Turkish Journal of Electrical Engineering and Computer Sciences

Volume 8 | Number 1 Article 4

1-1-2000

Information and Average Information Rates of a Graphical Access Structure on Six Vertices

MUSTAFA ATICI

Turk J Elec Engin, VOL.8, NO.1 2000, © TÜBİTAK

Information and Average Information Rates of a Graphical Access Structure on Six Vertices

Mustafa Atıcı
International Computer Institute,
Ege University,
35100 Bornova, Izmir-TURKEY
e-mail: atici@bornova.ege.edu.tr

Abstract

In this paper we study the optimal information and average information rates of secret sharing schemes which are all connected graphs on six vertices. There are 102 *connected graphs on six vertices that are not complete multipartite graphs. Of these* 102 *graphs, we determined the optimal information rate of* 71 *graphs, and the optimal average information rate of* 88 *graphs.*

1. Introduction

In a bank, there is a vault that must be opened every day. The bank employs three senior tellers, but they do not trust the combination to any individual teller. Hence, it is necessary to design a system whereby any two of the three senior tellers can gain access to the vault, but no individual teller can do so. This problem can be solved by means of a *secret sharing scheme*.

Here is an interesting real-world example of this case: According to *Time Magazine* (May 4, 1992, p.13), control of nuclear weapons in Russia involves a similar "two-out-of-three" access mechanism. The three parties involved are the President, the Defense Minister and the Defense Ministry.

The previous two examples show that two out of three participants should be able to determine the key. A more general situation is to specify exactly which subsets of participants should be able to determine the key and which should not. A secret sharing scheme is a method of dividing (sharing) a secret key K among a finite set $\mathcal{P}$ of participants in such a way that only certain specified subsets (qualified subsets) of participants can compute the secret key K by pooling their information.

As in the special cases given above, secret sharing schemes are useful in any situation that requires the concurrence of several choosen people to be initiated, such as launching a missile or entering an area of restricted access (e.g., a bank vault).

We will use the following notation. The *Dealer* is a special participant who chooses the secret key K; he is denoted by D. Let $\mathcal{P} = \{P_i : 1 \leq i \leq w\}$ be the set of participants. It is assumed that $D \notin \mathcal{P}$. Let $\mathcal{K}$ be the *key set* and let $\mathcal{S}$ be the *share set*. Let Γ be a set of subsets of $\mathcal{P}$. The subsets in Γ are those subsets of participants that should be able to compute the secret. Γ is called an *access structure* and the subsets in Γ are called *authorized subsets*.

When a dealer D wants to share a secret $K \in \mathcal{K}$, he or she will give each participant a share from $\mathcal{S}$. This distribution should be secret, so no participant knows the share given to another participant. At a later

time, a subset of participants B will try to recover K from the shares they have. We will say that a scheme is a *perfect secret sharing scheme realizing* the access structure Γ provided the following two properties are satisfied:

1. If an authorized subset of participants pool their shares, then they can recover the secret key K.

2. If an unauthorized subset of participants pool their shares, then they can compute nothing about the secret key K.

If Γ is an access structure, then $B \in \Gamma$ is a *minimal* authorized subset if $A \notin \Gamma$ whenever $A \subseteq B$, $A \neq B$. The set of minimal authorized subsets of Γ is denoted Γ_0 and is called the *basis* of Γ_0. We say that Γ is the *closure* of Γ_0 and write $\Gamma = cl(\Gamma_0)$.

Here is an example to illustrate perfect secret sharing.

Example

Let $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$. Let $\mathcal{S} = Z_n \times Z_n \times Z_n$, where $Z_n = \{1, 2, ..., n\}$, is the share set and take the access structure having basis

$$\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_4, P_5\}, \{P_5, P_6\}, \{P_6, P_1\}\}.$$

Thus, let us take $\mathcal{K} = Z_n \times Z_n$, $(K_1, K_2) \in \mathcal{K}$ and give the shares to the participants as follows:

$$\begin{aligned} P_1 &:= \{a_1, a_3, a_2 + K_1\}; \\ P_2 &:= \{a_2, a_5, a_1 + K_2\}; \\ P_3 &:= \{a_1, a_6, a_5 + K_1\}; \\ P_4 &:= \{a_5, a_4, a_6 + K_2\}; \\ P_5 &:= \{a_6, a_4 + K_1, a_3\}; \\ P_6 &:= \{a_2, a_4, a_3 + K_2\}; \end{aligned}$$

where $a_1, a_2, a_3, a_4, a_5, a_6 \in Z_n$ are random.

We will first verify that each basis subset can compute K. $\{P_1, P_2\}$ can compute $K = (K_1, K_2) = (a_2 + K_1 - a_2, a_1 + K_2 - a_1)$. Similarly, $\{P_2, P_3\}$ can compute $K = (K_1, K_2) = (a_5 + K_1 - a_5, a_1 + K_2 - a_1)$. $\{P_3, P_4\}$ can compute $K = (K_1, K_2) = (a_5 + K_1 - a_5, a_6 + K_2 - a_6)$. $\{P_4, P_5\}$ can compute $K = (K_1, K_2) = (a_4 + K_1 - a_4, a_6 + K_2 - a_6)$. $\{P_5, P_6\}$ can compute $K = (K_1, K_2) = (a_4 + K_1 - a_4, a_3 + K_2 - a_3)$. $\{P_6, P_1\}$ can compute $K = (K_1, K_2) = (a_2 + K_1 - a_2, a_3 + K_2 - a_3)$.

Can an unauthorized subset compute K? It suffices to consider the maximal unauthorized subsets, namely: $\{P_1, P_3, P_5\}, \{P_1, P_4\}, \{P_2, P_4, P_6\}, \{P_2, P_5\}$, and $\{P_3, P_6\}$. In each case, it is easy to see that K cannot be computed, because some necessary piece of random information is missing. For example, the subset $\{P_1, P_4\}$ possesses the shares $a_1, a_2 + K_1, a_3, a_6 + K_2, a_4, a_5$. Since the values of a_2 and a_6 are unknown random values, no information about K can be computed.

The next section, Section 2, gives a formal definition of a secret sharing scheme. Section 3 is about graph access structure. Section 4 gives some of the ways of computing information and average information rates. In Section 5, we compute optimal information and optimal average information rates of graph access structures on six vertices. In Section 6, we improve some of the lower bounds computed in Section 5.

2. Formal Definition of Secret Sharing

We now describe a general mathematical model for secret sharing and discuss the concept of security. In this model, we represent a secret sharing scheme by a set $\mathcal{F}$ of *distribution rules*. A distribution rule is a function

$$f\colon\ \mathcal{P}\ \cup\ \{D\}\ \longrightarrow\ \mathcal{K}\ \cup\ \mathcal{S}$$

which satisfies the conditions $f(D)\ \in\ \mathcal{K}$ and $f(P_i)\ \in\ \mathcal{S}$, for $1 \leq i \leq w$. A distribution rule f represents a possible distribution of shares to the participants, where $f(D)$ is the secret key being shared and $f\ (P_i)$ is the share given to P_i.

If $\mathcal{F}$ is a set of distribution rules and $K\ \in\ \mathcal{K}$, define

$$\mathcal{F}_K\ =\ \{\ f \in\ \mathcal{F}\ :\ f(D)\ =\mathrm{K}\ \}$$

$\mathcal{F}_K$ is the subset of distribution rules for key K. If $K\ \in\ \mathcal{K}$ is the value of the secret that D wants to share, then D will chose a random distribution rule $f \in\ \mathcal{F}_K$, and use f to distribute shares to the participants.

Let Γ be an access structure and let $\mathcal{F}$ be a set of distribution rules. Suppose the following two properties are satisfied:

1. Let $B\ \in\ \Gamma$, and suppose f and $g\ \in\ \mathcal{F}$. If $f(P_i) = g(P_i)$ for all $P_i\ \in\ B$, then $f(D) = g(D)$.
2. Let $B\ \notin\ \Gamma$ and suppose $f\colon\ B\ \longrightarrow\ \mathcal{S}$. Then there exists a non-negative integer $\mu(f\ ,\ B)$ such that, for every $K\ \in\ \mathcal{K}$

$$|\{g \in \mathcal{F}_K\ :\ g(P_i) = f(P_i)\ \text{for every}\ P_i \in B\}| = \mu(f, B).$$

Then $\mathcal{F}$ is a *perfect secret sharing scheme* that realizes the access structure Γ. Formal security proof can be found in [9]. We will use the notation $PS(\Gamma, q)$ to denote a perfect secret sharing scheme with access structure $cl(\Gamma)$ for a set of q keys.

In general, we measure the efficiency of a secret sharing scheme by the information rate. Suppose $\mathcal{F}$ is a set of distribution rules for a secret sharing scheme. For $1 \leq i \leq w$ define $\mathcal{S}_i = \{f(P_i) : f \in \mathcal{F}\}$. $\mathcal{S}_i$ represents the set of possible shares that P_i might receive. The *information rate for* P_i is the ratio

$$\rho_i(\mathcal{F}) = \frac{\log_2|\mathcal{K}|}{\log_2|\mathcal{S}_i|}.$$

The *information rate*, denoted by $\rho(\mathcal{F})$, is defined as $\rho(\mathcal{F}) = \min\ \{\rho_i(\mathcal{F}) : 1 \leq i \leq w\}$. The *average information rate*, denoted by $\widetilde{\rho}(\mathcal{F})$, is the harmonic mean of the $\rho_i\,(\mathcal{F})$'s:

$$\widetilde{\rho}(\mathcal{F}) = \frac{w\log_2|\mathcal{K}|}{\sum_{i=1}^{w}\log_2|\mathcal{S}_i|}.$$

For a given (fixed) scheme $\mathcal{F}$ we will write $\rho_i\ (1 \leq i \leq w)$, ρ, and $\widetilde{\rho}$.

It is not too difficult to prove that $\rho \leq \widetilde{\rho} \leq 1$ in any scheme, and that $\rho = 1$ if and only if $\widetilde{\rho} = 1$. Since $\rho = \widetilde{\rho} = 1$ is the optimal situation, we refer to such a scheme as an *ideal* scheme. Ideal schemes have been studied extensively [3, 4, 7, 8]. In the cases where ideal schemes do not exist, the objective is to construct a scheme with an (average) information rate as close to one as possible.

3. Graph Access Structures

The situation that has been studied the most is when the basis consists of the edges of a graph. We now briefly mention some results we will need later. Ideal schemes for connected graphs were characterized by Brickell and Davenport [4], as follows.

Theorem 3.1 *Suppose G is a connected graph. Then there exists a $PS(G,q)$ with $\rho = \widetilde{\rho} = 1$ (for some q) if and only if G is a complete multipartite graph.*

The following result from [5] specifies some value of q for which an ideal scheme can be constructed.

Corollary 3.1 *Suppose $q \geq t$ is a prime power. Then there is a $PS(K_{n_1,n_2,\ldots,n_t}, q)$ with $\rho = \widetilde{\rho} = 1$.*

4. Information and Average Information Rate

4.1. A Decomposition Construction

The main recursive construction uses small schemes as building blocks in the construction of larger schemes. We call this *decomposition construction*. Various versions of this construction have been described in several papers [2, 5, 6, 7, 10, 11]. Also, a new, more general version of this technique has been described [12].

Suppose Γ is an access structure having basis Γ_0. Let $\lambda \geq 1$ be an integer. A λ-*decomposition* of Γ_0 consists of a collection $\{\Gamma_1, \ldots, \Gamma_n\}$ such that the following properties are satisfied:

1. $\Gamma_k \subseteq \Gamma_0$ for $1 \leq k \leq n$.
2. $\lambda\Gamma_0 \subseteq \cup_{k=1}^{n}\Gamma_k$ (i.e., the multiset union of the Γ_k's contains every subset at least λ times)

For $1 \leq k \leq n$, define $\mathcal{P}_k = \cup_{B\in\Gamma_k} B$; $\mathcal{P}_k$ denotes the set of participants in a scheme with access structure $cl(\Gamma_k)$. We have the following construction proven in [12].

Theorem 4.1 *Let Γ be an access structure of w participants, having basis Γ_0, and suppose that $\{\Gamma_1, \ldots, \Gamma_n\}$ is a λ - decomposition of Γ_0. Let q be a prime power. Suppose that $L_k \in (GF(q))^{\lambda}$, $1 \leq k \leq n$, and for every $B \in \Gamma_0$, we have*

$$\langle L_k : B \in \Gamma_k \rangle = (GF(q))^{\lambda}. \tag{1}$$

For $1 \leq k \leq n$, suppose $\mathcal{F}^k$ is the set of the distribution rules of a $PS(\Gamma_k, q)$ with information rates $\rho_{ik} = \rho_i(\mathcal{F}^k)$, $P_i \in \mathcal{P}_k$.

Then there exists a $PS(\Gamma_0, q^{\lambda})$ with information rate ρ and average information rate $\widetilde{\rho}$, where

$$\rho = min\ \{\frac{\lambda}{\sum_{\{k:P_i\in\mathcal{P}_k\}}\frac{1}{\rho_{ik}}} : 1 \leq i \leq w\ \}\ and\ \widetilde{\rho} = \frac{w\lambda}{\sum_{k=1}^{n}\frac{|\mathcal{P}_k|}{\widetilde{\rho}_k(\mathcal{F}^k)}}.$$

4.2. A Linear Programming Approach

In this section, we describe a linear programming approach from [12] that is useful in applying the decomposition construction. Suppose Γ is an access structure with basis Γ_0. The first step is to produce a list of various schemes $PS(\Gamma_k, q)$, for some fixed prime power q, where $\Gamma_k \subseteq \Gamma_0$, $1 \leq k \leq m$. Since Γ is a graph access structure, in this paper we usually take the Γ_k's to be all the complete multipartite subgraphs of Γ.

For $1 \leq k \leq m$, suppose $\mathcal{F}^k$ is the set of the distribution rules of a $PS(\Gamma_k, q)$ with information rates $\rho_{ik} = \rho_i(\mathcal{F}^k)$, $P_i \in \mathcal{P}_k$. Let $\Gamma_0 = \{ B_1, \ldots, B_v \}$. For $1 \leq i \leq w$, $1 \leq k \leq m$, and $1 \leq j \leq v$ define

$$a_{ik} = \begin{cases} \frac{1}{\rho_{ik}} & \text{if } P_i \in \mathcal{P}_k \\ 0 & \text{otherwise} \end{cases} \qquad b_{jk} = \begin{cases} 1 & \text{if } B_j \in \Gamma_k \\ 0 & \text{otherwise.} \end{cases}$$

Now suppose we construct a decomposition using α_k copies of Γ_k for $1 \leq k \leq m$ where each $\alpha_k \geq 0$ is an integer. Then we have $\lambda = \min \{\sum_{k=1}^{m} \alpha_k b_{jk} : 1 \leq j \leq v \}$ and hence we produce a scheme $\mathcal{F}$ with

$$\rho(\mathcal{F}) = \min \{ \frac{\lambda}{\sum_{k=1}^{m} \alpha_k a_{ik}} : 1 \leq i \leq w \}.$$

We want to find the optimal linear combination of the Γ_k's. We rephrase this as a linear programming problem as follows. Note that taking a scalar multiple of all the α_k's does not affect the value of the resulting information rate $\rho(\mathcal{F})$. Hence, we can allow the α_k's to be non-negative rational numbers and "normalize" them by stipulating that $\max \{\sum_{k=1}^{m} \alpha_k a_{ik} : 1 \leq i \leq w\} = 1$. Then our objective is to maximize λ. Hence, the linear programming problem we consider is the following:

Maximize λ	subject to	
	$\alpha_k \geq 0$	$1 \leq k \leq m$
	$\sum_{k=1}^{m} \alpha_k a_{ik} \leq 1$	$1 \leq i \leq w$
	$\sum_{k=1}^{m} \alpha_k b_{jk} \geq \lambda$	$1 \leq j \leq v$

Now, if we solve this linear programming problem, the optimal solution will involve rational values α_k, $1 \leq k \leq m$. We can multiply by an appropriate factor so as to make all the α_k's integral. Then take the resulting linear combination of the bases Γ_k, $1 \leq k \leq m$, as the decomposition. The following theorem which is proven in [2] gives us the general upper bound.

Theorem 4.2 *Suppose G is a connected graph that is not a complete multipartite graph. Then $\rho(G) \leq 2/3$.*

For average information rate, we proceed slightly differently. Denote $\widetilde{\rho_k} = \widetilde{\rho}(\mathcal{F}^k)$, $1 \leq k \leq m$. $\widetilde{\rho}(\mathcal{F})$ is computed by the formula

$$\widetilde{\rho}(\mathcal{F}) = \frac{w\lambda}{\sum_{k=1}^{m} \frac{\alpha_k |\mathcal{P}_k|}{\widetilde{\rho_k}}}$$

where λ is the same as before. If we normalize the α_k's so that $\sum_{k=1}^{m} \frac{\alpha_k |\mathcal{P}_k|}{\widetilde{\rho_k}} = 1$ then $\widetilde{\rho} = \lambda w$, and we will maximize λ, as before. Here is the linear program to compute a lower bound for $\widetilde{\rho}$

Maximize λw	subject to	
	$\alpha_k \geq 0$	$1 \leq k \leq m$
	$\sum_{k=1}^{m} \frac{\alpha_k \lvert\mathcal{P}_k\rvert}{\widetilde{\rho_k}} \leq 1$	
	$\sum_{k=1}^{m} \alpha_k b_{jk} \geq \lambda$	$1 \leq j \leq v$

The upper bound of the average information rate has been studied [2]. Let G be a graph, and define a subgraph G_1 of G as follows: $bc \in E(G_1)$ if and only if there exist vertices $a, b, c, d \in V(G)$ such that $G[V'] = \{ ab, bc, cd \}$ or $\{ ab, bc, cd, bd \}$ where $V' = \{ a, b, c, d \}$. We will take $V(G_1)$ to consist of

all vertices in $V(G)$ that are incident with at least one edge in $E(G_1)$. We say that G_1 is the *foundation* of G.

Let G be a connected graph and let G_1 be the foundation of G. Consider the following linear programming problem $\mathcal{A}(G)$:

Minimize	$C = \sum_{v \in V(G)} a_v$	subject to
	$a_v \geq 0$	$v \in V(G)$
	$a_v + a_w \geq 1$	$vw \in E(G_1)$

Then we have following upper bound, which is proved in [2], on the average information rate.

Theorem 4.3 *Let G be a graph with foundation G_1. Let $\widetilde{C}$ be the optimal solution to the problem $\mathcal{A}(G)$. Then $\widetilde{\rho}(G) \leq \frac{|V(G)|}{\widetilde{C}+|V(G)|}$.*

The following lemma, which is proven in [2], gives us the general upper bound for the average information rate.

Lemma 4.1 *Let G be a connected graph with n vertices. If G is complete multipartite graph then $\widetilde{\rho}(G) = 1$; otherwise $\widetilde{\rho}(G) \leq n/(n+1)$.*

5. The Connected Graphs on Six Vertices

In this section, we will give upper and lower bounds on the information rate and average information rate for the connected graph on six vertices. There are 112 non-isomorphic connected graphs on six vertices. Of these 112 graphs, ten are complete multipartite graphs and permit ideal schemes. These graphs are $K_{5,1}$, $K_{4,2}$, $K_{4,1,1}$, $K_{3,3}$, $K_{3,2,1}$, $K_{3,1,1,1}$, $K_{2,2,2}$, $K_{2,2,1,1}$, $K_{2,1,1,1,1}$, and K_6. The remaining 102 graphs are shown in *Appendix A* of [1]. The decompositions used to obtain bounds on the optimal information and optimal average information rates are given in *Appendix B* of [1].

5.1. Lower Bound of Information Rate

In order to find lower bounds on the information rate of connected graph $G = (V, E)$ on six vertices, we first determine all the possible complete multipartite subgraphs of G. The algorithm to do this is as follows.

All Multipartite Subgraphs (V,E)
Input: $V(G)$ and $E(G)$.
Equivalence Relation (V,E)
Output is "Yes" if the given graph is an equivalence relation on the vertex set V. Otherwise output "No".
- **For** every $a \in V$
  - $(a, a) \in E$
  - **If** $(a, b) \in E$, then $(b, a) \in E$
  - **If** (a, b) and $(b, c) \in E$, then $(a, c) \in E$

For every subset $E_1 \subseteq E$ **do**
(a) let V_1 = vertices incident with E_1
(b) construct the graph $(V_1,(E_1)^c)$
(c) **Equivalence Relation** $(V_1,(E_1)^c)$
If "Yes" then (V_1,E_1) is a complete multipartite subgraph of G

Once we find all the complete multipartite subgraphs of given graph G, then we can construct the matrices $A = (a_{ik})$ and $B = (b_{jk})$ for the linear programming problem given in Section 4. Since all the subgraphs are complete multipartite, they permit ideal schemes (i.e., for $1 \leq i \leq w,\ 1 \leq k \leq m,\ \rho_{i,k} = 1$). Hence, from Section 4, we produce the following matrices: for $1 \leq i \leq w,\ 1 \leq k \leq m$, and $1 \leq j \leq v$

$$a_{ik} = \begin{cases} 1 & \text{if } P_i \in \mathcal{P}_k \\ 0 & \text{otherwise} \end{cases} \qquad b_{jk} = \begin{cases} 1 & \text{if } B_j \in \Gamma_k \\ 0 & \text{otherwise.} \end{cases}$$

5.2. Upper Bound of Information Rate

By using Theorem 4.2 we determined upper bounds on the information rate of connected, complete non-multipartite graphs on six vertices. More information can be found in [1].

5.3. Lower Bound of Average Information Rate

Recall that we use the notation $\mathcal{P}_k = \cup_{B \in \Gamma_k} B$ to denote the set of participants in a scheme with access structure $cl\ (\Gamma_k)$. Finding the edge sets of the complete multipartite subgraphs of given graph G is the same as determining the Γ_k's, $1 \leq k \leq m$. Since all the multipartite subgraphs permit ideal schemes, then the average information rates $\widetilde{\rho}_k = 1$ for $1 \leq k \leq m$. We use the linear programming given in Section 4 to find lower bounds on the average information rate, and the corresponding decompositions.

5.4. Upper Bound of Average Information Rate

We determined upper bounds on average information rate using Theorem 4.3. To do this, we first constructed the *foundation* graph of existing graph $G = (V, E)$. The algorithm we used to compute the foundation is the following:

Foundation of Graph (V, G)

(a) **Set** $E_1 = \emptyset$ (* Edge set of *foundation**)
(b) **For** every 4-subset V_0 of V **do**
  If $G[V_0] \simeq P_3$ **Then**
    add one edge $\{b, c\}$ to E_1
  Else if $G[V_0] \simeq H$ **Then**
    add two edges $\{b, c\}, \{b, d\}$ to E_1

H is a graph where $V_H =$ { a,b,c,d} and
$E_H = \{(a, b), (b, c), (c, d), (b, d)\}$.

Once we have found the foundation of a graph, then we solve the linear programming problem given in Section 4 to find $\widetilde{C}$, and use Theorem 4.3 to find the upper bounds on the average information rate. The lower and upper bounds on information and average information rate are summarized in the Appendix (also see [1]).

6. Improvements on the Lower Bounds of Information and Average Information Rate

In Section 5, we found upper and lower bounds on the information rate and average information rate for connected graphs on six vertices. In this section, we will try to improve the lower bounds we have previously obtained. First, it has been shown (and the scheme is also given) in [11] that the following graph achieves optimal information rates $\rho = 2/3$ and $\widetilde{\rho} = 10/13$.

From now on, we will name this graph U. The optimal information rates of vertices of U are $\rho(1) = \rho(2) = 1$ and $\rho(3) = \rho(4) = \rho(5) = 2/3$. This is the only graph on five vertices where the optimal rates are not obtained by the decomposition construction.

6.1. Improvements by Splitting the Graph U

Let G be a graph and $v \in V(G)$. We define a graph $G(v)$ by replacing v by two nonadjacent vertices v_1 and v_2, such that $v_i w$ is an edge of $G(v)$ if and only if vw is an edge of G ($i = 1,2$). We say that $G(v)$ is constructed from G by *splitting* v. We will obtain some of the optimal information rates using the following theorem from [5].

Theorem 6.1 *Suppose G is a graph and there exists a $PS(G, q)$ with information rate ρ. Then, for any vertex v of G, there exists a $PS(G(v), q)$ with the same information rate.*

Now, for any given connected graph G on six vertices we can determine if G is constructed by *splitting* as follows: First, compute $\mathrm{N}(v)$ for every $v \in V(G)$ and check if $\mathrm{N}(v) = \mathrm{N}(w)$ for any $w \in V(G)$, where v and w are not adjacent. If there are two such vertices v and w then we delete one of these vertices and all the edges incident with the deleted vertex. The remaining graph is a connected graph on five vertices and we know that it does permit an optimal scheme.

6.2. Decomposition Using the Graph U

In Section 5, to find decompositions we only use multipartite subgraphs of a given graph. We now know that U has optimal information rates; therefore we can use this graph in the decomposition construction to find lower bounds on the information and average information rates of other graphs. We give the following procedure that finds all the subgraphs isomorphic to U for given graph G.

$T = \emptyset$ /* Set of subgraphs isomorphic to U */
Find all the cycles C_3 of length 3
For each cycle C_3 where $V(C_3) = \{u, v, w\}$
  Compute
  $S_u = N(u) - \{v, w\}$, $S_v = N(v) - \{u, w\}$, $S_w = N(w) - \{v, u\}$
  a) **For** each $x \in S_u$
    add $C_3 \cup (u, x) \cup (v, y)$ to T for all $y \in S_v$ and $y \neq x$
  b) **For** each $x \in S_u$
    add $C_3 \cup (u, x) \cup (v, y)$ to T for all $y \in S_w$ and $y \neq x$
  c) **For** each $x \in S_v$
    add $C_3 \cup (u, x) \cup (v, y)$ to T for all $y \in S_w$ and $y \neq x$

Once we find all the complete multipartite subgraphs and all subgraphs that are isomorphic to U for a given graph G, then we can construct the matrices $A = (a_{ik})$ and $B = (b_{jk})$ for the linear programming given in Section 4. Therefore, we have following matrices: For $1 \leq i \leq w$, $1 \leq k \leq m$, and $1 \leq j \leq v$ define

$$a_{ik} = \begin{cases} 1 & \text{if } P_i \in \Gamma_k \text{ and } \Gamma_k \text{ is a complete multipartite subgraph} \\ 1 & \text{if } P_i \in \Gamma_k,\ \Gamma_k \simeq U, \text{ and } i \text{ is vertex 1 or 2} \\ 3/2 & \text{if } P_i \in \Gamma_k,\ \Gamma_k \simeq U, \text{ and } i \text{ is vertex 3, 4 or 5} \\ 0 & \text{otherwise} \end{cases}$$

$$b_{jk} = \begin{cases} 1 & \text{if } B_j \in \Gamma_k \\ 0 & \text{otherwise} \end{cases} .$$

We obtained only one improvement on the lower bounds of average information rates. That is for graph number 16 in [1]. The previous lower bound of 2/3, was improved to 12/17. We improved the lower bounds on the information rate in five cases. These are shown in Table A in [1].

References

[1] M. Atici and D.R. Stinson, Optimal information and average information rates of the connected graphs on six vertices, Report series: UNL-CSE - 94 - 013.

[2] C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, Graph Decompositions and Secret Sharing Schemes, *Journal of Cryptology*, **8** (1995), 39 - 64. Preliminary version appeared in *Lecture Notes in Computer Science*, **658**, (1993), pp. 1 - 24.

[3] E.F. Brickell, Some ideal secret sharing schemes, *J. Combin. Math. and Combin. Comput.*, **9**, (1989), pp.105 - 113.

[4] E.F. Brickell and D.M. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology*, **4**, (1991), pp. 123 - 134.

[5] E.F. Brickell and D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. Cryptology*, **5**, (1992), pp. 153 - 166. Preliminary version appeared in *Lecture Notes in Computer Science*, **537**, (1991), pp. 242 - 252.

[6] K.M. Martin, New secret sharing schemes from old, *J. Comb. Math. Comb. Comp.*, **14**, (1993), pp. 65 - 77.

[7] K.M. Martin, PhD thesis, Discrete Structures in the Theory of Secret Sharing, University of London, 1991.

[8] P.D. Seymour, On secret-sharing matroids, *Journal of Combin. Theory B*, **56**, (1992), pp. 69 - 73.

[9] G.J. Simmons, W. Jackson and K. Martin, The geometry of shared secret schemes, *Bulletin of the ICA*, **1**, (1991), pp. 71 - 88.

[10] D.R. Stinson, An explication of secret sharing schemes, *Designs, Codes and Cryptography*, **2**, (1992), pp. 357 - 390.

[11] D.R. Stinson, New general lower bounds on the information rate of secret sharing schemes, *Lecture Notes in Computer Science*, **740**, (1993), pp. 170 - 184.

[12] D.R. Stinson, Decomposition Construction for Secret Sharing Schemes, *IEEE Transactions on Information Theory*, **40**, (1994), pp. 118 - 125.

Appendix

Graph	*Optimal Information Rate*	*Optimal Average Info. Rate*
1	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
2	$\rho = 3/5$	$\widetilde{\rho} = 3/4$
3	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
4	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
5	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
6	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
7	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
8	$\rho = 3/5$	$2/3 \leq \widetilde{\rho} \leq 3/4$
9	$\rho = 3/5$	$\widetilde{\rho} = 3/4$
10	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
11	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
12	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
13	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
14	$\rho = 3/5$	$3/4 \leq \widetilde{\rho} \leq 6/7$
15	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
16	$6/11 \leq \rho \leq 2/3$ $(**)$	$12/17 \leq \widetilde{\rho} \leq 4/5$ $(**)$
17	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
18	$\rho = 2/3$ $(*)$	$\widetilde{\rho} = 4/5$ $(*)$
19	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
20	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
21	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
22	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 2/3$
23	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
24	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
25	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
26	$4/7 \leq \rho \leq 2/3$ $(**)$	$\widetilde{\rho} = 3/4$
27	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
28	$3/5 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 12/17$
29	$4/7 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
30	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
31	$\rho = 3/5$	$\widetilde{\rho} = 3/4$
32	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
33	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
34	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
35	$3/5 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 3/4$
36	$\rho = 2/3$ $(*)$	$\widetilde{\rho} = 3/4$
37	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
38	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
39	$8/13 \leq \rho \leq 2/3$ $(**)$	$24/37 \leq \widetilde{\rho} \leq 2/3$
40	$4/7 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 3/4$
41	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 2/3$
42	$4/7 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 3/4$
43	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 2/3$
44	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
45	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
46	$\rho = 2/3$	$\widetilde{\rho} = 6/7$

Graph	*Optimal Information Rate*	*Optimal Average Info. Rate*
47	$3/5 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 3/4$
48	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
49	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
50	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
51	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
52	$3/5 \leq \rho \leq 2/3$	$9/14 \leq \widetilde{\rho} \leq 2/3$
53	$\rho = 2/3$ $(*)$	$\widetilde{\rho} = 3/4$
54	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
55	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
56	$9/16 \leq \rho \leq 2/3$ $(**)$	$\widetilde{\rho} = 3/4$
57	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
58	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
59	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
60	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 2/3$
61	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
62	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
63	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
64	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
65	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
66	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
67	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 2/3$
68	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
69	$4/7 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 3/4$
70	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
71	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
72	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
73	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
74	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
75	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
76	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 2/3$
77	$3/5 \leq \rho \leq 2/3$	$2/3 \leq \widetilde{\rho} \leq 12/17$
78	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
79	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
80	$5/8 \leq \rho \leq 2/3$	$36/55 \leq \widetilde{\rho} \leq 2/3$
81	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
82	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
83	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
84	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
85	$5/8 \leq \rho \leq 2/3$	$24/37 \leq \widetilde{\rho} \leq 2/3$
86	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
87	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
88	$3/5 \leq \rho \leq 2/3$	$\widetilde{\rho} = 3/4$
89	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
90	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
91	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
92	$\rho = 2/3$	$\widetilde{\rho} = 6/7$
93	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
94	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
95	$\rho = 2/3$	$\widetilde{\rho} = 3/4$

Graph	*Optimal Information Rate*	*Optimal Average Info. Rate*
96	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
97	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
98	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
99	$\rho = 2/3$	$\widetilde{\rho} = 2/3$
100	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
101	$\rho = 2/3$	$\widetilde{\rho} = 3/4$
102	$\rho = 2/3$	$\widetilde{\rho} = 3/4$

(*) : Bound obtained from splitting.

(**): Bound obtained from decomposition construction using graph U.