A Study on the Average Information Ratio of Perfect Secret-Sharing Schemes for Access Structures Based on Bipartite Graphs

Hui-Chuan Lu

Abstract—A perfect secret-sharing scheme is a method to distribute a secret among a set of participants in such a way that only qualified subsets of participants can recover the secret and the joint share of participants in any unqualified subset is statistically independent of the secret. The collection of all qualified subsets is called the access structure of the perfect secret-sharing scheme. In a graph-based access structure, each vertex of a graph *G* represents a participant and each edge of *G* represents a minimal qualified subset. The average information ratio of a perfect secret-sharing scheme Σ realizing the access structure based on *G* is defined as $AR_\Sigma = (\sum_{v\in V(G)} H(\zeta_v))/(|V(G)|H(\zeta_s))$, where ζ_s is the secret and ζ_v is the share of v, both are random variables from Σ and *H* is the Shannon entropy. The infimum of the average information ratio of all possible perfect secret-sharing schemes realizing a given access structure is called the optimal average information ratio of that access structure. Most known results about the optimal average information ratio give upper bounds or lower bounds on it. In this present paper, we study the access structures based on bipartite graphs and determine the exact values of the optimal average information ratio of some infinite classes of them.

Keywords—secret-sharing scheme, average information ratio, star covering, core sequence.

I. Introduction

A *secret-sharing scheme* is a method to distribute a secret among a set of participants such that only participants in a qualified subset can recover the secret. If, in addition, the joint share of the participants in any unqualified subset is statistically independent of the secret, then this secret-sharing scheme is called *perfect*. We will use "secret-sharing scheme" for "perfect secret-sharing scheme" since all secret-sharing schemes considered in this paper are perfect. The collection of all qualified subsets in a secret-sharing scheme is the *access structure* of this scheme. An access structure is required to be *monotone* which means any subset of participants containing a qualified subset must also be qualified. Therefore, an access structure Γ is determined by the family of all minimal qualified subsets, the *basis* of Γ.

Shamir [21] and Blakley [2] independently introduced the first kind of secret-sharing schemes called the (t, n)-threshold scheme in 1979. In such a scheme, the basis of the access structure consists of all t-subsets of the set of participants of size n. Problems related to secret-sharing schemes have then received considerable attention. Extensive study has been focused on the discussion of the *information ratio* and the *average information ratio*. The information ratio of a secret-sharing scheme is the ratio of the maximum length (in bits) of the share given to a participant to the length of the secret, while the average information ratio is the ratio of the average length of the shares given to the participants to the length of the secret. These ratios represent the maximum and average number of bits the participants have to remember for each bit of the secret respectively. Note that some literature uses information rate (resp. average information rate) which is exactly the reciprocal of the information ratio (resp. the average information ratio). For higher efficiency of a secret-sharing scheme, the information ratio and average information ratio are expected to be as low as possible. Given an access structure, the infimum of the (average) information ratio of all possible secret-sharing schemes realizing this access structure is called the *optimal (average) information ratio* of the access structure. It has been shown that, for general access structures, the infimum is not always a minimum [1].

In this paper, we consider graph-based access structures. In such an access structure, each vertex of a graph G represents a participant and each edge $uv \in E(G)$ of G represents a minimal qualified subset. A secret-sharing scheme Σ for the access structure based on G is a collection of random variables ζ_s and ζ_v for $v \in V(G)$ with a joint distribution such that

(i) ζ_s is the secret and ζ_v is the share of v;
(ii) if $uv \in E(G)$, then ζ_u and ζ_v together determine the value of ζ_s; and
(iii) if $A \subseteq V(G)$ is an independent set in G, then ζ_s and the collection $\{\zeta_v | v \in A\}$ are statistically independent.

Recall that the Shannon entropy of a discrete random variable X with possible values $\{x_1, \ldots, x_n\}$ and a probability distribution $\{p(x_i)\}_{i=1}^n$ is defined as $H(X) = -\sum_{i=1}^n p(x_i) \log p(x_i)$. This value reflects the average number of bits needed to represent the element in X faithfully, cf [14]. The information ratio of Σ can be defined using Shannon entropy as $R_\Sigma = \max_{v\in V(G)}\{H(\zeta_v)/H(\zeta_s)\}$ and the average information ratio as $AR_\Sigma = (\sum_{v\in V(G)} H(\zeta_v))/(|V(G)|H(\zeta_s))$. For convenience, in what follows, with the same symbol G, we will denote both the graph and the access structure based on it. Consequently, "a secret-sharing scheme for the access structure based on G" is described as "a secret-sharing scheme on G" and "the optimal (average) information ratio of the access structure based on G" is written as "the optimal (average) information ratio of G". As mentioned above, the

Hui-Chuan Lu is with the Center for Basic Required Courses, National United University, Miaoli, Taiwan 36003. She is also with the Department of Applied Mathematics, National Chaio Tung University, Hsinchu, Taiwan 30010 e-mail: hjlu@nuu.edu.tw

optimal information ratio $R(G)$ (resp. the optimal average information ratio $AR(G)$) of G is the infimum of R_Σ (resp. AR_Σ) over all secret-sharing schemes Σ realizing G. It is well-known that $R(G) \geq AR(G) \geq 1$ and $R(G) = 1$ if and only if $AR(G) = 1$. A secret-sharing scheme with (average) information ratio equal to one is then called an *ideal* secret-sharing scheme. An access structure is *deal* if there exists an ideal secret-sharing scheme on it.

Determining the exact values of $R(G)$ and $AR(G)$ is extremely hard, it can be quite challenging even for small graphs. So, most of the known results give bounds on them, see for example, [3–8], [10], [11], [15], [16], [18], [19], [20], [22–24]. Stinson [24] showed that $R(G) \leq (d+1)/2$ where d is the maximum degree of G and $AR(G) \leq (2m+n)/2n$ where $n = |V(G)|$ and $m = |E(G)|$. This upper bound on $R(G)$ has been shown to be tight [3]. As to the exact values of these ratios, the problems have been settled for graphs with no more than five vertices [6], [16]. Exact values of the optimal information ratio for most of the six-vertex graphs have also been solved [15]. To the best of our knowledge, paths, cycles and trees are the only infinite classes of graphs whose optimal information ratio and optimal average information ratio are known [6], [7], [17]. In the present paper, we determine the exact values of the optimal average information ratio for some infinite classes of bipartite graphs. In Section II, some definitions, notations and known results to be used later will be introduced. In Section III, we give an extension of the idea used in [17] for trees first and subsequently present our main results. A concluding remark will be given in the final section.

II. Preliminaries

If there is no specification, any graph considered in the paper is a connected simple graph without loops. The ideal graph-based access structures have been completely characterized by Brickell and Davenport [7] in 1991.

Theorem 2.1 ([7]). *Suppose that G is a connected graph. Then $R(G) = AR(G) = 1$ if and only if G is a complete multipartite graph.*

To establish upper bounds on the optimal average information ratio for a graph that is not complete multipartite, the most commonly used method is to actually construct a secret-sharing scheme Σ on it. The average information ratio AR_Σ of the scheme Σ naturally makes an upper bound on $AR(G)$. Stinson's decomposition construction [24] enables us to build up secret-sharing schemes of larger graphs through *complete multipartite coverings*. A complete multipartite covering is a collection of complete multipartite subgraphs $\Pi = \{G_1, G_2, \ldots, G_l\}$ of G such that each edge of G appears in at least one subgraph in this collection. The sum $m_\Pi = \sum_{i=1}^{l} |V(G_i)|$ is called the *vertex-number sum* of Π.

Theorem 2.2 ([24]). *Suppose that $\Pi = \{G_1, G_2, \ldots, G_l\}$ is a complete multipartite covering of a graph G with $V(G) = \{1, 2, \ldots, n\}$. Let $k_i = |\{j | i \in V(G_j)\}|$, then there exists a secret-sharing scheme Σ on G with information ratio R_Σ and average information ratio AR_Σ where $R_\Sigma = \max_{1 \leq i \leq n} k_i$ and $AR_\Sigma = \frac{1}{n}\sum_{i=1}^{n} k_i = \frac{1}{n}\sum_{i=1}^{l} |V(G_i)|$.*

Since we are dealing with bipartite graphs with girth not less than six, the only possible complete multipartite subgraphs are the stars. For the construction of a secret-sharing scheme with higher efficiency, a star covering with the least vertex-number sum is what we are aiming for. We follow the notation used in [17] for trees and extend the idea to general graphs. Let $IN(G) = \{v \in V(G) | \deg_G(v) \geq 2\}$ and $in(G) = |IN(G)|$. Given a star covering Π of G with vertex-number sum m_Π, we define the *deduction* of Π as $d_\Pi = |V(G)| + in(G) - m_\Pi$. A star covering with the least vertex-number sum gives the largest deduction. We then let the largest deduction over all star coverings of G be the deduction of G, denoted as $d^*(G)$. We restate Stinson's result in the language of deduction for later use.

Theorem 2.3 ([24]). *Let Π be a star covering of a graph G with deduction d_Π, then $AR(G) \leq \frac{|V(G)| + in(G) - d_\Pi}{|V(G)|}$.*

For the derivation of lower bounds on $AR(G)$, we use information theoretic approach [3–5], [9–13], [15]. Let Σ be a secret-sharing scheme on G in which ζ_s and ζ_v, $v \in V(G)$, are the secret and the share of v respectively. Define a real-valued function f on the set of all subsets of $V(G)$ as $f(A) = H(\{\zeta_v | v \in A\})/H(\zeta_s)$ where H is the Shannon entropy. If $f(\{v\})$ is written as $f(v)$ for simplicity, then $AR_\Sigma = \frac{1}{n}\sum_{v \in V(G)} f(v)$, where $n = |V(G)|$. It was shown in [9] that f satisfies the following inequalities:

(a) $f(\emptyset) = 0$ and $f(A) \geq 0$;
(b) if $A \subseteq B \subseteq V(G)$, then $f(A) \leq f(B)$;
(c) $f(A) + f(B) \geq f(A \cap B) + f(A \cup B)$;
(d) if $A \subseteq B \subseteq V(G)$, A is an independent set and B is not, then $f(A) + 1 \leq f(B)$; and
(e) if neither A nor B is independent but $A \cap B$ is, then $f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$.

Csirmaz and Ligeti defined a *core* of a graph G in [12] as a subset V_0 of $V(G)$ satisfying that (i) V_0 induces a connected subgraph of G; (ii) each vertex $v \in V_0$ has a neighbor $\bar{v}$ outside V_0 and not adjacent to any other vertex in V_0; and (iii) $\{\bar{v} | v \in V_0\}$ is an independent set in G. They also showed the following result.

Theorem 2.4 ([13]). *Let V_0 be a core of a graph G and f is defined as above, then $\sum_{v \in V_0} f(v) \geq 2|V_0| - 1$.*

In the next section, we shall make use of the stated results to derive a lower bound on $AR(G)$ and determine the exact values of the optimal average information ratio for some infinite classes of bipartite graphs.

III. The main results

A. An extension

Lu and Fu [17] defined a core sequence of a tree T. We now define similarly a *core sequence of length k* of a graph G as a collection $\mathcal{C} = \{V_1, V_2, \ldots, V_k\}$ of nonempty subsets of $IN(G)$ such that $V_1, V_2, \ldots, V_k$ form a partition of $IN(G)$ and each V_i is a core of G. The length of $\mathcal{C}$ is written as $c_\mathcal{C}$. The *core number* of G, $c^*(G)$, is the minimum length of all core sequences of G. Now, we have a useful lower bound on $AR(G)$ in terms of the length of a core sequence.

Theorem 3.1. *Let G be a connected graph. If $\mathcal{C}$ is a core sequence of G, then $AR(G) \geq \frac{|V(G)|+in(G)-c_{\mathcal{C}}}{|V(G)|}$.*

Proof: Let $\mathcal{C} = \{V_1, V_2, \ldots, V_k\}$ and Σ be a secret-sharing scheme on G. Then the function f defined in Section II by the random variables from Σ satisfies inequalities (a) to (e) and Theorem 2.4. Since G is connected, $f(v) \geq 1$ for all $v \in V(G)$ [9]. We have $\sum_{v\in V(G)} f(v) = \sum_{v\in IN(G)} f(v) + \sum_{v:\deg_G(v)=1} f(v) \geq \sum_{i=1}^{k}\sum_{v\in V_i} f(v) + |\{v|\deg_G(v) = 1\}| \geq \sum_{i=1}^{k}(2|V_i| - 1) + |\{v|\deg_G(v) = 1\}| = |V(G)| + in(G) - k$. Hence, $AR_\Sigma \geq \frac{1}{|V(G)|}(|V(G)| + in(G) - k)$ for any secret-sharing scheme Σ on G. ■

From Theorem 2.3 and Theorem 3.1, we have the following immediate result.

Theorem 3.2. *$c_{\mathcal{C}} \geq d_\Pi$ holds for any star covering Π and any core sequence $\mathcal{C}$ of a connected graph G. In particular, $c^*(G) \geq d^*(G)$.*

Corollary 3.3. *If there exists a star covering Π and a core sequence $\mathcal{C}$ of a connected graph G of order n such that $c_{\mathcal{C}} = d_\Pi$, then $c^*(G) = d^*(G) = d_\Pi = c_{\mathcal{C}}$ and $AR(G) = \frac{|V(G)|+in(G)-c^*(G)}{|V(G)|}$.*

The equality $c^*(G) = d^*(G)$ makes a criterion for examining whether the upper bound and the lower bound on $AR(G)$ will match or not. G is said to be *realizable* if $c^*(G) = d^*(G)$ holds. In the next part of this section, we shall propose some infinite classes of bipartite graphs and show that each of them is realizable.

B. New results

Our approach is to define a star covering Π of the given bipartite graph G first and then, based on this covering, construct a core sequence $\mathcal{C}$ of G satisfying $c_{\mathcal{C}} = d_\Pi$. We use $N_G(u)$ to denote the set of all neighbors of u in G and $N_G(S) = \bigcup_{v\in S} N_G(v)$ for any set $S \subseteq V(G)$. A vertex of degree one is called a 1-*vertex*. If V' is any subset of $V(G)$, we use V'_{k^+} to denote the set of all vertices in V' whose degree is not less than k, that is, $V'_{k^+} = \{v \in V'|\deg_G(v) \geq k\}$. From now on, we mainly consider connected bipartite graphs with girth not less than six. For a better description of our approach, we express a core sequence in terms of a vertex labeling of $IN(G)$. Let $\mathcal{C} = \{V_1, V_2, \ldots, V_k\}$ be a core sequence of G. Define $g : IN(G) \to \{1, \ldots, k\}$ such that "$g(v) = i \Leftrightarrow v \in V_i$". Then $g^{-1}(i) = V_i$ and $c_{\mathcal{C}} = |g(IN(G))|$. In this case, we say that the inverse images of g form the core sequence $\mathcal{C}$ of G. Furthermore, given a star covering Π of G and a set $E' \subseteq E(G)$, a component G' of $G\backslash E'$ has an induced star covering $\Pi|_{G'} = \{T\backslash E'|T \in \Pi \text{ and } E(T) \cap E(G') \neq \emptyset\}$. Note that, in $T\backslash E'$, we remove not only the edges in E' but also the resulting isolated vertices from T. So, each $T\backslash E'$ in $\Pi|_{G'}$ is again a star in G'.

In the proof of the next theorem, we need to define an orientation on G. Let $v_0, v_1, \ldots, v_l$ be successive vertices on a v_0v_l-trail (the vertices may repeat). By "orienting the trail from v_0 to v_l" we mean choosing the orientation $v_i \to v_{i+1}$ for each edge v_iv_{i+1}, $i = 0, \ldots, l-1$.

Theorem 3.4. *Let $G = (X, Y)$ be a connected bipartite graph with girth not less than six and $|X| \geq |Y|$. If $\deg_G(x) \leq 2$ for all $x \in X$, then G is realizable and $c^*(G) = |Y_{2^+}|$.*

Proof: Recall that $Y_{2^+} = \{y \in Y|\deg_G(y) \geq 2\}$. We use S_y to denote the star centered at y and having its leaves all neighbors of y. Then $\Pi = \{S_y|y \in Y\}$ is a star covering of G with vertex number sum $m_\Pi = |V(G)| + |X_{2^+}|$. This gives $d_\Pi = |V(G)| + in(G) - m_\Pi = |Y_{2^+}|$. Next, we define an orientation on G to help us construct the core sequence we need.

Case 1. If G contains a cycle C, then we start with an orientation of the edges of C so that C becomes a directed cycle. Next, we repeat the following process until all edges of G are oriented. We take a uv-trail passing through unoriented edges where u is a vertex to which at least two oriented edges are incident and v is a 1-vertex or a repeated vertex on the trail or also a vertex to which at least two oriented edges are incident and then orient the trial from u to v. By repeatedly doing this, we will eventually obtain an orientation of G because of its connectedness.

Case 2. If G is a tree, let $X_1 = \{x \in X|\deg_G(x) = 1\}$. Counting the edges of G, we have $|X_1| + 2(|X| - |X_1|) = |X|+|Y|-1 \leq 2|X|-1$ which implies $|X_1| \geq 1$. Let $x_0 \in X_1$ be the root of G and orient all edges toward the leaves. We have the orientation we need.

Note that in both cases, each vertex $v \in IN(G)$ has at least one in-neighbor and one out-neighbor in the orientation we defined. Now, we construct a core sequence of G. Initially, we label the vertices in Y_{2^+} differently, that is, let $g : Y_{2^+} \to \{1, 2, \ldots, k\}$, $k = |Y_{2^+}|$, be a bijection. Then, we will extend the domain of g to $IN(G)$ and keep its image unchanged at the same time. For each $x \in X_{2^+}$, define $g(x) = g(y)$ if (y, x) is an arc in the orientation. Since $\deg_G(x) = 2$ for all $x \in X_{2^+}$, x actually has exactly one in-neighbor $y \in Y_2^+$. Therefore, the extended mapping $g : IN(G) \to \{1, 2, \ldots, k\}$ is well-defined.

We claim that $\mathcal{C} = \{g^{-1}(1), g^{-1}(2), \ldots, g^{-1}(k)\}$ is a core sequence of G. First, by definition, $g^{-1}(1)$, $g^{-1}(2)$, …, $g^{-1}(k)$ clearly form a partition of $IN(G)$ and each $g^{-1}(i)$ induces a connected subgraph of G. Besides, each $y \in Y_{2^+}$ has at least one in-neighbor which is either a 1-vertex or a vertex $x \in X$ who receives the label from its in-neighbor $y' \neq y$. Hence each $y \in Y_{2^+}$ has a neighbor not in $g^{-1}(g(y))$. Similarly, each $x \in X_{2^+}$ receives the label from its in-neighbor $y \in Y_{2^+}$ and also has at least one out-neighbor $y' \neq y$ which is a 1-vertex or has initially gotten a label different from y's. So each $x \in X_{2^+}$ also has at least one neighbor not in $g^{-1}(g(x))$. Now, each vertex in $g^{-1}(i)$ does have a neighbor outside $g^{-1}(i)$ and these outside neighbors of vertices in $g^{-1}(i)$ certainly form an independent set in G because $g^{-1}(i)$ induces a connected subgraph of diameter at most two and G has girth not less then six. This shows that $\mathcal{C}$ is indeed a core sequence of length k, where $k = |Y_{2^+}| = d_\Pi$. ■

In a graph G, k-*subdividing* an edge is the operation of replacing the edge with a path of length k. A graph G' is called

an *even-subdivision* of G if it is obtained by $2k_e$-subdividing each edge $e \in E(G)$, where $k_e \geq 1$.

Corollary 3.5. *If G is a simple connected graph, then any even-subdivision G' of G is realizable. In addition, if G' is obtained by $2k_e$-subdividing each edge e of G and G is not a tree, then* $AR(G') = \frac{|V(G)|-|E(G)|+3\sum_{e\in E(G)} k_e}{|V(G)|-|E(G)|+2\sum_{e\in E(G)} k_e}$.

Proof: We may assume that G is not a tree. Let $v_1^e, v_2^e, \ldots, v_{2k_e-1}^e$ be the consecutive internal vertices of the path in G' that replaces the edge e in G. Then G' is a bipartite graph with bipartition $X = \{v_{2i+1}^e | e \in E(G), i = 0, 1, \ldots, k_e - 1\}$ and $Y = \{v_{2i}^e | e \in E(G), i = 1, \ldots, k_e - 1\} \cup V(G)$. So, $|X| = \sum_{e\in E(G)} k_e$ and $|Y| = \sum_{e\in E(G)}(k_e - 1) + |V(G)| = \sum_{e\in E(G)} k_e - |E(G)| + |V(G)| \leq |X|$. Since the girth of G' is not less than six and $\deg_{G'}(x) = 2$ for all $x \in X$, we know that G' is realizable by Theorem 3.4 and $c^*(G') = |Y_{2^+}| = \sum_{e\in E(G)}(k_e - 1) + in(G)$. With the facts $|V(G')| = \sum_{e\in E(G)}(2k_e - 1) + |V(G)|$ and $in(G') = \sum_{e\in E(G)}(2k_e - 1) + in(G)$, the optimal average information ratio of G' can be easily evaluated.

$$\begin{aligned} AR(G') &= \frac{|V(G')| + in(G') - c^*(G')}{|V(G')|} \\ &= \frac{|V(G)| - |E(G)| + 3\sum_{e\in E(G)} k_e}{|V(G)| - |E(G)| + 2\sum_{e\in E(G)} k_e}. \end{aligned}$$

■

This proof actually also works when G is not simple and G' has girth not less than six.

Corollary 3.6. *Let G be a connected graph with multiple edges and loops. Any even-subdivision G' of G is realizable if G' is of girth not less than six.*

In the proof of Theorem 3.4, we could have omitted the case where G is a tree because the result has been shown in [17]. However, we give the proof for self-containedness and make it easier to be referred to for the proof of the next theorem as well.

Theorem 3.7. *Let $G = (X, Y)$, $|X| \geq |Y|$, be a connected bipartite graph with girth not less than eight and $N_G(u) \cap N_G(v) \cap Y_{3^+} = \emptyset$ for all $u, v \in X_{3^+}$ and $u \neq v$. If for each $u \in X_{3^+}$, there exist neighbors $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_{\deg_G(u)-1}$ in $IN(G)$ such that each component $\widetilde{G}$ in $G\backslash E'$, where $E' = \{u\bar{u}_i | u \in X_{3^+}, i = 1, \ldots, \deg_G(u) - 1\}$, satisfies $|X \cap V(\widetilde{G})| \geq |Y \cap V(\widetilde{G})|$, then G is realizable and $c^*(G) = |Y_{2^+}| - \sum_{u\in X_{3^+}}(\deg_G(u) - 2)$.*

Proof: Let $N^*(u) = \{\bar{u}_i | i = 1, \ldots, \deg_G(u) - 1\}$ be the set of the neighbors of $u \in X_{3^+}$ stated in the theorem. We first claim that $N^*(u) \cap N^*(v) = \emptyset$ for all $u, v \in X_{3^+}$ and $u \neq v$. If this does not hold, then, by assumption, there exists a vertex $w \in N^*(u) \cap N^*(v)$ with $\deg_G(w) = 2$. As a consequence, the isolated vertex $\{w\} \subset Y$ would be a component in $G\backslash E'$. This contradicts to the given conditions. Next, as in the proof of Theorem 3.4, we give G a star covering $\Pi = \{S_y | y \in Y\}$ and initially define $g : Y_{2^+} \to \{1, 2, \ldots, k\}$, where $k = |Y_{2^+}|$, to be a bijection. Let us further define $g(u) = g(\bar{u}_1)$ for each $u \in X_{3^+}$ and alter the labels of $\bar{u}_i$'s ($i \geq 2$) by redefining $g(\bar{u}_i) = g(\bar{u}_1)$ for $i = 2, 3, \ldots, \deg_G(u) - 1$. After this alteration $|g(Y_{2^+} \cup X_{3^+})| = k - \sum_{u\in X_{3^+}}(\deg_G(u) - 2)$.

Let $\widetilde{G}_1, \widetilde{G}_2, \ldots, \widetilde{G}_s$ be the components in $G\backslash E'$, then $\widetilde{G}_i = (X \cap V(\widetilde{G}_i), Y \cap V(\widetilde{G}_i))$. Applying the proof of Theorem 3.4 to each $\widetilde{G}_i$, we can extend the domain of $g|_{Y_2^+ \cap IN(\widetilde{G}_i)}$ to $IN(\widetilde{G}_i)$ and keep its image unchanged. Jointly, we have extended the domain of g to $IN(G)$ and kept its image unchanged. In the remainder of the proof, it will be verified that the inverse images of g form a core sequence of G. It suffices to prove that each $g^{-1}(g(v))$ is a core, for each $v \in IN(G)$. First we show that each vertex $v \in IN(G)$ has a neighbor not in $g^{-1}(g(v))$. If $v = u$ for some $u \in X_{3^+}$, there exists $y' \in N_G(u) - N^*(u)$ who is either a 1-vertex or has a different label from u's because y' was initially given a label different from $\bar{u}_1$'s and has never been altered. If $v = \bar{u}_i \in N^*(u)$ for some $u \in X_{3^+}$ and $\deg_G(\bar{u}_i) = 2$, then $\bar{u}_i$ is a 1-vertex of some $\widetilde{G}_j$. According to the way we extend $g|_{Y_2^+ \cap IN(\widetilde{G}_j)}$, the neighbor of $\bar{u}_i$ in $\widetilde{G}_j$ has a label different from $\bar{u}_i$'s. Finally, if $v \in IN(G)\backslash X_{3^+}\backslash\{\bar{u}_i \in N^*(u) | u \in X_{3^+}, \deg_G(\bar{u}_i) = 2\}$, then $v \in IN(\widetilde{G}_j)$ for some j. It has been shown that v has a neighbor in $\widetilde{G}_j$ who is either a 1-vertex or has a label different from v's in the proof of Theorem 3.4. Hence, each vertex $v \in IN(G)$ has a neighbor not in $g^{-1}(g(v))$. These outside neighbors of vertices in $g^{-1}(g(v))$ certainly form an independent set in G because $g^{-1}(g(v))$ induces a connected subgraph of diameter at most four and the girth of G is at least eight. We conclude that the inverse images of g form a core sequence $\mathcal{C}$ of G with $c_{\mathcal{C}} = k - \sum_{u\in X_3^+}(\deg_G(u) - 2)$. On the other hand, the star covering Π has vertex-number sum

$$\begin{aligned} m_\Pi &= |V(G)| + \sum_{u\in X_{2^+}} (\deg_G(u) - 1) \\ &= |V(G)| + \sum_{u\in X_{3^+}} (\deg_G(u) - 2) + |X_{2^+}|. \end{aligned}$$

Therefore, it has deduction $d_\Pi = |V(G)| + |X_{2^+}| + |Y_{2^+}| - m_\Pi = c_{\mathcal{C}}$ as desired and the proof is completed. ■

We apply Theorem 3.7 to some classes of graphs. First, a graph G is more likely to be realizable if the size of X_{3^+} is small. We give an easy example for this. The *connectivity* $\kappa(G)$ of a graph G is the minimum number of vertices whose deletion disconnects G or results in a single vertex. G is called *k-connected* if $\kappa(G) \geq k$.

Corollary 3.8. *Let $G = (X, Y)$, $|X| \geq |Y|$, be a k-connected bipartite graph with girth not less than eight and $N_G(u) \cap N_G(v) \cap Y_{3^+} = \emptyset$ for all $u, v \in X_{3^+}$ and $u \neq v$. If $|X_{3^+}| < k$, then G is realizable.*

Proof: If $k = 1$, then $|X_{3^+}| = 0$. This result holds by Theorem 3.4. Assume that $k \geq 2$. For any $u \in X_{3^+}$, let $N^*(u)$ be a set of any $\deg_G(u) - 1$ neighbors of u and $E' = \{u\bar{u}_i | u \in X_{3^+}, \bar{u}_i \in N^*(u)\}$. Since $|X_{3^+}| < k$, $G\backslash E'$ is connected and has the same bipartition as G does. G is then realizable by Theorem 3.7. ■

Next, we consider graphs with minimum degree $\delta(G) \geq 2$ and examine the properties of the components in $G\backslash X_{3^+}$ that may hinder the graph G from being realizable.

Corollary 3.9. *Let $G = (X, Y)$, $|X| \geq |Y|$, be a connected bipartite graph with girth not less than eight, $\delta(G) \geq 2$ and $N_G(u) \cap N_G(v) \cap Y_{3^+} = \emptyset$ for all $u, v \in X_{3^+}$ and $u \neq v$. If none of the components in $G\backslash X_{3^+}$ is a tree, then G is realizable.*

Proof: Let $H = (X_H, Y_H)$ be any component of $G\backslash X_{3^+}$, where $X_H = X \cap V(H)$ and $Y_H = Y \cap V(H)$. Since each vertex in X_H is of degree 2 and H is not a tree, one has $2|X_H| \geq |X_H| + |Y_H|$ which gives $|X_H| \geq |Y_H|$. For any $u \in X_{3^+}$, if there is a neighbor $w \in N_G(u)$ who is a 1-vertex, then $\{w\}$ would be a tree component in $G\backslash X_{3^+}$. So all neighbors of u must be in $IN(G)$. In this case, we may choose the $\bar{u}_i$'s, $i = 1, \ldots, \deg_G(u) - 1$, to be any $\deg_G(u) - 1$ neighbors of u. If $\widetilde{G}$ is a component in $G\backslash E'$ which is not the same as any component in $G\backslash X_{3^+}$, then there must exist a component H in $G\backslash X_{3^+}$ such that $|X \cup V(\widetilde{G})| \geq |(X \cap V(H))| + 1$ and $Y \cap V(\widetilde{G}) = Y \cap V(H)$. Now, all criteria in Theorem 3.7 are made and the result follows. ∎

This corollary assures that nontree components in $G\backslash X_{3^+}$ do not prohibit G from being realizable. It is the tree components in $G\backslash X_{3^+}$ that matter the most. Theorem 3.7 fails when tree components in $G\backslash X_{3^+}$ are concentrated around some vertices in X_{3^+}. We give a method to detect this situation.

Given a bipartite graph $G = (X, Y)$, $|X| \geq |Y|$, and some tree components $T_1, \ldots, T_t$ in $G\backslash X_{3^+}$, we define the *suspending number* of the collection $\mathbb{H} = \{T_1, \ldots, T_t\}$, written as $\mathrm{susp}(\mathbb{H})$, to be the cardinality of the set $\{u \in X_{3^+} | u$ is adjacent to some vertices of T_j in G, $1 \leq j \leq t\}$.

Corollary 3.10. *Let $G = (X, Y)$, $|X| \geq |Y|$, be a connected bipartite graph with girth not less than eight, $\delta(G) \geq 2$ and $N_G(u) \cap N_G(v) \cap Y_{3^+} = \emptyset$ for all $u, v \in X_{3^+}$ and $u \neq v$. If $\mathrm{susp}(\mathbb{H}) \geq |\mathbb{H}|$ holds for every collection $\mathbb{H}$ of tree components in $G\backslash X_{3^+}$, then G is realizable.*

Proof: If $T = (X_T, Y_T)$ is any tree component in $G\backslash X_{3^+}$ where $X_T = X \cap V(T)$ and $Y_T = Y \cap V(T)$, then $2|X_T| = |X_T| + |Y_T| - 1$ which implies that $|X_T| = |Y_T| - 1$. Let $\mathbb{U} = \{T_i | i \in I\}$ be the collection of all tree components in $G\backslash X_{3^+}$. We define a bipartite graph $A = (I, X_{3^+})$ in which (i, v) is an edge of A if and only if v is adjacent to some vertices of T_i in G. For every $J \subseteq I$, let $\mathbb{H} = \{T_j | j \in J\}$, then $|N_A(J)| = \mathrm{susp}(\mathbb{H}) \geq |\mathbb{H}| = |J|$. By Hall's Theorem, there exists a matching M in A that saturates I. Let $M = \{(i, v_i) | i \in I\}$ and, for each $i \in I$, let v_i^* be a vertex of T_i which is adjacent to v_i in G. For $v \in X_{3^+}\backslash\{v_i | i \in I\}$, v^* can be arbitrarily chosen from $N_G(v)$. Note that for any $u \in X_{3^+}$, $N_G(u)\backslash\{u^*\} \subseteq IN(G)$. If this does not hold, then there exists $w \in N_G(u)\backslash\{u^*\}$ with $\deg_G(w) = 1$. The trivial component $\{w\}$ would be a tree component in $G\backslash X_{3^+}$. The vertex w must be u^*, giving a contraction. Now, let $E' = \{uu' | u \in X_{3^+}, u' \in N_G(u)\backslash\{u^*\}\}$ and for all $i \in I$, we also let T_i^* be the graph obtained from T_i by attaching to T_i each edge vv^* with $v \in X_{3^+}$ and $v^* \in V(T_i)$. The collection of all tree components in $G\backslash E'$ is exactly $\{T_i^* | i \in I\}$. From what we have shown at the beginning of this proof, one has that $|X \cap V(T_i)| = |Y \cap V(T_i)| - 1$. This consequently gives $|X \cap V(T_i^*)| \geq |X \cap V(T_i)| + 1 = |Y \cap V(T_i)| = |Y \cap V(T_i^*)|$. Now, we have shown that all tree components in $G\backslash E'$ satisfy the criteria in Theorem 3.7. The proof of the previous corollary guarantees that nontree components also do. The result of this corollary follows immediately. ∎

IV. Conclusion

In this paper, we extend the idea $c^*(T) = d^*(T)$ for trees to general graphs and determine the exact values of the optimal average information ratio for some classes of bipartite graphs. Appendantly, we also conclude that the covering $\{S_y | y \in Y\}$ is a star covering with the least vertex-number sum for each of these realizable bipartite graphs.

There still is a lot of room for exploration in this direction of research. First of all, identifying exact conditions under which a bipartite graph is realizable is an interesting problem to investigate. Besides, the idea of the deduction of a star covering can be further generalized. One can define the deduction of a complete multipartite covering in the same way. Finding proper complete multipartite coverings of a graph with the largest deduction to match the core number of that graph is an intriguing generalization of what we have proposed in this paper.

Acknowledgment

This work is supported in part by the National Science Council of Taiwan under Grants NSC 100-2115-M-239-001.

References

[1] A. Beimel and N. Livne, On matroids and non-ideal secret sharing, in: Proceedings of the third theory of cryptography conference, *LNCS*, **3876** (2006), 482–501.

[2] G. R. Blakley, Safeguarding cryptographic keys, in "Proceedings of the National Computer Conference, 1979", *American Federation of Information Processing Societies Proceedings*, **48** (1979), 313–317.

[3] C. Blundo, A. De Santis, R. De Simone and U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Designs, Codes and Cryptography*, **11** (1997), 107–122.

[4] C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, On the information rate of secret sharing schemes, *Theoretical Computer Science*, **154** (1996), 283–306.

[5] C. Blundo, A. De Santis, A. Giorgio Gaggian and U. Vaccaro, New bounds on the information rate of secret sharing schemes, *IEEE Transactions on Information Theory*, **41** (1995), 549–554.

[6] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, *J. Cryptology*, **8** (1995), 39–64.

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

[8] E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. Cryptology*, **5** (1992), 153–166.

[9] L. Csirmaz, The size of a share must be large, *J. Cryptology*, **10** (1997), 223-231.

[10] L. Csirmaz, An impossibility result on graph secret sharing, *Designs, Codes and Cryptography*, **53** (2009), 195–209.

[11] L. Csirmaz, Secret sharing schemes on graphs, *Studia Mathematica Hungarica*, **10** (1997), 297–306.

[12] L. Csirmaz and P. Ligeti, On an infinite families of graphs with information ratio $2 - \frac{1}{k}$, *Computing*, **85** (2009), 127–136.

[13] L. Csirmaz and G. Tardas, Exact bounds on tree based secret sharing schemes, *Tatracrypt* 2007, Slovakia.

[14] I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

[15] M. van Dijk, On the information rate of perfect secret sharing schemes, *Designs, Codes and Cryptography*, **6** (1995), 143–169.

[16] W.-A. Jackson and K. M. Martin, Perfect secret sharing schemes on five participants, *Designs Codes and Cryptography*, **9** (1996), 267–286.
[17] H-C Lu and H-L Fu, The exact values of the average information ratio for tree-based access structures of perfect secret sharing schemes, submitted.
[18] J. Marti-Farré and C. Padró, Secret sharing schemes with three or four minimal qualified subsets, *Designs, Codes and Cryptography*, **34** (2005), 17–34.
[19] P. Morillo, C. Padro, G. Saez and J. L. Villar, Weighted threshold secret sharing schemes, *Information Processing Letters*, **704** (1999), 211–216.
[20] C. Padro and G. Saez, Secret Sharing Schemes with Bipartite Access Structure, *IEEE Transactions on Information Theory*, **46(7)** (2000), 2596–2604.
[21] A. Shamir, How to share a secret, *Communications of the ACM*, **22** (1979), 612–613.
[22] D. R. Stinson, An explication of secret sharing schemes, *Designs Codes and Cryptography*, **2** (1992), 357–390.
[23] D. R. Stinson, New general lower bounds on the information rate of perfect secret sharing schemes, in "Advances in Cryptology – CRYPTO '92", E. F. Brickell, ed., *Lecture Notes in Computer Science*, **740** (1993), 168–182.
[24] D. R. Stinson, Decomposition constructions for secret sharing schemes, *IEEE Transactions on Information Theory*, **40** (1994), 118–125.