*Discrete Mathematics and Theoretical Computer Science* DMTCS vol. **14:2**, 2012, 261–270

# Secure Frameproof Codes Through Biclique Covers

Hossein Hajiabolhassan[1,2†] and Farokhlagha Moazami[3‡]

[1] *Department of Mathematical Sciences, Shahid Beheshti University, Tehran, Iran*
[2] *School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*
[3] *Department of Mathematics, Alzahra University, Tehran, Iran*

*received 10th April 2012*, *revised 26th October 2012*, *accepted 15th November 2012*.

For a binary code $\Gamma$ of length $v$, a $v$-word $w$ produces by a set of codewords $\{w^1, \ldots, w^r\} \subseteq \Gamma$ if for all $i = 1, \ldots, v$, we have $w_i \in \{w_i^1, \ldots, w_i^r\}$. We call a code $r$-secure frameproof of size $t$ if $|\Gamma| = t$ and for any $v$-word that is produced by two sets $C_1$ and $C_2$ of size at most $r$, then the intersection of these sets is non-empty. A $d$-biclique cover of size $v$ of a graph $G$ is a collection of $v$ complete bipartite subgraphs of $G$ such that each edge of $G$ belongs to at least $d$ of these complete bipartite subgraphs. In this paper, we show that for $t \geq 2r$, an $r$-secure frameproof code of size $t$ and length $v$ exists if and only if there exists a 1-biclique cover of size $v$ for the Kneser graph $\mathrm{KG}(t, r)$ whose vertices are all $r$-subsets of a $t$-element set and two $r$-subsets are adjacent if their intersection is empty. Then we investigate some connection between the minimum size of $d$-biclique covers of Kneser graphs and cover-free families, where an $(r, w; d)$ cover-free family is a family of subsets of a finite set $X$ such that the intersection of any $r$ members of the family contains at least $d$ elements that are not in the union of any other $w$ members. The minimum size of a set $X$ for which there exists an $(r, w; d)$ cover-free family with $t$ blocks is denoted by $N((r, w; d), t)$. We prove that for $t > 2r$ and $r > s$, we have $bc_d(\mathrm{KG}(t, r)) \geq bc_m(\mathrm{KG}(t, s))$, where $m = N((r - s, r - s; d), t - 2s)$. Finally, we show that for any $1 \leq i < r$, $1 \leq j < w$, and $t \geq r + w$ we have $N((r, w; d), t) \geq N((r - i, w - j; m), t)$, where $m = N((i, j; d), t - r - w + i + j)$.

**Keywords:** cover-free family, secure frameproof code, biclique cover, Hadamard matrix

## 1 Introduction

Illegal copy is a major problem in digital data. *Frameproof codes* are one of many different techniques to prevent products against illegal copy that were first introduced by Boneh and Shaw [2]. To protect digital data, the distributor marks each copy uniquely with a codeword. These codewords have the property that an illegal copy can trace and back to the buyer. Also, these marks are impossible to remove or change for non-colluding buyers. But, whenever some malicious buyers (that are called pirates) are colluding, they can compare their copies and detect different positions. Colluding buyers have the ability to erase or change detected positions and construct some illegal marks. In order to formulate these conditions we

†Email: `hhaji@sbu.ac.ir`. This research was in part supported by a grant from IPM (No. 90050114).
‡Email: `f.moazami@alzahra.ac.ir`.

consider the following definitions and notations.
Let $\Gamma \subseteq \{0,1\}^v$ and $|\Gamma| = t$. $\Gamma$ is called a $(v,t)$-code and every element of $\Gamma$ is said to be a codeword. We write $w_i$ for the $i$th component of a word $w$. Also, the incidence matrix of $\Gamma$ is a $t \times v$ matrix whose rows are the codewords in $\Gamma$. Suppose $C = \{w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_d)}\} \subseteq \Gamma \subseteq \{0,1\}^v$. For $i \in \{1,2,\ldots,v\}$, the $i$th component is said undetectable for the coalition $C$ if

$$w_i^{(u_1)} = w_i^{(u_2)} = \cdots = w_i^{(u_d)}.$$

Let $U(C)$ be the set of undetectable components for $C$. The set

$$F(C) = \{x \in \{0,1\}^v : x|_{U(C)} = w^{(u_i)}|_{U(C)} \text{ for all } w^{(u_i)} \in C\}$$

represents all possible $v$-tuples that could be produced by the coalition $C$ by comparing the $d$ codewords.

**Definition 1** *An r-frameproof code is a subset $\Gamma \subseteq \{0,1\}^v$ such that for every $C \subseteq \Gamma$ where $|C| \leq r$, we have $F(C) \cap \Gamma = C$.*

Let $r - FPC(v,b)$ denotes an $r$-frameproof code $\Gamma \subseteq \{0,1\}^v$ such that $|\Gamma| = b$. The codewords in the set $\Gamma$are called registered codewords. Therefore, if we have an $r$-frameproof code, then the pirate in the set $C$ couldn't produce a registered illegal codeword other than their marks; that is not appropriate for the pirate copy. For more details about frameproof codes; see [1, 2, 11, 13, 14]. The following theorem was proved by Stinson, Trung, and Wei [10].

**Theorem 1** [10] *Suppose $\Gamma$ is an $r - FPC(v,b)$ with $b > 2r-1$. Suppose $D \subseteq \Gamma$, where $|D| = 2r-1$. Then there exists an unregistered word, say $maj(D) \in \{0,1\}^v$, such that $maj(D) \in F(C)$ for any $C \subseteq D$ with $|C| = r$.*

In view of the aforementioned theorem, $maj(D)$ is a codeword that is produced by the coalition of every $r$-subset of the set $D$. Therefore, in an $r - FPC$, there exist some illegal marks such that it is not possible to identify a pirate user. So they considered another condition and defined *secure frameproof codes* in which distributor is able to identify at least one pirate of the guilty coalitions.

**Definition 2** *Suppose that $\Gamma$ is a $(v,t)$-code. $\Gamma$ is said to be an $r$-secure frameproof code if for any $C_1, C_2 \subseteq \Gamma$ with $|C_1| \leq r$, $|C_2| \leq r$, and $C_1 \cap C_2 = \varnothing$, we have $F(C_1) \cap F(C_2) = \varnothing$. Also, $\Gamma$ is termed an $r - \mathrm{SFPC}(v,t)$, for short.*

In fact, when an illegal mark can be produced by two different $r$-subsets, in an $r - SFPC$, there exists at least one user in their intersection; whose can be considered as a pirate user. Stinson and Wei in [10] studied the relationship between binary secure frameproof codes and combinatorial aspects. In this paper, we establish the relationship between this concept and biclique cover. By a *biclique* we mean a bipartite graph with vertex set $(X,Y)$ such that every vertex in $X$ is adjacent to every vertex in $Y$. Note that every empty graph is a biclique. A $d$-*biclique cover* of a graph $G$ of size $s$ is a collection of $s$ bicliques of $G$ such that each edge of $G$ is in at least $d$ of the bicliques. The $d$-*biclique covering number* of $G$, denoted by $bc_d(G)$, is defined to be the minimum number of $s$ such that there exists a $d$-biclique cover of size $s$ for the graph $G$. For abbreviation, let $bc(G)$ stand for $bc_1(G)$.

**Definition 3** *Let $X$ be an $n$-set and $\mathcal{F} = \{B_1, \ldots, B_t\}$ be a family of subsets of $X$. $\mathcal{F}$ is called an $(r,w;d)$-cover-free family if for any two subsets $I,\ J \subseteq [t]$ such that $|I| = r$, $|J| = w$, and $I \cap J = \varnothing$, the following condition holds*

$$|(\bigcap_{i\in I} B_i) \setminus (\bigcup_{j \in J} B_j)| \geq d.$$

*We denote it briefly by* $(r, w; d) - CFF(n, t)$*.*

The minimum number of elements of $X$ for which there exists an $(r, w; d) - CFF$ with $t$ members is denoted by $N((r, w; d), t)$. For convenience, we use the notation $N((r, w), t)$ instead of $N((r, w; 1), t)$. This parameter has been studied extensively in the literature; see [4, 5, 7, 12]. The incidence matrix of an $(r, w; d) - CFF$ is a $t \times n$ binary matrix $A$ such that $a_{ij} = 1$ whenever $j \in B_i$ and $a_{ij} = 0$ otherwise. As usual, we denote by $[t]$ the set $\{1, 2, \ldots, t\}$, and denote by $\binom{[t]}{r}$ the collection of all $r$-subsets of$[t]$. The graph $I_t(r, w)$ is a bipartite graph with the vertex set $(\binom{[t]}{w}, \binom{[t]}{r})$ for which a $w$-subset is adjacent to an $r$-subset whenever their intersection is empty.

**Theorem 2** [5] *For any positive integers r, w, d, and t, where* $t \geq r + w$*, we have*

$$N((r, w; d), t) = bc_d(I_t(r, w)).$$

Throughout this paper, we only consider finite simple graphs. For a graph $G$, let $V(G)$ and $E(G)$ denote its vertex and edge sets, respectively. The *Kneser graph* $\mathrm{KG}(t, r)$ is the graph with vertex set $\binom{[t]}{r}$, and $A$ is adjacent to $B$ if $A \cap B = \varnothing$. A *homomorphism* from $G$ to $H$ is a map $\phi : V(G) \longrightarrow V(H)$ such that adjacent vertices in $G$ are mapped into adjacent vertices in $H$, i.e., $uv \in E(G)$ implies $\phi(u)\phi(v) \in E(H)$. In addition, if any edge in $H$ is the image of some edge in$G$, then $\phi$ is termed an onto-edge homomorphism. In this paper, by $A^c$ we mean the complement of the set $A$. In Section 2, we show that for $t \geq 2r$, an $r$-secure frameproof code of size $t$ and length $v$ exists if and only if there exists a 1-biclique cover of size $v$ for the Kneser graph $\mathrm{KG}(t, r)$. Also, we wish to investigate some connection between the $d$-biclique covering number of Kneser graphs and cover-free families. Moreover, we present an upper bound for the biclique covering number of Kneser graphs. In Section 3, we will look more closely at the biclique covering number of Kneser graphs. Also, it is shown that if there exists a Hadamard matrix of order $4d$, then $N((1, 1; d), 8d - 2) = 4d$ and $bc_{2d}(K_{8d}) = 4d$.

## 2 Secure Frameproof Codes

For a subset $A_i$ of $[t]$, the *indicator vector* of $A_i$ is the vector $v_{A_i} = (v_1, \ldots, v_t)$, where $v_j = 1$ if $j \in A_i$ and $v_j = 0$ otherwise.

**Theorem 3** *Let* $r$*,* $t$*, and* $v$ *be positive integers, where* $t \geq 2r$*. An* $r - \mathrm{SFPC}(v, t)$ *exists if and only if there exists a biclique cover of size* $v$ *for the Kneser graph* $\mathrm{KG}(t, r)$*.*

**Proof:** Assume that $A$ is the incidence matrix of an $r - \mathrm{SFPC}(v, t)$. Assign to the $j$th column of $A$, the set $A_j$ as follows

$$A_j \stackrel{\text{def}}{=} \{i | \, 1 \leq i \leq t, a_{ij} = 1\}.$$

Now, for $1 \leq j \leq v$, construct the bicliques $G_j$ with vertex set $(X_j, Y_j)$, where the vertices of$X_j$ are all $r$-subsets of $A_j$ and the vertices of $Y_j$ are all $r$-subsets of $A_j^c$, i.e., $[t] \setminus A_j$. It is easily seen that $G_j$, for $1 \leq j \leq v$, is a complete bipartite graph of $\mathrm{KG}(t, r)$. Let $C_1C_2$ be an arbitrary edge of $\mathrm{KG}(t, r)$. So $C_1, C_2 \subseteq [t]$, and $C_1 \cap C_2 = \varnothing$. Since $A$ is the incidence matrix of an $r - \mathrm{SFPC}(v, t)$, we have $F(C_1) \cap F(C_2) = \varnothing$. This means that there exists a bit position $i$ such that the $i$th bit of all code words of $C_1$ is $c_i$, for some $c_i \in \{0, 1\}$, and also the $i$th bit of all codewords of $C_2$ is $c_i + 1 \pmod 2$. So there exists a column of $A$ such that all entries corresponding to the rows of $C_1$ are equal to 1 and all entries corresponding to the rows of$C_2$ are equal to 0, or vice versa. Hence, $C_1C_2 \in E(G_i)$. Conversely, assume that we have a biclique cover of size $v$ for the graph $\mathrm{KG}(t,r)$. Our objective is to construct an $r$-SFPC. Label graphs in this biclique cover with $G_1,\ldots,G_v$, where $G_i$ has as its vertex set $(X_i,Y_i)$. Let $A_i$ be the union of sets that lie in $X_i$. Consider the indicator vectors of $A_i$'s , for $1\leq i\leq v$, and construct the matrix $A$ whose columns are these vectors. Assume that $C_1$ and $C_2$ are two disjoint subsets of $[t]$ of size $r$, i.e., $C_1C_2\in E(\mathrm{KG}(t,r))$. Let $G_i$ be the complete bipartite graph that covers the edge $C_1C_2$. Then in the $i$th column of the matrix $A$ all entries corresponding to the rows of $C_1$ are equal to 1 and all entries corresponding to the rows of $C_2$ are equal to 0, or vice versa. Consequently, $F(C_1)\cap F(C_2)=\varnothing$. $\square$

A *covering* of a graph $G$ is a subset $K$ of $V(G)$ such that every edge of $G$ has at least one end in $K$. The number of vertices in a minimum covering of $G$ is called the *covering number* of $G$ and denoted by$\beta(G)$. In [10], Stinson, Trung, and Wei construct an$r-\mathrm{SFPC}(2\binom{2r-1}{r-1},2r+1)$.

**Corollary 1** [10] *For any integer $r\geq 0$, there exists an $r-\mathrm{SFPC}(2\binom{2r-1}{r-1},2r+1)$.*

**Proof:** Easily, one can check that the biclique covering number of a graph $G$ without $C_4$ as a subgraph is equal to the covering number of $G$. On the other hand, $\mathrm{KG}(2r+1,r)$ does not contain $C_4$ as a subgraph. So $bc(\mathrm{KG}(2r+1,r)))=\beta(\mathrm{KG}(2r+1,r))$. Also, it is a well-known fact that $\beta(\mathrm{KG}(t,r))=\frac{t-r}{r}\binom{t-1}{r-1}$. An easy computation confirms the assertion. $\square$

In the next theorem, we show the relationship between the $d$-biclique cover of Kneser graphs and cover-free families.

**Theorem 4** *For any positive integers $r$, $d$, and $t$, where $t\geq 2r$, it holds that*

$$bc_{2d}(\mathrm{KG}(t,r))\leq N((r,r;d),t)\leq 2bc_d(\mathrm{KG}(t,r)).$$

**Proof:** First, assume that we have an optimal $(r,r;d)-CFF(n,t)$, i.e., $n=N((r,r;d),t)$ with incidence matrix $A$. Assign to the $j$th column of $A$, the set $A_j$ as follows

$$A_j\stackrel{\text{def}}{=}\{i|\ 1\leq i\leq t,\ \ a_{ij}=1\}.$$

Consider the biclique $G_j$ with vertex set $(X_j,Y_j)$, where the vertices of $X_j$ are all $r$-subsets of $A_j$ and the vertices of $Y_j$ are all $r$-subsets of $A_j^c$. Also, two vertices are adjacent if the subsets corresponding to these vertices are disjoint. It is not difficult to see that $G_j$'s, for $1\leq j\leq N((r,r;d),t)$, form a $2d$-biclique cover of $\mathrm{KG}(t,r)$. So $bc_{2d}(\mathrm{KG}(t,r))\leq N((r,r;d),t)$.
Conversely, assume that we have a $d$-biclique cover of $\mathrm{KG}(t,r)$. Label graphs in this biclique cover with $G_1,\ldots,G_l$, where $G_i$ has as its vertex set $(X_i,Y_i)$. Let $A_i$ be the union of sets that lie in $X_i$ and $B_i$ be the union of sets that lie in $Y_i$. Obviously, $A_i$ and $B_i$ are disjoint. Consider the indicator vectors of $A_i$'s and $B_i$'s, for $i=1,\ldots,l$. Construct the matrix $A$ whose columns are these vectors. Then $A$ is the incidence matrix of an $(r,r;d)-CFF(2l,t)$. So $N((r,r;d),t)\leq 2bc_d(\mathrm{KG}(t,r))$. $\square$

**Corollary 2** *For any positive integers $r$, and $t$, where $t\geq 2r$, it holds that*

$$bc_2(\mathrm{KG}(t,r))\leq N((r,r),t)\leq 2bc(\mathrm{KG}(t,r)).$$

A similar result has been obtained by Stinson et al. [10].

**Theorem 5** [10] *Let $r$ and $t$ be positive integers, where $t\geq 2r$, then*

**1.** *If there exists an $r-SFPC(v,t)$, then there exists an $(r,r)-CFF(2v,t)$.*

**2.** *Any $(r,r)$-cover free family is an $r$-secure frameproof code.*

Stinson et al. [10] have obtained the following upper bounds for $SFPC$.

**Theorem 6** [10] *Suppose that $r$ and $t$ are positive integers and $p = 1 - \frac{1}{2^{2r-1}}$. If*

$$v \geq \frac{\ln(\frac{1}{2}\binom{t}{r}\binom{t-r}{r})}{-\ln p},$$

*then there exists an $r - SFPC(v,t)$.*

The following upper bound is shown in Deng et al. [3], by the Lovász Local Lemma.

**Theorem 7** [3] *There exists an $r - SFPC(v,t)$ if*

$$v \geq \frac{\ln(e(\binom{t}{r}\binom{t-r}{r} - \binom{t-2r}{r}\binom{t-3r}{r}))}{-\ln p},$$

*where*

$$p = 1 - \frac{1}{2^{2r-1}}.$$

Let $p = 1 - \frac{1}{2^{2r-1}}$. Using the approximation $e^{-x} \approx 1 - x$, if we set $x = \frac{1}{2^{2r-1}}$, then we can see that

$$\frac{1}{-\ln p} \approx 2^{2r-1}.$$

In the next theorem, by the alternation method, we present a bound that is a slight improvement of Theorem 6. Also, it is a slight improvement of Theorem 7 provided that $t$ is not large relative to $r$.

**Theorem 8** *Let $r$ and $t$ be positive integers. If $t > 3r$ and*

$$v \geq 2^{2r-1}(1 + \ln(\binom{\lceil \frac{t}{2} \rceil}{r}\binom{\lfloor \frac{t}{2} \rfloor}{r}))\prod_{i=0}^{r-1}(1 - \frac{1}{t-2i+1}),$$

*then there exists an $r - SFPC(v,t)$.*

**Proof:** We show that if $v \geq \lfloor 2^{2r-1}(1 + \ln(\binom{\lceil \frac{t}{2} \rceil}{r}\binom{\lfloor \frac{t}{2} \rfloor}{r}))\prod_{i=0}^{r-1}(1 - \frac{1}{t-2i+1})\rfloor$, then there exists a biclique cover of size $v$ for the Kneser graph $\mathrm{KG}(t,r)$. Let $\mathcal{A}$ be $\binom{[t]}{\lceil \frac{t}{2} \rceil}$. For every member of $\mathcal{A}$, say $A_i$, we can construct the biclique $G_i$ with vertex set $(X_i, Y_i)$, where the vertices of $X_i$ are all $r$-subsets of $A_i$ and the vertices of $Y_i$ are all $r$-subsets of $A_i^c$. We define $\mathcal{B}$ to be the collection of these bicliques. Let $p \in [0,1]$ be arbitrary, later, we specify an optimized value for $p$. Let us pick, randomly and independently, each biclique of $\mathcal{B}$ with probability $p$ and $\mathcal{F}$ be the random set of all bicliques picked and let $Y_{\mathcal{F}}$ be the set of all edges $AB$ of the graph $\mathrm{KG}(t,r)$ which are not covered by the set $\mathcal{F}$. The expected value of $|\mathcal{F}|$ is clearly $\binom{t}{\lceil \frac{t}{2} \rceil}p$. For every edge $AB$, $pr(AB \in Y_{\mathcal{F}}) = (1-p)^l$ where $l = 2\binom{t-2r}{\lceil \frac{t}{2} \rceil - r}$. So the expected value of the $|\mathcal{F}| + |Y_{\mathcal{F}}|$ is at most

$$\binom{t}{\lceil \frac{t}{2} \rceil}p + \frac{1}{2}\binom{t}{r}\binom{t-r}{r}(1-p)^{2\binom{t-2r}{\lceil \frac{t}{2} \rceil - r}}.$$

If we set $\mathcal{F}' = \mathcal{F} \bigcup Y_{\mathcal{F}}$, then clearly all edges of the graph $\mathrm{KG}(t,r)$ are covered by $\mathcal{F}'$. So we want to estimate $p$ such that $|\mathcal{F}'|$ is minimum. For convenient, we bound $1 - p \leq e^{-p}$ to obtain

$$E(|\mathcal{F}| + |Y_{\mathcal{F}}|) \leq \binom{t}{\lceil \frac{t}{2} \rceil}p + \frac{1}{2}\binom{t}{r}\binom{t-r}{r}e^{-2\binom{t-2r}{\lceil \frac{t}{2} \rceil - r}p}.$$

The right hand side is minimized at $p = \frac{\ln \alpha}{\beta}$, which $\alpha = \binom{\lceil \frac{t}{2} \rceil}{r}\binom{\lfloor \frac{t}{2} \rfloor}{r}$ and $\beta = 2\binom{t-2r}{\lceil \frac{t}{2} \rceil - r}$ where $p \in [0,1]$ if $t$ is sufficiently large respect to $r$ (e.g., $t > 3r$). So we have an $r - SFPC(v,t)$ that

$$v \leq \frac{\binom{t}{\lceil \frac{t}{2} \rceil}}{2\binom{t-2r}{\lceil \frac{t}{2} \rceil - r}}(1 + \ln(\binom{\lceil \frac{t}{2} \rceil}{r}\binom{\lfloor \frac{t}{2} \rfloor}{r}))).$$

Furthermore, it is straightforward to check that

$$\frac{\binom{t}{\lceil \frac{t}{2} \rceil}}{2\binom{t-2r}{\lceil \frac{t}{2} \rceil - r}} \leq 2^{2r-1}\prod_{i=0}^{r-1}(1 - \frac{1}{t-2i+1}).$$

Hence, the bound follows. $\square$

# 3 Biclique Cover of Kneser Graphs

By the mentioned results in the previous section, it may be of interest to find some bounds for the biclique covering number of Kneser graphs.

**Theorem 9** *For any positive integers d, r, s, and t, where $t > 2r$ and $r > s$, we have*

$$bc_d(\mathrm{KG}(t, r)) \geq bc_m(\mathrm{KG}(t, s)),$$

*where $m = N((r - s, r - s; d), t - 2s)$.*

**Proof:** Let $\{G_1, G_2, \ldots, G_l\}$ be an optimal $d$-biclique cover of $\mathrm{KG}(t, r)$. Also, assume that $G_i$ has as its vertex set $(X_i, Y_i)$. Let $A_i$ and $B_i$ be the union of sets that lie in $X_i$ and $Y_i$, respectively. For any $1 \leq i \leq l$, consider the biclique $G'_i$, as a subgraph of $\mathrm{KG}(t, s)$, with vertex set $(X'_i, Y'_i)$, where $X'_i$ is the set of all $s$-subsets of $A_i$ and $Y'_i$ is the set of all $s$-subsets of $B_i$. One can check that$G'_i$'s cover all edges of $\mathrm{KG}(t, s)$. Moreover, any edge $UV \in E(\mathrm{KG}(t, s))$ is contained in at least $m$-bicliques, where $m = N((r-s, r-s; d), t-2s)$. To see this, consider the bipartite graph $I_{\{U,V\}}$ (as an induced subgraph of $\mathrm{KG}(t, r)$) with vertex set $(X_U, Y_V)$, where

$$X_U = \{W |\ U \subseteq W \subseteq [t], W \cap V = \emptyset, |W| = r\}$$
$$Y_V = \{W |\ V \subseteq W \subseteq [t], W \cap U = \emptyset, |W| = r\}.$$

It is a simple matter to check that $I_{\{U,V\}}$ and $I_{t-2s}(r - s, r - s)$ are isomorphic. Also, if $G_j$ covers any edge of $I_{\{U,V\}}$, then $UV$ is contained in $G'_j$. Consequently, by Theorem 2 the assertion follows. $\square$

In view of the proof of Theorem 9, similarly, one can extend any biclique of $I_t(r, w)$ to a biclique of $I_t(r - i, w - j)$. Consequently, we have the following theorem.

**Theorem 10** *Let d, r, w, and t be positive integers, where $t \geq r + w$. For any $1 \leq i < r$ and $1 \leq j < w$, we have $N((r, w; d), t) \geq N((r - i, w - j; m), t)$, where $m = N((i, j; d), t - r - w + i + j)$.*

The fractional biclique covering number $bc^*(G)$ is defined as follows

$$bc^*(G) = \inf_d \frac{bc_d(G)}{d} = \lim_{d\to\infty} \frac{bc_d(G)}{d}.$$

It is known that if a graph is edge-transitive, then one can compute its fractional biclique covering number, see [9] for more about fractional graph theory.

**Theorem 11** [9] *For every non-empty edge-transitive graph G,*

$$bc^*(G) = \frac{|E(G)|}{B(G)},$$

*where $B(G)$ is the maximum number of edges among the bicliques of G.*

The next result is a consequence of Theorem 10.

**Theorem 12** [12] *Let $d$, $r$, $w$, $i$, $j$, and $t$ be non-negative integers, where $t \geq r + w$, $1 \leq i < r$, and $1 \leq j < w$. Then*

$$N((r,w;d),t) \geq N((i,j;d),t-r-w+i+j) \min_{w-j \leq m \leq t-r+i} \frac{\binom{t}{m}}{\binom{t-r-w+i+j}{m-w+j}}.$$

**Proof:** In view of definition of fractional biclique cover and since $bc_{ts}(G) \leq s.bc_t(G)$ for every positive integers $t$ and $s$, one can conclude that for every graph $G$, we have $t.bc^*(G) \leq bc_t(G)$. By this fact and using Theorem 10, we have

$$N((r,w;d),t) \geq N((i,j;d),t-r-w+i+j) bc^*(I_t(r-i,w-j)). \tag{1}$$

The graph $I_t(r,w)$ is an edge-transitive graph. Therefore, using Theorem 11 and an easy calculation

$$bc^*(I_t(r,w)) = \min_{t'+t''=t} \frac{\binom{t}{r}\binom{t-r}{w}}{\binom{t'}{r}\binom{t''}{w}} = \min_{w \leq m \leq t-r} \frac{\binom{t}{m}}{\binom{t-r-w}{m-w}}.$$

Therefore, according to the inequality 1 it follows that

$$N((r,w;d),t) \geq N((i,j;d),t-r-w+i+j) \min_{w-j \leq m \leq t-r+i} \frac{\binom{t}{m}}{\binom{t-r-w+i+j}{m-w+j}}.$$

□

We know that the image of a biclique under a graph homomorphism is a biclique. This leads us to the following lemma.

**Lemma 1** *Let $G$ and $H$ be two graphs and $\phi : G \to H$ be an onto-edge homomorphism. Also, assume that $d$ and $t$ are positive integers and for any edge $e \in E(H)$, $bc_d(\phi^{-1}(e)) \geq t$. Then $bc_d(G) \geq bc_t(H)$.*

**Proof:** Let $\{K_1, K_2, \ldots, K_l\}$ be an optimal $d$-biclique cover of $G$. One can check that for any $0 \leq i \leq l$, $\phi(K_i)$ is a biclique and the family $\{\phi(K_1), \phi(K_2), \ldots, \phi(K_l)\}$ is a $t$-biclique cover of $H$. □

**Proposition 1** *For any positive integers $t$ and $r$, where $t > 2r$, we have*

$$bc_d(\mathrm{KG}(t,r)) \geq bc_{3d}(\mathrm{KG}(t-2,r-1)).$$

**Proof:** First, we present an onto-edge homomorphism $\phi$ from $\mathrm{KG}(t,r)$ to $\mathrm{KG}(t-2,r-1)$. To see this, for every vertex $A$ of $\mathrm{KG}(t,r)$, define $\phi(A) := A'$ as follows. If $A$ does not contain both $t$ and $t-1$, then define $A' := A \setminus \{maxA\}$. Otherwise, set $A' := \{x\} \cup A \setminus \{t, t-1\}$, where $x$ is the maximum element of $[t-2]$ absent from $A$. It is simple to check that the subgraph induced by the inverse image of any edge of $\mathrm{KG}(t-2,r-1)$ contains an induced cycle of size six or an induced matching of size three. Hence, in view of Lemma 1, if $\{K_1, \ldots, K_l\}$ is a $d$-biclique cover of $\mathrm{KG}(t,r)$, then $\{\phi(K_1), \ldots, \phi(K_l)\}$ is a $3d$-biclique cover of $\mathrm{KG}(t-2,r-1)$. □

The aforementioned results motivate us to consider the following question.

**Question 1** *Let $d$, $r$, and $t$ be positive integers, where $t > 2r$. What is the exact value of $bc_d(\mathrm{KG}(t,r))$?*

Determining the exact value of the parameter $N((r, w; d), t)$, even for special $r$, $w$, $d$ and $t$, is an interesting and challenging problem that is studied in the literature; see [5, 6, 7, 8]. An $n \times n$ matrix $H$ with entries $+1$ and $-1$ is called a *Hadamard matrix* of *order* $n$ whenever $HH^t = nI$. It is not difficult to see that any two columns of $H$ are also orthogonal. If we permute rows or columns or if we multiply some rows or columns by $-1$, then this property does not change. Two such Hadamard matrices are called *equivalent*. For a given Hadamard matrix, we can find an equivalent one for which the first row and the first column consist entirely of $+1$ï¿$\frac{1}{2}$s. Such a Hadamard matrix is called *normalized*. We will denote by $K^-_{m,m}$ the complete bipartite graph with a perfect matching removed. Obviously, $K^-_{m,m}$ is isomorphic to $I_m(1, 1)$.

**Theorem 13** *Let $d$ be a positive integer such that there exists a Hadamard matrix of order $4d$, then*

**1.** $bc_{2d}(K_{8d}) = 4d$,

**2.** $N((1, 1; d), 8d - 2) = bc_d(K^-_{8d-2,8d-2}) = 4d$.

**Proof:** Let $H = [h_{ij}]$ be a Hadamard matrix of order $4d$. Suppose that $K_{8d}$ has $\{u_1, \ldots, u_{4d}, v_1, \ldots, v_{4d}\}$ as its vertex set. For the $j$th column of $H$, two sets $X_j$ and $Y_j$ are defined as follows

$$X_j := \{u_i|h_{ij} = +1\} \cup \{v_i|h_{ij} = -1\} \;\; \& \;\; Y_j := \{u_i|h_{ij} = -1\} \cup \{v_i|h_{ij} = +1\}.$$

By constructing a bipartite graph $G_j$ with vertex set $(X_j, Y_j)$, indeed, we assign a biclique to each column. It is well-known that for any two rows of a Hadamard matrix, the number of columns for which corresponding entries in these rows are different in sign, are equal to $2d$. So, for $i \neq j$ the edges $u_iu_j$, $v_iv_j$, and $u_iv_j$ of the graph $K_{8d}$ are covered by $2d$ bicliques. Also, for the edge $u_iv_i$, there exist $4d$ bicliques that cover it. According to the above argument every edge is covered at least $2d$ times, so $bc_{2d}(K_{8d}) \leq 4d$. On the other hand, for every graph $G$, we have $\frac{|E(G)|}{B(G)} \leq \frac{bc_d(G)}{d}$, where $B(G)$ is the maximum number of edges among the bicliques of $G$. Therefore,

$$4d - \tfrac{1}{2} \leq bc_{2d}(K_{8d}).$$

Since $bc_{2d}(K_{8d})$ is an integer, we have $4d \leq bc_{2d}(K_{8d})$ which completes the proof. For the proof of the second part, assume that $H$ is a normalized Hadamard matrix of order $4d$. Delete the first row of $H$ and denote it by $H' = [h'_{ij}]$. Also, assume that $K^-_{8d-2,8d-2}$ has $(X, Y)$ as its vertex set where $X = \{u_1, \ldots, u_{4d-1}, v_1, \ldots, v_{4d-1}\}$, $Y = \{u'_1, \ldots, u'_{4d-1}, v'_1, \ldots, v'_{4d-1}\}$, and $u_iu'_i, v_iv'_i \notin E(K^-_{8d-2,8d-2})$. Assign to the $j$th column of $H'$, two sets $X_j$ and $Y_j$ as follows

$$X_j := \{u_i|h'_{ij} = +1\} \cup \{v_i|h'_{ij} = -1\} \quad \& \quad Y_j := \{u'_i|h'_{ij} = -1\} \cup \{v'_i|h'_{ij} = +1\}.$$

By the same argument in the first part of the proof and using the well-known fact that in $H'$ every two distinct rows $i, j$ and for any $a, b \in \{-1, +1\}$ there are exactly $d$columns that the corresponding entries are $a$ and $b$ in the rows $i$ and $j$, respectively, one can see that every edge is covered at least $d$ times. So $bc_d(K^-_{8d-2,8d-2}) \leq 4d$. On the other hand, $4d - \frac{2d}{4d-1} \leq bc_d(K^-_{8d-2,8d-2})$, and $\frac{2d}{4d-1} < 1$. Therefore, $4d \leq bc_d(K^-_{8d-2,8d-2})$ which establishes the second part. $\square$

## Acknowledgements

This paper has been revised and resubmitted for review while Hossein Hajiabolhassn was on leave at Technical University of Denmark (the academic year 2012-2013). Hossein Hajiabolhassan is grateful to professor Carsten Thomassen for his hospitality and support. Also, the authors wish to thank the anonymous referees for their useful comments.


## References


[1] Simon R. Blackburn. Frameproof codes. *SIAM J. Discrete Math.*, 16(3):499–510 (electronic), 2003.

[2] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. *IEEE Trans. Inform. Theory*, 44(5):1897–1905, 1998.

[3] D. Deng, D. R. Stinson, and R. Wei. The Lovász local lemma and its applications to some combinatorial arrays. *Des. Codes Cryptogr.*, 32(1-3):121–134, 2004.

[4] A. D'yachkov, P. Vilenkin, and S. Yekhanin. Upper bounds on the rate of superimposed $(s, l)$-codes based on engel's inequality. In *Proceedings of the International Conf. on Algebraic and Combinatorial Coding Theory (ACCT)*, pages 95–99, 2002.

[5] H. Hajiabolhassan and F. Moazami. Some new bounds on cover-free families through biclique covers. *Discrete Math.*, 312(24):3626–3635, 2012.

[6] Hyun Kwang Kim, Vladimir Lebedev, and Dong Yeol Oh. Some new results on superimposed codes. *J. Combin. Des.*, 13(4):276–285, 2005.

[7] Sh. Kh. Kim and V. S. Lebedev. On the optimality of trivial $(w, r)$-cover-free codes. *Problemy Peredachi Informatsii*, 40(3):13–20, 2004.

[8] P. C. Li, G. H. J. van Rees, and R. Wei. Constructions of 2-cover-free families and related separating hash families. *J. Combin. Des.*, 14(6):423–440, 2006.

[9] E. R. Scheinerman and D. H. Ullman. *Fractional graph theory*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, 1997. A rational approach to the theory of graphs, With a foreword by Claude Berge, A Wiley-Interscience Publication.

[10] D. R. Stinson, Tran van Trung, and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Statist. Plann. Inference*, 86(2):595–617, 2000. Special issue in honor of Professor Ralph Stanton.

[11] D. R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM J. Discrete Math.*, 11(1):41–53 (electronic), 1998.

[12] D. R. Stinson and R. Wei. Generalized cover-free families. *Discrete Math.*, 279(1-3):463–477, 2004. In honour of Zhu Lie.

[13] Gábor Tardos. Optimal probabilistic fingerprint codes. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 116–125 (electronic), New York, 2003. ACM.

[14] Gábor Tardos. Optimal probabilistic fingerprint codes. *J. ACM*, 55(2):Art. 10, 24, 2008.