Secure Frameproof Code Through Biclique Cover

Hossein Hajiabolhassan* and Farokhlagha Moazami†

*Department of Mathematical Sciences
Shahid Beheshti University, G.C.
P.O. Box 1983963113, Tehran, Iran
School of Mathematics
Institute for Research in Fundamental Sciences (IPM)
P.O. Box 193955746, Tehran, Iran
hhaji@sbu.ac.ir
†Department of Mathematics
Alzahra University
P.O. Box 1993891176, Tehran, Iran
f.moazami@alzahra.ac.ir

Abstract

For a binary code Γ of length v, a v-word w produces by a set of codewords \{w^1, \ldots, w^r\} ⊆ Γ if for all i = 1, \ldots, v, we have \(w_i \in \{w^1_i, \ldots, w^r_i\}\). We call a code r-secure frameproof of size t if |Γ| = 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 nonempty. 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 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 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. Also, we present an upper bound for 1-biclique covering number of Kneser graphs.

Key words: cover-free family, secure frameproof code, biclique cover, Hadamard matrix.

Subject classification: 05B40.

1 Introduction

Frameproof codes were first introduced by Boneh and Shaw [2]. 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 code word. We write \(w_i\) for the ith 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 \(C = \{w^{(u_1)}, w^{(u_2)}, \ldots, w^{(u_d)}\}\) ⊆ \(\Gamma \subseteq \{0, 1\}^v\). For \(i \in \{1, 2, \ldots, v\}\), the ith component is said undetectable for \(C\) if

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

*This research was in part supported by a grant from IPM (No. 90050114).
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 they jointly hold.

**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 $F(C) \cap \Gamma = C$.

*See [1] [2] [6] [8] [9] for more details about frameproof codes. The following theorem was proved by Stinson and Wei [5].*

**Theorem A.** [5] 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 $\text{maj}(D) \in \{0, 1\}^v$, such that $\text{maj}(D) \in F(C)$ for any $C \subseteq D$ with $|C| = r$.

In view of the aforementioned theorem, it is not possible to identify a pirate user in an $r$-FPC($v, b$). So they were considered a weaker 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 $C_1 \cap C_2 = \emptyset$, we have $F(C_1) \cap F(C_2) = \emptyset$. Also, $\Gamma$ is termed an $r$-SFPC($v, t$), for short.

Stinson and Wei in [5] 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 $G$.

**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 $I, J \in [t]$ such that $|I| = r$, $|J| = w$, and $I \cap J = \emptyset$ the following condition holds
$$\bigcap_{i \in I} B_i \nsubseteq \bigcup_{j \in J} B_j.$$ We denote it briefly by $(r, w) - \text{CFF}(n, t)$.

The minimum number of elements for which there exists an $(r, w; d) - \text{CFF}$ with $t$ blocks is denoted by $N((r, w; d), t)$. The incidence matrix of an $(r, w; d) - \text{CFF}$ 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 $(\binom{[t]}{w}, \binom{[t]}{r})$ which a $w$-subset is adjacent to an $r$-subset whenever their intersection is empty.
Theorem B. [4] For any positive integers \( r, w, d, \) and \( t \), where \( t \geq r + w \), we have
\[
N((r, w; d), t) = bc_d(I_t(r, w)).
\]

For abbreviation, let \( bc(G) \) stand for \( bc_1(G) \). The Kneser graph \( KG(t, r) \) is the graph with vertex set \( \binom{[t]}{r} \), and \( A \) is adjacent to \( B \) if \( A \cap B = \emptyset \). 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. A homomorphism from \( G \) to \( H \) is a map \( \phi : V(G) \to V(H) \) 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 the next section, 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 \( KG(t, r) \). Also, we wish to investigate some connection between the \( d \)-biclique covering number of Kneser graphs and cover-free families. Finally, we present an upper bound for the biclique covering number of Kneser graphs.

\section{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 1. Let \( r, t, \) and \( v \) be positive integers, where \( t \geq 2r \). An \( r \)-SFPC\((v, t) \) exists if and only if there exists a biclique cover of size \( v \) for the Kneser graph \( KG(t, r) \).

Proof. Assume that \( A \) is the incidence matrix of an \( r \)-SFPC\((v, t) \). Assign to the \( j \)th column of \( A \), the set \( A_j \) as follows
\[
A_j \overset{\text{def}}{=} \{ i | 1 \leq i \leq t, a_{ij} = 1 \}.
\]

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 \( A^c_j \) 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 \( KG(t, r) \). Let \( C_1C_2 \) be an arbitrary edge of \( KG(t, r) \). So \( C_1, C_2 \subseteq [t] \), and \( C_1 \cap C_2 = \emptyset \). Since \( A \) is the incidence matrix of an \( r \)-SFPC\((v, t) \), we have \( F(C_1) \cap F(C_2) = \emptyset \). 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 \( c_i + 1 \) (mod 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, \( C_1C_2 \in E(G_t) \). Conversely, assume that we have a biclique cover of size \( v \) for the graph \( KG(t, r) \). 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 \( A_i \), 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,
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, $F(C_1) \cap F(C_2) = \emptyset$.

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 [5], Stinson, Trung, and Wei construct an $r$-SFPC($2^{(2r-1)/r}, 2r+1$).

**Corollary 1.** [5] For any integer $r \geq 0$, there exists an $r$-SFPC($2^{(2r-1)/r}, 2r+1$).

**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 KG($2r+1, r$) does not contain $C_4$ as a subgraph. So $bc(KG(2r+1, r)) = \beta(KG(2r+1, r))$. Also, it is a well-known fact that $\beta(KG(t, r)) = \frac{t + r}{t - 1}$. An easy computation confirms the assertion. 

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

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

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

**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

$$A_j \equiv \{i | 1 \leq i \leq t, \ a_{ij} = 1\}.$$ 

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 $1 \leq j \leq t$, form a $2d$-biclique cover of $KG(t, r)$. So $bc_{2d}(KG(t, r)) \leq N((r, r; d), t)$.

Conversely, assume that we have a $d$-biclique cover of $KG(t, r)$. Label graphs in this biclique cover with $G_1, \ldots, G_t$, 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 $N((r, r; d), t) \leq 2bc_d(KG(t, r))$.

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

**Theorem 3.** For any positive integers $d$, $r$, $s$, and $t$, where $t > 2r$ and $r > s$, we have

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

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

4
The aforementioned results motivate us to consider the following question.

\[ \text{then} \]

\[ \text{\{three. Hence, in view of Lemma 1, if} \]

\[ KG(\text{is simple to check that the subgraph induced by the inverse image of any edge of} \]

\[ \text{set} \]

\[ A \]

\[ 2 \]

\[ \text{Proof.} \]

\[ \text{Let} \]

\[ \text{assume that} \]

\[ G_i \]

\[ \text{has as its vertex set} \]

\[ (X_i, Y_i) \]. \text{Let} \[ A_i \] \text{and} \[ B_i \] \text{be the union of sets that lie in} \[ X_i \] \text{and} \[ Y_i \], respectively. \text{For any} \[ 1 \leq i \leq l \], \text{consider the bijection} \[ G_i' \], as a subgraph of \[ KG(t, s) \], with vertex set \[ (X_i', Y_i') \], where \[ X_i' \] \text{is the set of all} \[ s \]-subsets of \[ A_i \] \text{and} \[ Y_i' \] \text{is the set of all} \[ s \]-subsets of \[ B_i \]. \text{One can check that} \[ G_i' \] \text{s cover all edges of} \[ KG(t, s) \]. \text{Moreover, any edge} \[ UV \in E(KG(t, s)) \] \text{is contained in at least} \[ m \]-bicliques, where \[ m = N((r - s, r - s; d), t - 2s) \]. \text{To see this, consider the bipartite graph} \[ I_{U,V} \] \text{as an induced subgraph of} \[ KG(t, r) \] \text{with vertex set} \[ (X_U, Y_V) \], \text{where} \[
\begin{align*}
X_U &= \{W \mid U \subseteq W \subseteq \{t\}, W \cap V = \emptyset, |W| = r\} \\
Y_V &= \{W \mid V \subseteq W \subseteq \{t\}, W \cup U = \emptyset, |W| = r\}.
\end{align*}
\]

\text{It is a simple matter to check that} \[ I_{U,V} \] \text{and} \[ I_{U-2s} \] \text{are isomorphic. Also, if} \[ G_j \] \text{covers any edge of} \[ I_{U,V} \], \text{then} \[ UV \] \text{is contained in} \[ G_j' \]. \text{Consequently, by Theorem 3, the assertion follows.} \]

In view of the proof of Theorem 3, similarly, one can extend any biclique of \[ I_i(r, w) \] to a biclique of \[ I_i(r - i, w - j) \]. \text{Consequently, we have the following corollary.}

\textbf{Corollary 2.} \textit{Let} \[ d, r, w, \text{and} t \] \textit{be positive integers, where} \[ t \geq r + w \]. \textit{For any} \[ 1 \leq i < r \] \textit{and} \[ 1 \leq j < w \], \textit{we have} \[ N((r, w; d), t) \geq N((r - i, w - j; m), t) \], \textit{where} \[ m = N((i, j; d), t - r - w + i + j) \].

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

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

\textbf{Theorem 4.} \textit{For any positive integers} \[ t \] \textit{and} \[ r \], \textit{where} \[ t > 2r \], \textit{we have} \[
bc_d(KG(t, r)) \geq bc_{3d}(KG(t - 2, r - 1)).
\]

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

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 $bc_d(KG(t,r))$?

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 $+1$s. Such a Hadamard matrix is called normalized. We will denote by $K^\sim_{m,m}$ the complete bipartite graph with a perfect matching removed. Obviously, $K^\sim_{m,m}$ is isomorphic to $I_m(1,1)$.

**Theorem 5.** 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

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

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 are $+1$ and $-1$ 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. Finally, consider the edge $u_iv_i$, then 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 $\frac{|E(G)|}{\beta(G)} \leq \frac{bc_d(G)}{d}$, therefore

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

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 $i, j$ have exactly $d$ columns that the corresponding entries are $+1$ and $-1$ 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.
Stinson et al. [5], using the probabilistic method, obtain an upper bound for SFPC. In the next theorem, we present a slight improvement of this upper bound.

**Theorem 6.** Let \( r \) and \( t \) be positive integers. If \( t \) is sufficiently large respect to \( r \) then there exists an \( r - SFPC(v, t) \) where

\[
v \leq \frac{\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)}{2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right)} \left(1 + \ln\left(\frac{\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)}{r}\right)\right)
\]

**Proof.** We show that if \( v \geq \frac{\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)}{2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right)} \left(1 + \ln\left(\frac{\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)}{r}\right)\right) \) then there exists a biclique cover of size \( v \) for the Kneser graph \( KG(t, r) \). Let \( A \) be \( \left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right) \). For every member of \( A \), 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 \( B \) to be the collection contains all 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 \( B \) with probability \( p \) and \( F \) be the random set of all bicliques picked and let \( Y_F \) be the set of all edges \( AB \) of the graph \( KG(t, r) \) which are not covered by the set \( F \). The expected value of \( |F| \) is clearly \( \left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right) \). For every edge \( AB \), \( pr(AB \in Y_F) = (1-p)^t \) where \( l = 2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right) \). So the expected value of the \( |F| + |Y_F| \) is at most

\[
\left(\frac{t}{\lfloor \frac{t}{2} \rfloor}\right)p + \frac{1}{2}\left(\frac{t}{r}\right)\left(\frac{t-r}{r}\right)(1-p)^{2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right)}.
\]

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

\[
E(|F| + |Y_F|) \leq \left(\frac{t}{\lfloor \frac{t}{2} \rfloor}\right)p + \frac{1}{2}\left(\frac{t}{r}\right)\left(\frac{t-r}{r}\right)e^{-2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right)}p.
\]

The right hand side is minimized at \( p = \frac{\ln(\alpha)}{\beta} \), which \( \alpha = \left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right) \) and \( \beta = 2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right) \) where \( p \in [0, 1] \) if \( t \) is sufficiently large respect to \( r \). So we have an \( r - SFPC(v, t) \) that

\[
v \leq \frac{\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)}{2\left(\frac{t-2r}{\lfloor \frac{t}{2} \rfloor - r}\right)} \left(1 + \ln\left(\frac{\left(\begin{array}{c}
t \\ \lfloor \frac{t}{2} \rfloor \end{array}\right)}{r}\right)\right).
\]

\[
\blacksquare
\]

**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] H. Hajiabolhassan and F. Moazami. Some new bounds for cover-free families through biclique cover. Manuscript 2011.

[5] 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.

[6] 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.

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

[8] 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.

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