column in an $\mathrm{OA}(t,k,s)$ is $\{s_1, s_2, \cdots, s_k\}$. Define a block as

$$\{(s_1,1),(s_2,2),\cdots,(s_k,k)\}$$

accordingly. In this way, we can obtain a t-$(ks,k,1)$ packing design from an $\mathrm{OA}(t,k,s)$. It is known that if q is a prime power and $t < q$, then there exists an $\mathrm{OA}(t,q+1,q)$ (see [7]), and hence a t-$\left(q^2+q, q+1, 1\right)$ packing design with q^t blocks exists. Therefore we have the following results.

Theorem 2.2 *For any prime power q and any integer $t < q$, there exists a $\left(\left\lfloor \frac{q-d}{t-1} \right\rfloor; d\right)$-CFF$(q^2+q, q^t)$*

Corollary 2.3 *For any prime power q and any integer $t < q$, there exists a $(2; q-2t+2)$-CFF(q^2+q, q^t)*

Corollary 2.4 *For any odd prime power q, there is a 2-CFF$(q^2+q, q^{\frac{q+1}{2}})$.*

A t-$(v,k,1)$ design is a special case of t-$(v,k,1)$ packing design, in which every t-subset occurs in exactly one block. In a $t-(v,k,1)$ design, the number of blocks is

$$\binom{v}{t} \Big/ \binom{k}{t}.$$

There are many known results on the existence and constructions of t-$(v,k,1)$ designs. For example, there exists 2-$(v,3,1)$ designs for $v \equiv 1$ or $3 \pmod 6$ and 3-$(q^n+1, q+1, 1)$ designs for any prime power q. Using these designs and Theorem 1.1, the following results on k-CFF for small values of k were proved in [11]:

$$\begin{aligned} T_1(2,v) &= v, \ T_2(2,v) = v-1, \\ T_3(2,v) &= T_4(2,v) = v^2/6 + O(v), \\ T_5(2,v) &= T_6(2,v) = v^3/60 + o(v^3). \end{aligned}$$

On the other hand, no t-$(v,k,1)$ design with $v > k > t$ is known to exist for $t \geq 6$ (See [7] for the details).

In [21], another combinatorial method is used to construct CFFs, which uses separating hash families.

Definition 2.2 An $(n, m, \{w_1, w_2\})$-λ-*separating hash family* is a set of functions $\mathcal{F}$, such that $|Y| = n$, $|X| = m$, $f : Y \to X$ for each $f \in \mathcal{F}$, and for any $C_1, C_2 \subseteq \{1, 2, \ldots, n\}$ such that $|C_1| = w_1$, $|C_2| = w_2$ and $C_1 \cap C_2 = \emptyset$, there exist at least λ functions $f \in \mathcal{F}$ such that

$$\{f(y) : y \in C_1\} \cap \{f(y) : y \in C_2\} = \emptyset.$$

The notation λ-SHF$(N; n, m, \{w_1, w_2\})$ will be used to denote an $(n, m, \{w_1, w_2\})$-λ-separating hash family with $|\mathcal{F}| = N$. When $\lambda = 1$, it is omitted from the notation.

A λ-SHF$(N; n, m, \{w_1, w_2\})$ can be depicted as an $N \times n$ matrix with entries from $\{1, 2, \ldots, m\}$, such that in any two disjoint sets C_1 and C_2 of w_1 and w_2 columns (respectively), there exists at least λ rows such that the entries in the columns C_1 are distinct from the entries in the columns C_2. Suppose that A is an $n \times N$ matrix whose transpose depicts an λ-SHF$(N; n, m, \{1, r\})$. Suppose that the entries of A belong to the set $\{1, 2, \cdots, m\}$. Suppose B is the incidence matrix of a $(r; d)$-CFF(v, m). Let $b_1, b_2, \cdots, b_m$ the rows of B. We construct a $n \times Nv$ matrix A' by substituting the element i in A by b_i. It can be verified that A' is an incidence matrix of a $(r; \lambda(d+1)-1)$-CFF(vN, n). Thus we have the following construction.

Theorem 2.5 *If there exists an $(r; d)$-CFF(v, m) and a λ-SHF$(N; n, m, \{1, r\})$, then there exists an $(r; \lambda(d + 1) - 1)$-CFF(vN, n).*

Using a recursive method introduced in [1], the following result is proved in [21].

Theorem 2.6 *Suppose there exists an r-CFF(N_0, n_0), where $\gcd(n_0, r!) = 1$. Then there exists an r-CFF$\left((r + 1)^k N_0, {n_0}^{2^k}\right)$ for any integer $k \geq 0$.*

Consider a code $\mathcal{C}$ of length N on an alphabet Q with $|Q| = q$. Then $\mathcal{C} \subseteq Q^N$ and we will call it an (N, n, q)-code if $|\mathcal{C}| = n$. The elements of $\mathcal{C}$ are called *codewords*; each codeword is $x = (x_1, \cdots, x_N)$, where $x_i \in Q$, $1 \leq i \leq N$. Suppose $\mathcal{C}$ is an (N, n, q) code on an alphabet Q. Define $X = \{1, \cdots, N\} \times Q$, and for each codeword $c = (c_1, \cdots, c_N) \in \mathcal{C}$, define an N-subset of X as follows:

$$B_c = \{(i, c_i) : 1 \leq i \leq N\}.$$

Finally, define $\mathcal{B} = \{B_c : c \in \mathcal{C}\}$. Then we obtain an N-uniform set system $(X, \mathcal{B})$. Using this correspondence between a code and a set system, we are able to construct uniform CFFs from codes which satisfy certain properties. The following theorem is easy to prove.

Theorem 2.7 *Suppose that $\mathcal{C}$ is an (N, n, q)-code having minimum distance D. Then there is an $(r; d)$-CFF(Nq, n), where $r = \left\lfloor \frac{N-d-1}{N-D} \right\rfloor$.*

Reed-Solomon codes were used in [12, 17, 20] to construct CFF. Since a Reed-solomon code is an (N, q^t, q)-code with minimum distance $D = N - t + 1$, we have the following.

Theorem 2.8 *Suppose N, q, r and d are given, with q a prime power and $N \leq q+1$. Then there exists an $(r; d)$-CFF(qN, T) where $T = q^{\lceil (N+r-d-1)/r \rceil}$.*

The CFF constructed from a Reed-Solomon code is the same as a CFF constructed from an orthogonal array. A shortened Reed-Solomon code is used to construct r-CFF in [8]. A shortened Reed-Solomon code is a sub-code of a Reed-Solomon $(q+1, q^t, q)$-code, which contains all the codewords whose first s elements are all zeros, where $0 \leq s \leq t-1$. So the shortened Reed-Solomon code is a $(q+1-s, q^{t-s}, q)$-code. The minimum distance of a shortened code is the same as the original Reed-Solomon code: $D = q - t + 2$. Hence we obtain the following result.

Theorem 2.9 *Suppose q and r are given, with q a prime power. Then there exists an $(r; d)$-CFF$((q+1-s)q, T)$ where $T = q^{\lceil (q+r-d-s)/r \rceil}$ and $s \leq q - d$.*

Setting $r = 2$, Theorem 2.9 immediately gives the following result.

Corollary 2.10 *For any prime power q, there exists a $(2; d)$-CFF$\big((q+1-s)q, q^{\lceil (q+2-d-s)/2 \rceil}\big)$, where $0 \leq s \leq q - d$.*

3 New constructions

In this section, we provide some new constructions for $(2; d)$-CFFs. It is easy to see that if there is a $(2; d)$-CFF(v, b), then there is a $(2; (d+1)n - 1)$-CFF(nv, b). However, this is not a very good construction. Hence, we want to find better recursive constructions. Our first construction is very straightforward.

Lemma 3.1 *If there exist an $(r; d)$-CFF(v_1, b_1) and an $(r; d)$-CFF(v_2, b_2), then there exists an $(r; d)$-CFF$(v_1 + v_2, b_1 + b_2)$.*

Proof. Suppose A is the incidence matrix of the r-CFF(v_1, b_1) and B is the incidence matrix of the r-CFF(v_2, b_2). We construct a matrix as follows:

$$\begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix},$$

where $\mathbf{0}$ is a zero matrix. This matrix is the incidence matrix of an $(r; d)$-CFF$((v_1 + v_2, b_1 + b_2)$. □

In the next two results, we make use of Sperner's Theorem, which states that any family of subsets of an n-set satisfying the property that any element in the family is not contain in any other element of the family, can have at most $\binom{n}{\lceil n/2 \rceil}$ elements in the family.

Theorem 3.2 *If there is a $(2; d)$-CFF(v, b), then there exists a $(2; d)$-CFF$(v + (s+2)(d+1), 2b)$ for any integer s satisfying $\binom{s}{\lceil \frac{s}{2} \rceil} \geq b$.*

Proof. Suppose the incidence matrix of the $(2;d)$-CFF(v,b) is A. Let B be a $b \times s$ $0-1$ matrix such that each of its rows contains distinct sets of $\lceil \frac{s}{2} \rceil$ 1's. Let

$$C = (B\ \mathbf{1}\ \mathbf{0}),$$

where $\mathbf{0}$ is a column of all 0's and $\mathbf{1}$ is a column of all 1's. We construct a $2b \times (v+(s+2)(d+1))$ matrix as follows:

$$\begin{pmatrix} A & C & \cdots & C \\ A & \overline{C} & \cdots & \overline{C} \end{pmatrix},$$

where $\overline{C}$ is the complement of C (i.e., '0' is changed to '1' and '1' is changed to '0'). It is readily checked that this is an incidence matrix of a $(2;d)$-CFF$(v+(s+2)(d+1), 2b)$. □

In case s is odd, the $\mathbf{1}$ column can be left out of C, as any 2 rows in $\overline{C}$ must contain two zeroes in some column. This gives the following result.

Theorem 3.3 *If there is a $(2;d)$-CFF(v,b), then there exists a $(2;d)$-CFF$(v+(s+1)(d+1), 2b)$ for any odd integer s satisfying $\binom{s}{\lceil \frac{s}{2} \rceil} \geq b$.*

Example 3.1 *From a 3-$(17,5,1)$ design, we have a 2-CFF$_5(17,68)$. Using the construction of Theorem 3.2, we have a 2-CFF$_{10}(27,136)$, a 2-CFF$_{16}(39,272)$, etc.*

We now give some product theorems. The first one is easy.

Theorem 3.4 *Suppose there exists a $(2;d_1)$-CFF(v_1,b_1) and a $(2;d_2)$-CFF(v_2,b_2). Then there exists a $(2;(d_1+1)(d_2+1)-1)$-CFF(v_1v_2, b_1b_2).*

Proof. Let the incidence matrix of the $(2;d_1)$-CFF(v_1,b_1) be A_1 and let the incidence matrix of the $(2;d_2)$-CFF(v_2,b_2) be A_2. Construct a $b_1b_2 \times v_1v_2$ $0-1$ matrix as follows. In A_1, substitute 1 with A_2 and substitute 0 with a $b_2 \times v_2$ 0 matrix. It is readily checked that the new matrix is the incidence matrix of a $(2;(d_1+1)(d_2+1)-1)$-CFF(v_1v_2, b_1b_2). □

Theorem 3.5 *Suppose there exists a $(2;d)$-CFF(v_1,b_1) and a $(2;d)$-CFF(v_2,b_2). Then there exists a $(2;d)$-CFF(sv_1+v_2, b_1b_2) for any integer s satisfying $\binom{s}{\lceil \frac{s}{2} \rceil} \geq b_2$.*

Proof. Let the incidence matrix of the $(2;d)$-CFF(v_1,b_1) be A_1 and let the incidence matrix of the $(2;d)$-CFF(v_2,b_2) be A_2. We construct a $b_2 \times s$ $0-1$ matrix B such that each of its rows contains distinct sets of $\lceil s/2 \rceil$ 1's. Then we construct a $b_1b_2 \times (sv_1+v_2)$ matrix C as follows. For the i^{th} row of B, substitute 1 with matrix A_1, substitute 0 with a zero matrix and append i^{th} row of A_2 to each of the b_1 new rows. We are going to prove that C is an incidence matrix of a $(2;d)$-CFF(sv_1+v_2, b_1b_2). Consider three blocks (rows) F_0, F_1 and F_2 in C. We want to prove that

$$|F_0 \backslash F_1 \cup F_2| > d.$$

Case 1. The three blocks are in a same row of B. Then we can find a sub-matrix in these 3 rows of C that consists of 3 rows from A_1. Since A_1 is an incidence matrix of a $(2;d)$-CFF, the conclusion is true.

Case 2. The three blocks are from three different rows of B. Then we can find a sub-matrix in these 3 rows of C that consists of 3 rows from A_2. Since A_2 is the incidence matrix of a $(2;d)$-CFF, the conclusion is true.
Case 3. The three blocks are from 2 different rows of B. In this case, we can find a sub-matrix in these 2 rows of B as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

So the conclusion follows from Lemma 3.1. □

From Corollary 2.10 we have a $(2;2)$-CFF$(49, 343)$ and a $(2;2)$-CFF$\Big((q+1-s)q, q^{\lceil \frac{q-s}{2} \rceil}\Big)$ for q a prime power and $0 \leq s \leq q-2$. So we have the following by Theorem 3.5.

Example 3.2 *There exists a* $(2;2)$*-CFF*$\Big(11(q+1-s)q+49, 343q^{\lceil \frac{q-s}{2} \rceil}\Big)$ *for* q *a prime power and* $0 \leq s \leq q-2$.

4 Construction of SHFs

In this section we consider constructions of SHFs. Our motivation for studying these systems is that they may be used to construct cover free families and other codes (see [21]). On the other hand, there is little known explicit construction of SHF since it was invented in [21]. We say that an SHF$(N; n, m, \{1,2\})$ is *optimal* if for fixed N and m, the value of n is as large as possible. We begin by considering small values of N.

Lemma 4.1 *There exists an SHF*$(2; 2m-2, m, \{1,2\})$ *for each positive integer* m.

Proof. It is easy to check that the following matrix gives the required SHF.

$$\begin{pmatrix} 1 & 2 & \cdots & m-1 & m & m & \cdots & m \\ m & m & \cdots & m & 1 & 2 & \cdots & m-1 \end{pmatrix}$$

□

The following result states that the SHF constructed in Lemma 4.1 is optimal.

Theorem 4.2 *There is no SHF*$(2; 2m-1, m, \{1,2\})$ *for any positive integer* m.

Proof. Suppose $f : \mathbb{Z}_{2m-1} \to \mathbb{Z}_m$ is a function in an $SHF(2, 2m-1, m, \{1,2\})$. Let g be the other function. Consider the set $M = \{y \in \mathbb{Z}_m : |x \in \mathbb{Z}_{2m-1} : f(x) = y| \leq 1\}$. It is clear that $|M| \leq m-1$. If $|M| < m-1$, then the elements in $\mathbb{Z}_m \setminus M$ occur at least $2m-1-(m-2) = m+1$ times in the range of f. Let A be the set of all points in $\mathbb{Z}_{2m-1}$ that map to a point in $\mathbb{Z}_m \setminus M$ by f. It is easy to see that in order for g to be valid, $g(x) \neq g(y)$ if $x \neq y \in A$. But this is impossible since $|A| \geq m+1 > m$. If $|M| = m-1$, then m elements of $\mathbb{Z}_{2m-1}$ are mapped to an element of $\mathbb{Z}_m$ by f and mapped to distinct elements of $\mathbb{Z}_m$ by g. But wherever g maps the elements of M there is a contradiction. □

Lemma 4.3 *There exists an SHF*$(3; m^2, m, \{1, 2\})$ *for each positive integer* m.

Proof. Let X be $\mathbb{Z}_m$ and $Y = X \times X$. For $(x, y) \in Y$, define $\phi_1(x, y) = x, \phi_2(x, y) = y$ and $\phi_3(x, y) = x + y \pmod{m}$. Suppose $C_1 = \{(x_1, y_1)\}, C_2 = \{(x_2, y_2), (x_3, y_3)\}$. We want to show that there is one function separating C_1 and C_2. If $x_1 \neq x_2$ and $x_1 \neq x_3$ (or $y_1 \neq y_2$ and $y_1 \neq y_3$), then ϕ_1 (or ϕ_2) separates C_1 and C_2. In the other cases, ϕ_3 separates C_1 and C_2. □

By using Lemma 4.3 and Theorem 2.5 repeatedly, we have the following result.

Corollary 4.4 *If there is a* $(2; d)$*-CFF*(v, b)*, then there is a* $(2; d)$*-CFF*$(3^t v, b^{2^t})$.

The SHF constructed in Lemma 4.3 is optimal. We indicate that fact in the following Theorem.

Theorem 4.5 *There is no SHF*$(3; m^2 + 1, m, \{1, 2\})$ *for any positive integer* m.

Proof. Suppose there does exist an SHF$(3; m^2 + 1, m, \{1, 2\})$. Let A denote its $3 \times (m^2 + 1)$ matrix. First we note that if there are two columns in A as follows:

$$\begin{matrix} a & a \\ b & b \\ x & y \end{matrix}$$

then x and y cannot appear in other positions of the third row.

Let

$$f(v) = \max_{1 \leq i \leq 3} \{\text{number of appearance of } v \text{ in row } \ i\}.$$

Suppose a is an element of X such that $f(a)$ is the biggest. Then $f(a) = m + t, t \geq 1$, because we have $m^2 + 1$ columns. Without loss of generality, we may assume that a appears in the first $m + t$ columns in the first row. In the second row in the first $m + t$ columns there must be t repeated elements among x different elements. The number of occurrences of these x elements in the first $m + t$ columns is $t + x$. Let these elements occur in the first $t + x$ columns of row 2. Then we know that any element in the first $t + x$ columns of the third row may appear only once in the third row by the argument of paragraph one of this proof.

Since at least $t + 1$ elements only appear once in the third row and at most $m - t - 1$ elements occupy the other $m^2 - t$ positions in the third row, there must be an element that appears at least $m + t + 1$ times in the third row, which is a contradiction to the assumption that $f(a) = m + t$ is the biggest. The conclusion follows. □

Here is another way to construct an optimal SHF$(3; m^2, m, \{1, 2\})$, using Steiner triple systems for $m \equiv 1, 3 \pmod{6}$. We begin with an easy lemma.

Lemma 4.6 *If* A *is an* $r \times c$ *array with entries from* $\mathbb{Z}_m$ *where* $r \geq 3$ *with the property that any two columns agree in at most one row, then the array* A *is an* $SHF(r; c, m, \{1, 2\})$.

We now show how to construct an optimal $SHF(3; m^2, m, \{1, 2\})$ using Steiner triple systems of order m, $m \equiv 1, 3 \pmod{6}$.

Theorem 4.7 *An optimal $SHF(3, m^2, m, \{1, 2\})$ can be constructed using Steiner triple systems of order m, where $m \equiv 1, 3 \pmod 6$.*

Proof. Suppose $m \equiv 1, 3 \pmod 6$ and let $\mathcal{B}$ be the $m(m-1)/6$ triples of a Steiner triple system of order m with point set $\mathbb{Z}_m$. For each $B \in \mathcal{B}$, consider each permutation of the elements of B and make it a column of an array A. Clearly, the array A contains $(3!)m(m-1)/6 = m(m-1) = m^2 - m$ columns. Because each column of A is a permutation of the elements in a block of the Steiner triple system, any two columns of A agree in at most one row. Now, add m columns $(0, 0, 0)^T$, $(1, 1, 1)^T$,...,$(m-1, m-1, m-1)^T$ to array A. Array A now has m^2 columns and clearly, adding these last m columns does not cause the array A to violent the property of the previous lemma. Hence the array A is an $SHF(3, m^2, m, \{1, 2\})$. □

It is easy to see that the systems obtained from Steiner triple systems of order greater than 3 are non-isomorphic from those constructed in Lemma 4.3. We now provide some properties of optimal $SHF(3; m^2, m, \{1, 2\})$, where $m > 1$.

Lemma 4.8 *Any optimal $SHF(3, m^2, m, \{1, 2\})$ must satisfy the property that every element appears exactly m times in each row.*

Proof. Very similar to the proof that no $SHF(3, m^2 + 1, m, \{1, 2\})$ exists. □

Theorem 4.9 *Any optimal $SHF(3; m^2, m, \{1, 2\})$ must satisfy the property that any two distinct columns agree in at most one row.*

Proof. Suppose there are two columns $c_1 = (a, b, c)^T$ and $c_2 = (a, b, d)^T$ that agree in at exactly two coordinates. It cannot agree in three since separating hash families cannot have identical columns and hence $c \neq d$. It is easy to see that the elements c and d cannot appear again in the third row. This contradicts to Lemma 4.8 when $m > 1$. □

This tells us that a set of m^2 3-tuples over $\mathbb{Z}_m$ is a $SHF(3; m^2, m, \{1, 2\})$ if and only if any two distinct 3-tuples agree in at most one coordinate. This result can be stated in coding theory terms.

Corollary 4.10 *The size of the largest code over $\mathbb{Z}_m$ of length 3 with minimum distance 2 is m^2.*

We should point out that there will probably be many non-isomorphic $SHF(3; m^2, m, \{1, 2\})$, since there are many non-isomorphic Steiner triple systems for values of $m \equiv 1, 3 \pmod 6$.

Theorem 4.11 *There does not exist a $SHF(4; m^3, m, \{1, 2\})$ for each positive integer $m \geq 2$.*

Proof. Suppose a $SHF(4; m^3, m, \{1, 2\})$ exists and it is represented by a $4 \times m^3$ array whose entries are from $\mathbb{Z}_m$. Since an $SHF(3; m^2, m, \{1, 2\})$ is optimal, each row of the array must contain each of the elements from $\mathbb{Z}_m$ exactly m^2 times. Otherwise, one element will appear at least $m^2 + 1$ times and the other 3 rows of these columns will form an

$SHF(3; m^2+1, m, \{1,2\})$. Without loss of generality, suppose the columns of the array are permuted so that the first row is of the form $0000\cdots001111\cdots12222\cdots2\cdots m-1\ m-1\ m-1\ m-1\cdots m-1$. We now show there does not exist two columns of the form $(i,x,y,z)^T$ and $(j,x,y,z)^T$. If these two columns do appear in the matrix, then let $(i,a,b,c)^T$ be any other column with an i in row 1. Then $\{(i,x,y,z)^T\}$ and $\{(j,x,y,z)^T,(i,a,b,c)^T\}$ cannot be separated.

Now, if we remove the first row of the array, all the columns must be distinct and all m^3 3-tuples from $(\mathbb{Z}_m)^3$ appear as a column. Since $m \geq 2$, there must be two columns $(0,x,y,z)^T$ and $(0,x,a,b)^T$, where either $y \neq a$ or $z \neq b$ (easy to see such an x occurs). Similarly, there must exist a column $(i,c,a,b)^T$ in the array for some $i \neq 0$ or $c \neq x$. Now $\{(0,x,a,b)^T\}$ and $\{(0,x,y,z)^T,(i,c,a,b)^T\}$ cannot be separated. Hence, we have shown that no $SHF(4; m^3, m, \{1,2\})$ exists. □

One open question is what is the largest integer a so that an SHF$(4; m^2+a, m, \{1,2\})$ exists. The following shows that there is an SHF$(4; m^2+1, m, \{1,2\})$ for $m = 2, 3$.

Example 4.1 *There exist an SHF*$(4; 5, 2, \{1,2\})$ *and an SHF*$(4; 10, 3, \{1,2\})$ *as follows:*

$$\begin{pmatrix} 1 & 2 & 1 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 2 & 2 & 3 & 3 & 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 3 & 1 & 2 & 1 & 2 & 3 & 1 \\ 3 & 2 & 3 & 1 & 2 & 1 & 1 & 2 & 3 & 3 \\ 1 & 1 & 3 & 2 & 1 & 3 & 1 & 2 & 1 & 2 \end{pmatrix}$$

With some effort it can be shown that the SHF$(4; 5, 2, \{1,2\})$ *is optimal.*

In the following, we consider SHF with $\lambda = 2$, which can be used to construct CFFs of $d > 0$.

Lemma 4.12 *There exists a 2-SHF*$(4; m^2, m, \{1,2\})$ *for each positive integer* $m \geq 2$.

Proof. Let X be $\mathbb{Z}_m$ and $Y = X \times X$. For $(x,y) \in Y$, define $\phi_1(x,y) = x, \phi_2(x,y) = y, \phi_3(x,y) = x+y \pmod m$ and $\phi_4(x,y) = x-y \pmod m$. Suppose $C_1 = \{(x_1,y_1)\}, C_2 = \{(x_2,y_2),(x_3,y_3)\}$. We want to show that there are at least two functions separating C_1 and C_2.
Case 1. $x_1 \neq x_2, x_1 \neq x_3$. If $y_1 \neq y_2, y_1 \neq y_3$, then ϕ_1 and ϕ_2 separate C_1 and C_2. If $y_1 = y_2, y_1 \neq y_3$, then $x_3+y_3 = x_1+y_1$ and $x_3-y_3 = x_1-y_1$ cannot be both true since $x_3 \neq x_1$. So ϕ_1 and ϕ_3 or ϕ_1 and ϕ_4 separate C_1 and C_2. If $y_1 = y_2 = y_3$, then ϕ_1 and ϕ_3 separate C_1 and C_2.
Case 2. $x_1 = x_2, x_1 \neq x_3$. In this case, $y_2 \neq y_1$. If $y_1 \neq y_3$, then the situation is similar to Case 1. If $y_1 = y_3$, then ϕ_3 and ϕ_4 separate C_1 and C_2.
Case 3. $x_1 = x_2 = x_3$. In this case, $y_1 \neq y_2, y_2 \neq y_3, y_3 \neq y_1$. So ϕ_2 and ϕ_3 separate C_1 and C_2. □

Using Theorem 2.5 we have the following corollaries.

Corollary 4.13 *Suppose there exists a* $(2;d)$*-CFF*(v,b)*, then there exists a* $(2; 2d+1)$*-CFF*$(4v, b^2)$.

Corollary 4.14 *Suppose there exists a* $(2;d)$*-CFF*(v,b)*, then there exists a* $(2;2^td+2^t-1)$*-CFF*$(4^tv,b^{2^t})$*.*

Using the results Corollary 2.10, we have the following theorem.

Theorem 4.15 *There exists an* $(2;2^td+2^t-1)$*-CFF*$(4^tq(q+1-s),q^{\lceil\frac{(q+2-s)}{2}\rceil 2^t})$*, where* q *is a prime power,* $0\le s\le q-2$*.*

The SHF in Lemma 4.12 is also optimal, which can be proved using the following Lemma and Theorem 4.5 .

Lemma 4.16 *Suppose there exists a* 2*-SHF*$(N;n,m,\{w_1,w_2\})$*. Then there exists an SHF*$(N-1;n,m,\{w_1,w_2\})$*.*

Proof. Delete one function from the 2-SHF$(N;n,m,\{w_1,w_2\})$. □

Theorem 4.17 *There does not exists a* 2*-SHF*$(4;m^2+1,m,\{1,2\})$ *for each positive integer* m*.*

Proof. Conclusion comes from Lemma 4.16 and Theorem 4.5. □

5 A construction algorithm

In [11], an algorithm was given for finding a 2-CFF$_k(v,m)$, where $m>\frac{\binom{n}{\lceil k/2\rceil}}{\binom{k}{\lceil k/2\rceil}^2}$. This method can be generalized to the case of $d>0$.

The algorithm is as follows. Let $\mathcal{F}_0=\emptyset$ and $\mathcal{G}_0=\binom{X}{k}$ (So $\mathcal{G}_0$ contains all the k-subsets of an n-set X). If $\mathcal{F}_i,\mathcal{G}_i$ are defined, then let F be an arbitrary member of $\mathcal{G}_i$ and set

$$\mathcal{F}_{i+1}=\mathcal{F}_i\cup\{F\},\ \mathcal{G}_{i+1}=\mathcal{G}_i-\left\{G\in\binom{X}{k}:|G\cap F|\ge\left\lceil\frac{k+d}{2}\right\rceil\right\}.$$

The following result is simple.

Lemma 5.1 *Let* $F\in\binom{X}{k}$ *and let* $\mathcal{G}=\{G\in\binom{X}{k}:|G\cap F|\ge\lceil(k+d)/2\rceil\}$*. Then,*

$$|\mathcal{G}|=\sum_{i=\lceil(k+d)/2\rceil}^{k}\binom{k}{i}\binom{n-k}{k-i}.$$

Applying Lemma 5.1, we have

$$|\mathcal{G}_{i+1}-\mathcal{G}_i|\le\sum_{j=\lceil(k+d)/2\rceil}^{k}\binom{k}{j}\binom{n-k}{k-j}.$$

which gives following result.

Theorem 5.2 *There exists a* $(2;d)$*-*$CFF_k(v,m)$*, where*

$$m \geq \frac{\binom{n}{k}}{\sum_{i=\lceil (k+d)/2 \rceil}^{k} \binom{k}{i}\binom{n-k}{k-i}}.$$

Setting $d = 0$, we have a 2-CFF$_k(v,m)$, where

$$m \geq \frac{\binom{n}{k}}{\sum_{i=\lceil k/2 \rceil}^{k} \binom{k}{i}\binom{n-k}{k-i}}$$

This bound is slightly better than that given by Proposition 1 of [11].

6 Lower bounds and optimal results for small 2-CFF

In this section we consider small 2-CFFs. First we give some simple lemmas about $T(r,v)$.

Lemma 6.1 $T(r,v) \geq T_k(r,v)$.

Lemma 6.2 $T(r,v)+1 \leq T(r,v+1) \leq 2T(r,v)$

Proof. The first inequality is easy, because we can always add one block consisting of only the new element. For the second inequality, suppose the incidence matrix of an r-CFF$(v+1,b)$ is A. Without loss of generality, we assume that

$$A = \begin{pmatrix} \mathbf{1} & A_1 \\ \mathbf{0} & A_2 \end{pmatrix}.$$

Then both A_1 and A_2 are incidence matrix of r-CFF on v points. So the conclusion follows. □

We can view an incidence matrix of an r-CFF as a binary code. In this way, we have some relationship between CFFs and binary codes. For our purpose, we consider constant weight binary codes.

Let $A(N,D,w)$ be the maximal possible number of codewords in a binary code of length N, minimal distance D and weight w. Then we have the following lemma.

Lemma 6.3 $T(2,v) \geq T_{2e-1}(2,v) \geq A(v,2e,2e-1)$.

Proof. Write down all the codewords of the constant weight binary code as a matrix such that each row of the matrix is a codeword. Then it is easy to check that it is an incidence matrix of a 2-CFF. □

Using the previous lemma, tables of bounds on A$(v,2e,2e-1)$ [3] can be converted to tables of lower bounds on 2-CFFs. These lower bounds are listed in Table 1. However, we do not know whether these the CFFs obtained from the constant weight binary codes are optimal CFFs or not. For example, we know $T(2,12) \geq 20$ from Table 1. But we don't know whether $T(2,12) = 20$. The next few results prove that the CFFs obtained from the constant weight binary codes are indeed optimal for $v \leq 11$. This will be marked by an asterisk in the table.

We begin, for completeness sake, with Sperner's Theorem.

Theorem 6.4 *(Sperner's Theorem) If $\mathcal{F}$ is a family of subsets of an n-set in which no member of $\mathcal{F}$ contains another, then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.*

¿From Sperner's Theorem, we can prove the following simple but useful lemma.

Lemma 6.5 *Suppose $(X, \mathcal{B})$ is a 2-CFF(v, b). If $\mathcal{B}$ contains a block of size m, then $|\mathcal{B}| \leq 1 + \binom{v-m}{\lceil \frac{(v-m)}{2} \rceil}$.*

Proof. Let A be a block of $\mathcal{B}$ with cardinality m. Let B and C be two other distinct blocks of $\mathcal{B}$. As $(X, \mathcal{B})$ is a 2-CFF(v, b), then $B \setminus A$ cannot be a subset of $C \setminus A$ and vice versa. For if $B \setminus A$ is a subset of $C \setminus A$, then $B \subseteq A \cup C$, which is a contradiction. Hence, by Sperner's Theorem, we have the required result. □

Before using this lemma, we need to define the following concept. The *support* of a CFF is the the list of all block sizes (including multiplicities) of the CFF.

Using the above lemma, it is easy to show that the optimal 2-CFF(v, b), for $v \leq 6$ consists of v singleton blocks. For $v = 7$ and 8, an exhaustive computer search program was used to find the optimal CFFs. For $v = 7$, there are exactly 2 CFFs with different support: the all singleton CFF and the all tripleton CFF, which is the Steiner Triple System of order 7. This shows that two optimal CFFs exist with different supports, although each support consists of 1 block size. For $v = 8$, the optimal solution has 8 blocks but there are several optimal CFFs with different supports. One is the all singleton CFF. Another optimal CFF is the Steiner triple system of order 7 with one additional block of size 1 or 2 containing the eighth element. There is also the all tripleton CFF with every element having frequency 3. This shows that there are optimal CFFs that have more than one block size.

Before we examine the next 3 cases in detail, we prove the following useful lemma.

Lemma 6.6 *Suppose $b > T(2, v-1) + 1$. Then there are no blocks of size 1 or 2 in a 2-CFF(v, b).*

Proof. If there is a block of size 1 in the 2-CFF(v, b), then the element in that block has frequency 1. If that block is deleted we get a 2-CFF$(v-1, b-1)$ which is a contradiction. If there is a block of size 2, then at least one of 2 elements in the block has frequency 1 as otherwise this block could be covered by the one or two other blocks containing those elements. If the block containing the element of frequency 1 is deleted, a 2-CFF$(v-1, b-1)$ is produced which again is a contradiction. □

At this point, we need a definition and lemma from [11].

Definition 6.1 *Let $(X, \mathcal{B})$ be a set system. If $B \in \mathcal{B}$ and $A \subset B$, then we say A is a* private set *(of $\mathcal{B}$) if A does not appear as a subset of any other member of $\mathcal{B}$.*

The following results states that in any 2-CFF, if a block is partitioned into two parts, then one of the two parts must be a private set.

Lemma 6.7 *Let $(X, \mathcal{B})$ be a 2-CFF(v, b). If $B \in \mathcal{B}$, $B = A \cup C$ and $A \cap C = \emptyset$, then either A or C is a private set.*

Proof. Suppose the hypothesis is false and that both A and C are not private sets. Then there exists $E, F \subseteq \mathcal{B}$ such that $A \subseteq E$ and $C \subseteq F$, which implies $B = A \cup C \subseteq E \cup F$. But this contradicts the assumption that $(X, \mathcal{B})$ is a 2-CFF(v, b). □

Corollary 6.8 *Suppose $b > T(2, v-1) + 1$. Then a block of size k in a 2-CFF(v, b), can not intersect any other block in $k-1$ elements.*

Proof. If a block A of size k intersects another block B in $k-1$ elements, then we can let $A = C \cup \{a\}$, where $C \subset B$ and $|C| = k-1$. According to the previous lemma, $\{a\}$ is a private set. Therefore deleting A will produce a 2-CFF$(v-1, b-1)$. This is a contradiction. □

Theorem 6.9 $T(2, 9) = 12$ *and the 2-CFF that meets this bound is the Steiner Triple System of order* 9.

Proof. We assume that a 2-CFF(9,13) exists. By Lemma 6.5 and Lemma 6.6, we know that all blocks are of size 3. Clearly, some pair must occur twice violating Corollary 6.8. So consider a 2-CFF(9,12). Using Lemma 6.5 and Lemma 6.6, it can be shown that all block sizes are 3 and no pair is repeated. This CFF could only be the Steiner Triple System of order 9. □

We now give a useful lemma about the frequency of elements in a 2-CFF.

Lemma 6.10 *Suppose $b = T(2, v-1) + p$. Then all elements in a 2-CFF(v, b) must occur in at least p blocks.*

Proof. Assume some element in a 2-CFF(v, b) occurs in s blocks where $s < p$. If this element and the blocks it occurs in are deleted, then a 2-CFF$(v-1, b-s)$ is formed. This contradicts the hypothesis. □

We now proceed to show that $T(2, 10) = 13$.

Theorem 6.11 $T(2, 10) = 13$.

Proof. It suffices to show that $T(2, 10) \leq 13$, as it is easy to construct a 2-$CFF(10, 13)$. Suppose that there exists a 2-CFF$(10, 14)$, $(X, \mathcal{B})$. By Lemma 6.5 and Lemma 6.6, we know that the only block sizes are 3 and 4. There must be at least 42 elements in the 14 blocks so some element, say a, occurs at least 5 times. If all blocks have size 3, then some element occurs twice with a, violating Corollary 6.8. So some blocks must have size 4.

Case 1 (1 block of size 4): By Corollary 6.8, no pair of elements can occur twice in the CFF. By counting, we see that every pair of elements occur precisely once in the design. There must be an element a that occurs only in blocks of size 3. Since, in such a block, there are two pairs containing a, there are even number of pairs containing a. However, there should be 13 such pairs. Hence this case is impossible.

Case 2 (2 blocks of size 4): By Corollary 6.8, it is evident that the two blocks of size 4 contain twelve pairs of elements from X, and at least 11 distinct pairs. The 12 blocks of

size 3 contain 36 distinct pairs of elements from X, giving a total of at least 47 distinct pairs in the blocks of $\mathcal{B}$. Hence there exists two blocks with a common pair, at least one of which has size 3. This violates Corollary 6.8 and this case is ruled out.

Case 3 (3 or more blocks of size 4): Again, we note that two blocks of size 4 contain at least eleven distinct pairs. In addition, each of the remaining twelve blocks must contain at least three private pairs. This gives a total of at least $11 + 3(12) = 47$ distinct pairs in $\mathcal{B}$. This is impossible since $\binom{10}{2} = 45$. Hence this case is not possible.

Hence we have shown that there does not exist a 2-CFF$(10, 14)$. The conclusion follows. □

To continue, we need to use another definition from Erdös [11]

Definition 6.2 *Let $(X, \mathcal{B})$ be a set system. A set $A \subseteq X$ is* free*, if A is not a subset of any member of $\mathcal{B}$.*

Theorem 6.12 $T(2, 11) = 17$.

Proof. It suffices to show that $T(2, 11) \leq 17$, as we can easily construct a 2-CFF$(11, 17)$ using binary codes. Suppose there exists a 2-CFF$(11, 18)$ $(X, \mathcal{B})$. By Lemma 6.10, we know that each element must have frequency at least 5. So there must be a block of size at least 4. By Lemma 6.6 and Lemma 6.5, we know that the block sizes are 3, 4 or 5. Let there be a, b and c blocks of size 3, 4 and 5 respectively. Consider the sum of the private and free triples which must be less than or equal to $\binom{11}{3} = 165$. Consider a block of size 3, say $\{1, 2, 3\}$. First the 3-set itself is a private set. If the elements are partitioned 1 and $\{2, 3\}$, we know that 1 can not be private so the pair $\{2, 3\}$ is private and the triples $\{2, 3, 4\}, \{2, 3, 5\}, \ldots, \{2, 3, 11\}$ are free. So a block of size three generates 1 private triple and $3 \cdot 8 = 24$ free triples. Consider a block of size 4, say $\{1, 2, 3, 4\}$. Since a single element can not be private, the 4 triples in the block must be private. If the elements are partitioned $\{1, 2\}$ and $\{3, 4\}$, we know that at least one of the pairs is private, say $\{1, 2\}$, and the triples $\{1, 2, 5\}, \{1, 2, 6\}, \ldots, \{1, 2, 11\}$ are free. So a block of size 4 generates 4 private triples and $3 \cdot 7 = 21$ free triples. Consider a block of size 5, say $\{1, 2, 3, 4, 5\}$. If the elements are partitioned $\{1, 2\}$ and $\{3, 4, 5\}$, we know that either the pair or triple is private. If the pair is private then the triples $\{1, 2, 6\}, \{1, 2, 7\}, \ldots, \{1, 2, 11\}$ are free. So any block of size 5 has 10 such partitions and so generates $6s$ free triples and t private triples, where $s + t = 10$. But we have counted some free triples more than once. So let us consider a free triple $\{a, b, c\}$. It could have come from the following blocks:

$\{a, b, -\}$	$\{a, c, -\}$	$\{b, c, -\}$
$\{a, b, -, -\}$	$\{a, c, -, -\}$	$\{b, c, -, -\}$
$\{a, b, -, -, -\}$	$\{a, c, -, -, -\}$	$\{b, c, -, -, -\}$

Recall that the pairs listed in the blocks in the table must be private. It is clear that the free set could be generated by only one of the sets in a column. So at most, a particular free set could be generated by at most three blocks. So we must divide the numbers of free sets by three to ensure we do not over count these triples. We will call this the weighted count. In the case of a block of size 5, it means that a 2-3 partition could generate either

one private triple or at most 6/3=2 weighted free triples. Thus a block of size 5 generates at least 10 private or weighted free sets. Putting this together gives:

$$9a + 11b + 10c \leq 165$$

$$a + b + c = 18$$

This implies that $2b + c \leq 3$. The few cases that satisfy this condition can easily be ruled out by counting pairs in the design as in Theorem 6.11. Hence, we conclude that no 2-CFF$(11, 18)$ exists. □

Since we are also interested in the support of an optimal 2-CFF, we give the following theorem.

Theorem 6.13 *There are exactly four* 2*-CFF*$(10, 13)$*s with different supports.*

Proof. If an 2-CFF(10,13) contains a singleton block then the singleton block must be private or else this block would be contained in some other block, contradicting the definition of a 2-cover-free family. If this singleton block is deleted then the result must be a 2-CFF(9,12) which is the Steiner Triple system of order nine. So all 2-CFF(10,13)'s which have a singleton block have one block of size 1 and 12 blocks of size 3. If a 2-CFF(10,13) has a doubleton block then the doubleton block must contain a private element. If not, the union of 2 blocks each containing one of the elements of the doubleton block would contain the doubleton block violating the definition of a 2-cover-free family. If the doubleton block is deleted then we again get the 2-CFF(9,12). So any 2-CFF(10,13) which contains a doubleton block has one block of size 2 and 12 blocks of size 3.

By Lemma 6.5, we know there are no blocks of size more than 4 in a 2-CFF(10,13). So let us consider 2-CFF(10,13)s containing only blocks of sizes 3 and 4. Since any two blocks of size 4 can intersect in at most 2 elements, if there are at least three blocks of size 4 then they have at least $3 \cdot 6 - 3 \cdot 1 = 15$ distinct pairs. The remaining blocks, whether of size 3 or 4, contain 3 private pairs apiece. So there are at least 45 distinct pairs in the 2-CFF. So every possible pair appears in some block. Without loss of generality, there is only one way that the three blocks of size 4 can intersect while containing only 15 distinct pairs of elements, i.e. $\{\{1, 2, 3, 4\}, \{1, 2, 5, 6\}, \{1, 3, 5, 7\}\}$. The element 1 must appear with 8,9,10 and this can not be done in blocks of size only 3, as a block of size 4 and a block of size 3 can intersect in only 0 or 1 elements. So element 1 must appear with one or more of the elements 7,8 or 9 in a block of size 4. But the only block of size 4 that element 1 is allowed to appear in is $\{1, 4, 6, 7\}$ as otherwise we get three blocks of size 4 which violates the pair count or the definition of 2-CFF. So 3 blocks of size 4 leads to a contradiction.

So let us assume that there are exactly 2 blocks of size 4. As previous, there are at least 11 distinct pairs in the 2 blocks of size 4 and $3 \cdot 11 = 33$ private pairs in the 11 blocks of size 3 for a total of at least 44 distinct pairs in the 2-CFF. We may assume the blocks are $\{1, 2, 3, 4\}$ and $\{1, 2, 5, 6\}$. Then one of 7, 8 or 9, say 7 occurs with every other element. But 7 occurs only in blocks of size 3 where every pair is private. So this is impossible. So we must have 45 distinct pairs in the 2-CFF with exactly 2 blocks of size 4. One possibility for the blocks of size 4 is $\{1, 2, 3, 4\}$ and $\{1, 5, 6, 7\}$. In this case, element 1 must appear with elements 7, 8 and 9 in blocks of size 3 where all the pairs are private. But this is impossible.

The other possibility is $\{1,2,3,4\}$ and $\{5,6,7,8\}$ but then element 9 must appear with every other element in blocks of size 3 which is impossible. So there is at most 1 block of size 4.

The binary codes supply an example of a 2-CFF(10,13) with 13 blocks of size 3 and a 2-CFF(10,13) with 1 block of size 4 and 12 blocks of size 3 will be exhibited later. □

Many of the small optimum 2-CFF(v,b)s can be constructed from one-factorizations of K_{2n} where $4n-1 \geq v \geq 2n+3$. Add $v-2n$ new elements to $v-2n$ one factors so that each pair from the same one factor has the same new element added to it. Then delete extra pairs in the one-factors not used. This creates $(v-2n)n$ blocks of size 3. Finally add on a few blocks of size at least 3 containing only new elements. It is easy to check that this is a 2-CFF(v,b). Optimal CFFs with $v = 7, 10, 11$ can be made this way. A currently best 2-CFF(14,28) can also be constructed in this fashion.

As an example, we list the blocks of a 2-CFF$(10,13)$ as follows. We start with a one-factorization of K_6 and then add a,b,c,d to 4 of one factors. In the list, each column is formed from a one factor.

$$\begin{array}{cccc} 12a & 13b & 14c & 15d \quad abcd \\ 34a & 25b & 26c & 24d \\ 56a & 46b & 35c & 36d \end{array}$$

For $v = 7, 9, 13$, some of the currently best 2-CFFs are Steiner Triple Systems. For $v = 12$, a currently best 2-CFF can be made by deleting one element and the blocks it is in, from Steiner Triple System of order 13. Similarly, a S(3,5;17) is a current best 2-CFF(17,68). Again if one element and the blocks it is in are deleted from the S(3,5;17) we get a current best 2-CFF$(16, 48)$. Other interesting examples are quasi-symmetric BIBDs, see [7]. A quasi-symmetric BIBD(21,7,12) is a current best 2-CFF(21,120), a quasi-residual BIBD(22,7,16) is a current best 2-CFF(22,176). Finally, the BIBD(15,5,4) which only has block intersections 0,1,2 is a current best 2-CFF(15,42) and if one element and the blocks that contain it are deleted then we have the current best 2-CFF(14,28). All of these CFFs have only one block size.

So far we have always seen there exists an optimal or best 2-CFF with just one block size. But for some v there are many non-constant block size 2-CFFs. This leads to the following open question.

Open question 6.14 *Does there exist a value of v, for which no optimal 2-CFF$(v, T(2, v))$ has all its blocks sizes the same?*

7 Conclusion

In this paper, we have stated several new recursive constructions for $(2;d)$-CFF. We have also stated several results for separating hash families, which can be used for constructing cover-free families. Finally, we have constructed several optimal cover free families and placed bound on the optimal size for several more.

v	$T(2,v)$
3	3*
4	4*
5	5*
6	6*
7	7*
8	8*
9	12*
10	13*
11	17*
12	20
13	26
14	28
15	42
16	48
17	68
18	69
19	76
20	84
21	120
22	176
23	253

Table 1: Lower bounds for small 2-CFF (* means the bound is tight)

Acknowledgements

The authors thank the referees' useful comments on a previous version of this paper. R. Wei's research is supported by NSERC grant 239135-01 and G. H. J. van Rees's research is supported by NSERC grant 003358-04.

References

[1] M. Atici, S. S. Magliveras, D. R. Stinson and W.-D. Wei. Some recursive constructions for perfect hash families, *J. Combinatorial Designs* **4** (1996), 353-363.

[2] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data, *IEEE Tran. Information Theory* **44** (1998), 1897-1905. (*Lecture Notes in Computer Science* **963** (1995), 452-465 (Crypto '95)).

[3] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane and W.D. Smith, A new table of constant weight codes, *IEEE Tran. Information Theory* **36** (1990), 1334-1380.

[4] K. A. Bush, W. T. Federer,H. Pesotan and D. Raghavarao. New combinatorial designs and their application to group testing, *Journal of Statistical Planning and Inference* **10** (1984), 335–343.

[5] B. Chor, A. Fiat and M. Naor. Tracing traitors, in "Advances in Cryptology – Crypto '94", *Lecture Notes in Computer Science* **839** (1994), 480–491.

[6] B. Chor, A. Fiat, M. Naor and B. Pinkas. Tracing traitors, *IEEE Transactions on Information Theory* **46**(2000), 893–910.

[7] C. J. Colbourn and J. H. Dinitz, eds., *CRC Handbook of Combinatorial Designs*, CRC Press, Inc., 1996.

[8] A. G. Dyachkov, A. J. Macula and V. V. Rykov. New constructions of superimposed codes, *IEEE Information Theory*, **46** (2000), 248–290.

[9] M. Dyer, T. Fenner, A. Frieze and A. Thomason. On key storage in secure networks, *J. Cryptology* **8** (1995),189–200.

[10] A. G. Dyachkov, V. V. Rykov and A. M. Rashad. Superimposed distance codes, *Problems of Control and Information Theory* **18** (1989), 237–250.

[11] P. Erdös, P. Frankl and Z. Füredi. Families of finite sets in which no set is covered by the union of two others, *Journal of Combinatorial Theory A* **33** (1982), 158–166.

[12] P. Erdös, P. Frankl and Z. Füredi. Families of finite sets in which no set is covered by the union of r others, *Isreal Journal of Mathematics* **51** (1985), 75–89.

[13] E. Gafni, J. Staddon and Y. L. Yin. Efficient methods for integrating traceability and broadcast encryption, in "Advances in Cryptology – Crypto '99", *Lecture Notes in Computer Science* **1666**(1999), 372–387.

[14] J. A. Garay, J. Staddon and A. Wool, Long-lived broadcast encryption, in "Advances in Cryptology – Crypto' 00", *Lecture Notes in Computer Science* **1880**(2000), 335-353.

[15] F. K. Hwang and V. T. Sós. Non-adaptive hyper geometric group testing, *Studia Sci. Math. Hungar.* **22** (1987), 257–263.

[16] W. H. Kautz and R. C. Singleton. Nonrandom binary superimposed codes, *IEEE Trans. Inform. Theory* **10**(1964), 363–377.

[17] R. Kumar, S. Rajagopalan and A. Sahai. Coding constructions for blacklisting problems without computational assumptions, in "Advances in Cryptology –Crypto '99", *Lecture Notes in Computer Science* **1666** (1999), 609–623.

[18] C. J. Mitchell and F. C. Piper. Key storage in secure networks, *Discrete Applied Mathematics* **21** (1988), 215–228.

[19] R. Safavi-Naini and H. Wang. New results on multi-receiver authentication codes, in "Advances in Cryptology – Eurocrypt '98", *Lecture Notes in Computer Science* **1438** (1998), 527–541.

[20] J. N. Staddon, D. R. Stinson and R. Wei, Combinatorial properties of frameproof and traceability codes, *IEEE Tran. Information Theory* **47**(2001), 1042-1049.

[21] 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.

[22] 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.

[23] D. R. Stinson and R. Wei. Key preassigned traceability schemes for broadcast encryption, in "Selected Areas in Cryptology – SAC'98", *Lecture Notes in Computer Science* **1556** (1999), 144–156.

[24] R. Wei. On cover-free families, *Discrete Math.*, to appear.