International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:7, 2014

A New Bound on the Average Information Ratio of Perfect Secret-Sharing Schemes for Access Structures Based On Bipartite Graphs of Larger Girth

Hui-Chuan Lu

Abstract—In a perfect secret-sharing scheme, a dealer distributes 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 the participants in any unqualified subset is statistically independent of the secret. The access structure of the scheme refers to the collection of all qualified subsets. In a graph-based access structures, 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 realizing a given access structure is the ratio of the average length of the shares given to the participants to the length of the secret. The infimum of the average information ratio of all possible perfect secret-sharing schemes realizing an access structure is called the optimal average information ratio of that access structure. We study the optimal average information ratio of the access structures based on bipartite graphs. Based on some previous results, we give a bound on the optimal average information ratio for all bipartite graphs of girth at least six. This bound is the best possible for some classes of bipartite graphs using our approach.

Keywords—Secret-sharing scheme, average information ratio, star covering, deduction, core cluster.

I. Introduction

In a *secret-sharing scheme*, there is a dealer who has a secret, a finite set P of participants and a collection Γ of subsets of P called the *access structure*. Each subset in Γ is a qualified subset. A secret-sharing scheme is a method by which the dealer distributes a secret among the participants in P such that only the 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 the secret-sharing scheme is called *perfect*. Since we only consider perfect ones, "secret-sharing scheme" will be used for "perfect secret-sharing scheme" throughout this paper. An access structure of a secret-sharing scheme must be *monotone* which means that any subset of P containing a qualified subset must also be qualified. Therefore, the family of all minimal subsets of Γ, called the *basis* of it, completely determine the access structure Γ.

The first secret-sharing schemes are the (t, n)-*threshold schemes* introduced by Shamir [18] and Blakley [1] independently in 1979. In such a scheme, the basis of the access structure consists of all t-subsets of the participant set of size n. The problem regarding secret sharing has been widely studied since then. The *information ratio* and the *average information ratio* of secret-sharing schemes have been the main subjects of discussion. 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. The average information ratio of a secret-sharing scheme specifies the ratio of the average length of the shares given to the participants to the length of the secret. For the efficiency of a scheme, these ratios are expected to be as low as possible. Given an access structure Γ, the infimum of the (average) information ratio of all possible secret-sharing schemes realizing this access structure Γ is referred to as the *optimal (average) information ratio* of Γ.

Hui-Chuan Lu is with Center for Basic Required Courses, National United University, Miaoli, Taiwan 36003. (e-mail: hjlu@nuu.edu.tw; hht0936@seed.net.tw)

In this paper, we consider graph-based access structures. In the *access structure based on a simple graph* G, each vetex represents a participant and each edge 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.

Given a discrete random variable X with possible values $\{x_1, x_2, \ldots, x_n\}$ and a probability distribution $\{p(x_i)\}_{i=1}^n$, the Shannon entropy of X is defined as $H(X) = -\sum_{i=1}^n p(x_i) \log p(x_i)$ [13]. Using Shannon entropy, the information ratio of the scheme Σ can be defined as $R_\Sigma = \max_{v \in V(G)}\{H(\zeta_v)/H(\zeta_S)\}$ and the average information ratio of Σ is $AR_\Sigma = (\sum_{v \in V(G)} H(\zeta_v))/(|V(G)|H(\zeta_S))$. For simplicity, with the same symbol G, we will denote both the graph as well as the access structure based on it. For instance, "a secret-sharing scheme on G" refers to "a secret-sharing scheme for the access structure based on G". Furthermore, the optimal information ratio $R(G)$ of G and the optimal average information ratio $AR(G)$ of G are the infimum of the information ratio R_Σ and the average information ratio AR_Σ over all possible secret-sharing schemes Σ on G respectively. It is well known that $R(G) \geq AR(G) \geq 1$ [8] and that $R(G) = 1$ if and only if $AR(G) = 1$. A secret-sharing scheme Σ with the optimal ratio $R_\Sigma = 1$ or $AR_\Sigma = 1$ is called *ideal*. An access structure G is ideal if there exists an ideal secret-

sharing scheme on it.

Most results regarding $R(G)$ and $AR(G)$ give bounds on them [2]–[7], [9], [10], [14], [15], [19]–[21]. Stinson [21] showed that $R(G) \leq \frac{d+1}{2}$, where d is the maximum degree of G, and $AR(G) \leq \frac{2m+n}{2n}$, where $n = |V(G)|$ and $m = |E(G)|$. These are the most important bounds for general graphs. Due to the difficulty of finding results on general graphs, most efforts have been focused on graphs with better structures such as paths and cycles [2], [5], [9], [21] and small graphs which are of order no more than six [5], [14], [15]. The optimal information ratio and the optimal average information ratio of any tree were determined by Csirmaz and Tardos [12] in 2007 and by Lu and Fu [16] in 2011 respectively. Csirmaz and Ligeti [11] showed that $R(G) = 2 - 1/k$, where k is the maximum degree of G, in 2009 for some graphs of larger girth. Lu and Fu [17] have determined the exact vlaues of the optimal average information ratio of some bipartite graphs of larger girth in 2014. Based on their results, we give bounds on the optimal average information ratio of all bipartite graphs of girth at least six.

This paper is organized as follows. In Section II, we recall some basic definitions and state some previous results for the discussion later. In Section III, we present our bound on $AR(G)$ for any bipartite graph G of girth at least six. Our bound is the best possible for some classes of bipartite graphs using our approach. A concluding remark will be given in the final section.

II. Preliminaries

In this paper, we only consider simple graphs without loops and isolated vertices, not necessarily connected. For terms and notations in Graph Theory, please refer to [22]. Birckell and Davenport [6] have given complete characterization of ideal graph-based access structures as follows.

Theorem 1 ([6]). *Suppose that G is a connected graph. Then $R(G) = AR(G) = 1$ if and only if G is a complete multipartite graph.*

A *complete multipartite covering* of a graph G 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. Using a complete multipartite covering of G, Stinson [21] provides an excellent method for building up a secret-sharing scheme on G.

Theorem 2 ([21]). *Suppose that $\Pi = \{G_1, G_2, \ldots, G_l\}$ is a complete multipartite covering of a graph G of order n. Then there exists a secret-sharing scheme Σ on G with average information ratio $AR_\Sigma = m_\Pi/n$.*

According to this result, a complete multipartite covering with the least vertex-number sum is what we need to construct a secret-sharing scheme on a graph with lower average information ratio. If each subgraph in a complete multipartite covering is a star, then this covering is also called a *star covering*. A star covering is most suitable for graphs of larger girth. Finding a suitable star covering of G is the main tool in [17] to obtain upper bounds on $AR(G)$.

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, the *deduction* of Π is defined as $d_\Pi = |V(G)| + in(G) - m_\Pi$. A star covering with the least vertex-number sum gives the largest deduction. The largest deduction over all star coverings of G is denoted as $d^*(G)$, called the deduction of G. A star covering Π with $d_\Pi = d^*(G)$ is referred to as an *optimal star covering* of G. An upper bound on $AR(G)$ obtained from Theorem 2 can be written in terms of deduction as follows.

Corollary 1 ([21]). *If Π is a star covering of a graph G with deduction d_Π, then $AR(G) \leq \frac{|V(G)|+in(G)-d_\Pi}{|V(G)|}$.*

Next, we introduce some definitions and notations in order to describe the lower bound on $AR(G)$ in [17]. A subset $V_0 \subseteq V(G)$ is said to be *connected* if it induces a connected subgraph in G. Csirmaz et al [11] defined a *core* of G as a connected subset $V_0 \subseteq V(G)$ satisfying that (i) each vertex $v \in V_0$ has a *designated outside neighbor* $\bar{v}$ which is defined as a neighbor of v that is outside V_0 and is not adjacent to any other vertex in V_0, and (ii) $\{\bar{v} | v \in V_0\}$ is an independent set in G. A *core cluster* g of G of size c_g is defined in [16] as a vertex labeling $g : IN(G) \to \mathbb{N} \cup \{0\}$ such that each $g^{-1}(i)$, $i \in g(IN(G))$, is a core of G, where $c_g = |g(IN(G))|$. We also denote the minimum size of a core cluster of G as $c^*(G)$, called the *core number* of G. The core number of $K_{1,1}$ is naturally defined as $c^*(K_{1,1}) = 0$. A core cluster of size $c^*(G)$ is referred to as an *optimal core cluster* of G.

Theorem 3 ([16]). *If g is a core cluster of a graph G, then $AR(G) \geq \frac{|V(G)|+in(G)-c_g}{|V(G)|}$.*

By Theorem II and Corollary II, the following results are straightforward.

Theorem 4 ([16]). *The inequality $c_g \geq d_\Pi$ holds for any star covering Π and core cluster g of a graph G. In particular, $c^*(G) \geq d^*(G)$.*

Corollary 2 ([16]). *If there exists a star covering Π and a core cluster g of a graph G such that $c_g = d_\Pi$, then $c^*(G) = d^*(G) = c_g = d_\Pi$ and $AR(G) = \frac{|V(G)|+in(G)-c^*(G)}{|V(G)|}$.*

Therefore, the equality $c^*(G) = d^*(G)$ makes a criterion for examining whether the lower bound and the upper bound on $AR(G)$ will match. G is called *realizable* if $c^*(G) = d^*(G)$ holds. An infinite class of realizable bipartite graphs of larger girth proposed by Lu and Fu [17] will be introduced later.

Let $G = (X, Y)$ be a bipartite graph with partite sets X and Y where $|X| \geq |Y|$. For $\widetilde{V} = X$ or Y, we denote as $\widetilde{V}^{k^+}$ the set $\{x \in \widetilde{V} | \deg_G(x) \geq k\}$. A component H in $G - X^{3^+}$ with $|X \cap V(H)| \geq |Y \cap V(H)|$ is called a *proper component* in $G - X^{3^+}$. A component in $G - X^{3^+}$ is *improper* if it is not proper. Lu and Fu define an *adjacency graph of improper components* A_G as follows. Let $\mathbb{U}_0 = \{T_i | i \in I_0\}$ be the collection of improper components in $G - X^{3^+}$ and let $\widetilde{X}^{3^+} = \{v \in X^{3^+} | v \text{ is adjacent to some } T_i \in \mathbb{U}_0 \text{ in } G\}$. The adjacency graph of improper components is a bipartite graph

$A_G = (\mathbb{U}_0, \widetilde{X}^{3^+})$ such that for all $T_i \in \mathbb{U}_0$ and $v \in \widetilde{X}^{3^+}$, (T_i, v) is an edge in A_G if and only if v is adjacent to some vertex of T_i in G. Suppose that $M_0 = \{(T_j, v_j)|j \in J_0\}$ ($J_0 \subseteq I_0$) is a maximum matching in A_G. The number $|I_0 \backslash J_0|$ is independent of the choices of maximum matchings and is denoted as $\mathrm{exc}(G)$.

Theorem 5 ([16]). *If $G = (X, Y)$ and $|X| \geq |Y|$, then there exists a star covering Π of G with $d_\Pi = |Y^{2^+}| - \sum_{v \in X^{3^+}} (\deg_G(v) - 2) + \mathrm{exc}(G)$.*

Let us denote the value $|Y^{2^+}| - \sum_{v \in X^{3^+}} (\deg_G(v) - 2) + \mathrm{exc}(G)$ as $\beta(G)$ in the remainder of this paper. A cycle is called *feasible* if it contains two vertices of degree two which are of distance at least four. A feasible cycle is of length at least eight. If every cycle in a graph G is feasible, then G is called feasible as well.

Theorem 6 ([16]). *Let $G = (X, Y)$ and $|X| \geq |Y|$. If G is feasible, then G is realizable and $c^*(G) = \beta(G)$.*

Based on these results, we derive a bound on $AR(G)$ in the next section.

III. A Bound on $AR(G)$

A *k-subdivision* of an edge in a graph is the operation of replacing the edge with a path of length k. An unfeasible graph can be made feasible by suitably subdividing some edges of it. This suggests a possibility to derive bounds on the optimal average information ratio of the graph. We investigate the effect of subdividing an edge of G on the values of $c^*(G)$ and $d^*(G)$ first. In the discussion of the following results, we assume that G' is obtained by replacing an edge u_0u_1 of G with a path which has consecutive vertices $u_0 = w_0, w_1, \ldots, w_{2l+1} = u_1$.

Proposition 1. *If G' is a graph obtained by $(2l+1)$-subdividing a nonpendant edge of G where $l \geq 3$, then $d^*(G') = d^*(G) + l$.*

Proof. Let Π be a star covering of G, then a star covering of G' can be constructed in a natural way. Let us denote the star with only two edges $w_{i-1}w_i$ and w_iw_{i+1} as S_i. Since we may assume that u_0u_1 belong to a star S_{u_0} centered at u_0 in Π, $\Pi' = (\Pi \backslash \{S_{u_0}\}) \cup \{(S_{u_0} - u_0u_1) + w_0w_1, S_{w_2}, S_{w_4}, \ldots, S_{w_{2l}}\}$ is a star covering of G' with vertex-number sum $m_{\Pi'} = m_\Pi + 3l$. The deduction of Π' will then be $d_{\Pi'} = (|V(G)| + 2l) + (in(G) + 2l) - (m_\Pi + 3l) = d_\Pi + l$. Therefore, we have $d^*(G') \geq d^*(G) + l$. On the other hand, if Π' is an optimal star covering of G', then a star covering of G can be constructed from Π' as follows. First, if none of w_0 and w_{2l+1} is the center of any star in Π' which has some leaves in $V(G)$, then we let S be the star with a unique edge u_0u_1. For the rest case, since the w_0w_{2l+1}-path which replaces u_0u_1 is of odd length, we may assume that only w_0 is the center of a star S'_{w_0} in Π' which has leaves in both $V(G)$ and $\{w_i|i = 1, \ldots, 2l\}$, and that w_{2l+1} is not the center of such kind of stars. In this case, we let $S = (S'_{w_0} - \{w_1\}) + u_0u_1$. Now, discarding all stars containing vertices in $\{w_1, w_2, \ldots, w_{2l}\}$ from Π' and adding the star S to it, we have a star covering Π of G which has vertex-number sum $m_\Pi = m_{\Pi'} - 3l$ where $m_{\Pi'}$ is the vertex-number sum of Π' and the deduction $d_\Pi = (|V(G')| - 2l) + (in(G') - 2l) - (m_{\Pi'} - 3l) = d_{\Pi'} - l$. This gives $d^*(G) \geq d^*(G') - l$ and the result follows. □

The gap between $c^*(G)$ and $c^*(G')$ depends largely on the edge that is being subdivided. We classify the edges of G as follows. An edge u_0u_1 is said to be of *type 1* if either one of the following two conditions is true: (1) u_0u_1 does not belong to any cycle in G, or (2) it belongs to some cycle $(u_0u_1 \cdots u_l)$ and there is no path in G which connects u_0 and some u_i, $i \in \{1, 2, \ldots, l\}$, without traversing any edge of the cycle. In case (1), any vertex in $N_G(u_0) \backslash \{u_1\}$ is called a *friendly neighbor* of the edge u_0u_1. In case (2), the vertex u_l of u_0 is assigned to be the friendly neighbor of u_0u_1. An edge not of type 1 is said to be of *type* $r+1$, $r \in \mathbb{N}$, if it is the unique common edge of exactly r cycles and any two of these r cycles have no common vertices other than u_0 and u_1. In the proof of the next two lemmas, the construction of desired core cluster involves fiddly description. We make use of the following notations and an operation to facilitate the discussion. If g is a core cluster of G and $u \in IN(G)$, then we denote the designated outside neighbor of u as $(u)^*_g$ and let $(\widetilde{V})^*_g = \{(u)^*_g | u \in \widetilde{V}\}$. Besides, if $\widetilde{V}$ is a connected subset of $V(G)$ which induces a connected subgraph K of G, and A_0 and A_1 are disjoint connected subsets of $\widetilde{V}$, then we define a *splitting operation* on $\widetilde{V}$ as follows. Suppose that $\mathbb{U} = \{O_i | i \in I\}$ is the collection of all components in $K - A_0$ and $O_1 \in \mathbb{U}$ is the component containing A_1. Let $\widetilde{V}^{[1]} = V(O_1)$ and $\widetilde{V}^{[0]} = \widetilde{V} \backslash \widetilde{V}^{[1]}$, then both $\widetilde{V}^{[0]}$ and $\widetilde{V}^{[1]}$ are connected. By applying the splitting operation to $\widetilde{V}$ w.r.t. A_0 and A_1, we have two disjoint subsets $\widetilde{V}^{[0]}$ and $\widetilde{V}^{[1]}$ with $A_i \subseteq \widetilde{V}^{[i]}$, $i = 0, 1$, such that $\widetilde{V}^{[0]} \cup \widetilde{V}^{[1]} = \widetilde{V}$. Let us denote this process as $\mathrm{Split}(\widetilde{V}; A_0, A_1) = (\widetilde{V}^{[0]}, \widetilde{V}^{[1]})$.

Let g' be an optimal core cluster of G'. In the proof of Lemma 1 and Lemma 2, we initially define a labeling g on $IN(G)$ as $g = g'|_{IN(G)}$ and let $(u)^*_g = (u)^*_{g'}$ for all $u \in IN(G)$ when there is no specification. The labeling g may require some modification accordingly in order to reach to a core cluster of G. There are many cases to discuss. Let $(g')^{-1}(i) \cap V(G) = V_i$. One situation that worsens our problem the most is when $\{u_0, u_1\} \subseteq (V_a)^*_{g'}$ for some $a \in g'(IN(G'))$ where u_0u_1 is the edge been subdivided. This situation is referred to as Situation (S^*). In what follows, we assume that $u_0 = (y^i_0)^*_{g'}$ and $u_1 = (y^i_1)^*_{g'}$ where $\{y^i_0, y^i_1\} \subseteq V_{a_i}$ for all $i = 1, 2, \ldots, t$, and $\{u_0, u_1\} \nsubseteq (V_i)^*_{g'}$ for all $i \in g'(IN(G')) \backslash \{a_i | i = 1, \ldots, t\}$. Naturally, $t > 0$ when Situation (S^*) occurs and $t = 0$ otherwise. When $t > 0$, we use $V^{[0]}_{a_i}$ and $V^{[1]}_{a_i}$ to denote the resulting subsets from applying the splitting operation to V_{a_i} w.r.t. $\{y^i_0\}$ and $\{y^i_1\}$, i.e. $\mathrm{Split}(V_{a_i}; \{y^i_0\}, \{y^i_1\}) = (V^{[0]}_{a_i}, V^{[1]}_{a_i})$, for all $i = 1, \ldots, t$. Moreover, the numbers $c_0, c_1, \ldots, c_t$, d_0 and d_1 that will be used in the proof always represent distinct integers in $\mathbb{N} \backslash g'(IN(G'))$. The girth of G is written as $\mathrm{girth}(G)$ in the following results. With the aid of these notations, we can present our construction of core clusters of G in a more systematic way.

Lemma 1. *Let G' be a graph obtained by $(2l+1)$-subdividing*

a nonpendant edge u_0u_1 of a simple graph G with $\mathrm{girth}(G) \geq 6$*, where $l \geq 3$. If g' is an optimal core sequence of G' and $g'(u_0) = g'(u_1)$, then $c^*(G) \leq c^*(G') - l + r$ provided that u_0u_1 is an edge of type r.*

Proof. If $\{(u_0)^*_{g'}, (u_1)^*_{g'}\} \subseteq V(G)$, then $|\{g'(w_i)|\ i = 1, \ldots, 2l\}\backslash\{g'(u_0)\}| \geq l - 1$ and the labeling $g = g'|_{IN(G)}$ is a core cluster of G with $|g(IN(G))| \leq |g'(IN(G'))| - (l - 1)$. Now, we assume that $g'(u_0) = g'(u_1) = 0$ and $\{(u_0)^*_{g'}, (u_1)^*_{g'}\} \nsubseteq V(G)$, then $|\{g'(w_i)|i = 1, \ldots, 2l\}\backslash\{0\}| \geq l$ and g may no longer be qualified as a core cluster of G. We shall make some local modifications of g and assign $(u_0)^*_g = u_1$ and $(u_1)^*_g = u_0$ to reach our goal. Set $A_0 = \{u_0\} \cup ((N_G(u_0)\backslash\{u_1\}) \cap V_0)$ and $A_1 = \{u_1\} \cup ((N_G(u_1)\backslash\{u_0\}) \cap V_0)$. Since u_0 and u_1 have no common neighbors, A_0 and A_1 are disjoint connected subsets of the connected set V_0. Applying the splitting operation $\mathrm{Split}(V_0; A_0, A_1) = (V_0^{[0]}, V_0^{[1]})$, we have two disjoint connected subsets $V_0^{[0]}$ and $V_0^{[1]}$ with $V_0^{[0]} \cup V_0^{[1]} = V_0$.

(1) Suppose first that $t = 0$, that is, Situation (S^*) does not occur. By redefining $g(V_0^{[0]}) = \{c_0\}$, we claim that the resulting labeling g is a core cluster of G. Note that now $g(u_0) = c_0 \neq g(u_1)$, and u_0 is adjacent to $u_1 \in V_0^{[1]}$ and no other vertices in $V_0^{[1]}$. Besides, $\{u_0\} \cup (V_0^{[1]})^*_{g'}$ is independent because $(g')^{-1}(0)$ is a core in G' containing $\{u_0\} \cup V_0^{[1]}$ and each $(w)^*_{g'} \in (V_0^{[1]})^*_{g'}$ is adjacent to the unique vertex w in $(g')^{-1}(0)$. Hence, $(u_1)^*_g = u_0$ and $(w)^*_g = (w)^*_{g'}$, for all $w \in V_0^{[1]}\backslash\{u_1\}$, are qualified designated outside neighbors of vertices in $V_0^{[1]}$ and then $V_0^{[1]} = g^{-1}(0)$ is a core of G. The fact $g^{-1}(c_0) = V_0^{[0]}$ is also a core of G can be shown by similar reasoning. We then conclude that g is a core cluster of G and $|g(IN(G))| \leq |g'(IN(G'))| - l + 1$.

(2) Suppose that $t > 0$, then $r \geq t + 1$. Besides making $g(V_0^{[0]}) = \{c_0\}$, we further redefine $g(V_{a_i}^{[0]}) = \{c_i\}$ for all $i = 1, \ldots, t$. Since $g(y_0^i) = c_i \neq g(y_1^i) = a_i$, $V_{a_i}^{[0]}$ and $V_{a_i}^{[1]}$ are cores of G. g is then a core cluster of G with $|g(IN(G))| \leq |g'(IN(G'))| - l + (t + 1)$. □

Lemma 2. *Let G' be a graph obtained by $(2l+1)$-subdividing a nonpendant edge u_0u_1 of a simple graph G with* $\mathrm{girth}(G) \geq 6$*, where $l \geq 3$. If g' is an optimal core cluster of G' and $g'(u_0) \neq g'(u_1)$, then $c^*(G) \leq c^*(G') - l + r$ provided that u_0u_1 is an edge of type r.*

Proof. We split the discussion into two cases.

Case 1. Assume that $g'(u_0) = 0 \neq g'(u_1) = 1$ and $\{(u_0)^*_{g'}, (u_1)^*_{g'}\} \subseteq V(G)$, then $|\{g'(w_i)|i = 1, \ldots, 2l\}\backslash\{0, 1\}| \geq l - 1$ and $g = g'|_{IN(G)}$ is not a core cluster of G only when any of the following three situations occurs. Situation $(S1) : u_1 = (x_1)^*_{g'}$ for some $x_1 \in V_0$; Situation $(S2) : u_0 = (x_0)^*_{g'}$ for some $x_0 \in V_1$; and the stated Situation (S^*). We shall fix the problem by shifting some vertices between V_0 and V_1 or adding some extra values to $g(IN(G))$ as follows.

Subcase 1-1. Suppose that both Situation $(S1)$ and $(S2)$ do not occur, then $t > 0$. If $r = t = 1$, let us assume that y_0^1 is the friendly neighbor of u_0u_1. We redefine $g(V_{a_1}^{[0]}) = \{0\}$ and then assign $(u_0)^*_g = u_1$ and choose a neighbor of y_0^1 in $V_{a_1}^{[1]}$ to be $(y_0^1)^*_g$. Since u_0u_1 is of type 1, each vertex in $V_{a_1}^{[0]}$ is not adjacent to any vertex in $V_0\backslash\{u_0\}$ and $\{(y_0^1)^*_g\} \cup (V_{a_1}^{[0]}\backslash\{y_0^1\})^*_{g'} \cup (V_0)^*_{g'}$ is independent. This guarantees that $g^{-1}(0) = V_0 \cup V_{a_1}^{[0]}$ is a core of G. Besides, $g(y_0^1) \neq g(y_1^1)$ implies that $V_{a_1}^{[1]}$ is also a core. Hence, g is a core cluster of G with $|g(IN(G))| \leq |g'(IN(G'))| - (l - 1) = c^*(G') - l + r$. If $r > 1$, then $r \geq t + 1$. By redefining $g(V_{a_i}^{[0]}) = \{c_i\}$ for all $i = 1, \ldots, t$, and letting $(u)^*_g = (u)^*_{g'}$ for all $u \in IN(G)$, we have a core cluster g of G with $|g(IN(G))| \leq |g'(IN(G'))| - (l - 1) + t \leq c^*(G') - l + r$.

Subcase 1-2. Suppose that Situation $(S1)$ occurs and $(S2)$ does not, then either $t = 0$ and $r \geq 1$ or $t > 0$ and $r \geq t + 2$. Let $\mathrm{Split}(V_0; \{u_0\}, \{x_1\}) = (V_0^{[0]}, V_0^{[1]})$. When $r \in \{1, 2\}$ $(t = 0)$, we redefine $g(V_0^{[0]}) = \{1\}$. One can easily verify that $g^{-1}(1) = V_0^{[0]} \cup V_1$ is a core of G and therefore g is a core cluster of G with $|g(IN(G))| \leq |g'(IN(G'))| - (l - 1)$. When $r \geq 3$, redefining $g(V_0^{[0]}) = \{c_0\}$ is sufficient if $t = 0$. After assigning $u_1 = (x_1)^*_g$, g is a core cluster of G with $|g(IN(G))| \leq |g'(IN(G'))| - (l - 1) + 1 \leq c^*(G') - l + 2$. If $t > 0$, we further redefine $g(V_{a_i}^{[0]}) = \{c_i\}$ for all $i = 1, \ldots, t$. The resulting labeling g is a core cluster of G with $|g(IN(G))| \leq |g'(IN(G'))| - (l-1) + t + 1 \leq c^*(G') - l + r$.

Subcase 1-3. Suppose that Situation $(S1)$ and $(S2)$ occur simultaneously, then $r \geq t + 3$. When $t = 0$, we redefine $g(V_0^{[0]} \cup V_1^{[0]}) = \{d_0\}$ if $r = 3$, and redefine $g(V_0^{[0]}) = \{d_0\}$ and $g(V_1^{[0]}) = \{d_1\}$ if $r \geq 4$. In both cases, g is a core cluster of G with $|g(IN(G))| \leq c^*(G') - l + 3$. When $t > 0$, besides making $g(V_0^{[0]}) = \{d_0\}$ and $g(V_1^{[0]}) = \{d_1\}$, we further redefine $g(V_{a_i}^{[0]}) = \{c_i\}$ for all $i = 1, \ldots, t$. This results in a core cluster g of G that meets our requirement where $|g(IN(G))| \leq c^*(G) - l + r$.

Case 2. Assume that $g(u_0) = 0 \neq g(u_1) = 1$ and $\{(u_0)^*_{g'}, (u_1)^*_{g'}\} \nsubseteq V(G)$, then $|\{g'(w_i)|i = 1, \ldots, 2l\}\backslash\{0, 1\}| \geq l$. When we try to assign $(u_0)^*_g = u_1$ and $(u_1)^*_g = u_0$, the labeling $g = g'|_{IN(G)}$ will not be a core cluster of G only when any of the following three situations occurs. Situation $(T1) : N_G(u_1) \cap V_0 \neq \emptyset$ or $N_G(u_1) \cap (V_0)^*_{g'} \neq \emptyset$; Situation $(T2) : N_G(u_0) \cap V_1 \neq \emptyset$ or $N_G(u_0) \cap (V_1)^*_{g'} \neq \emptyset$; and the Situation (S^*).

Subcase 2-1. Suppose that both Situation $(T1)$ and $(T2)$ do not occur and $t > 0$, then either $r = t = 1$ or $r > 1$ and $r \geq t + 1$. We redefine $g(V_{a_i}^{[0]}) = c_i$, for all $i = 1, \ldots, t$, and assign $(u_0)^*_g = u_1$ and $(u_1)^*_g = u_0$. The resulting labeling g is obviously a core cluster with $|g(IN(G))| \leq |g'(IN(G'))| - l + t$.

Subcase 2-2. Suppose that Situation $(T1)$ occurs and $(T2)$ does not, then either $t = 0$ and $r \geq 1$ or $t > 0$ and $r \geq t + 2$. Now, let x_1 be a vertex in $N_G(u_1) \cap V_0$ if $N_G(u_1) \cap V_0 \neq \emptyset$, and x_1 be a vertex in V_0 such that $(x_1)^*_{g'} \in N_G(u_1)$ otherwise. Choose a vertex $z_0 \in N_G(u_0)$ which is on a u_0x_1-path whose vertices are in V_0, and then consider $\mathrm{Split}(V_0; \{u_0\}, \{z_0\}) = (V_0^{[0]}, V_0^{[1]})$. After redefining $g(V_0^{[0]}) = \{c_0\}$ and assigning $(u_0)^*_g = z_0$ and $(u_1)^*_g = u_0$, one can easily verify that $V_0^{[0]} = g^{-1}(c_0)$ is a core. If $t > 0$, we further redefine $g(V_{a_i}^{[0]}) = \{c_i\}$ for all $i = 1, 2, \ldots, t$. Then the labeling g is a core cluster of

G with $|g(IN(G))| \leq |g'(IN(G'))| - l + t + 1$.

Subcase 2-3. Suppose that both Situation $(T1)$ and $(T2)$ occur, then $r \geq t + 3$. Using the manner we chose z_0 in the previous subcase, we select $z_1 \in N_G(u_1)$ such that z_1 is on a path with vertices in V_1 connecting u_1 to a vertex x_0 where $x_0 \in N_G(u_0) \cap V_1$ if $N_G(u_0) \cap V_1 \neq \emptyset$, and $x_0 \in V_1$ such that $(x_0)^*_{g'} \in N_G(u_0)$ if $N_G(u_0) \cap V_1 = \emptyset$. Consider $\text{Split}(V_0; \{u_0\}, \{z_0\}) = (V_0^{[0]}, V_0^{[1]})$ and $\text{Split}(V_1; \{u_1\}, \{z_1\}) = (V_1^{[0]}, V_1^{[1]})$. By redefining $g(V_0^{[0]}) = \{d_0\}$ and $g(V_1^{[0]}) = \{d_1\}$ and assigning $(u_i)^*_g = z_i$, $i = 0, 1$, $g^{-1}(d_0) = V_0^{[0]}$ and $g^{-1}(d_1) = V_1^{[0]}$ are both cores of G. If $t > 0$, we further redefine $g(V_{a_i}^{[0]}) = \{c_i\}$ for all $i = 1, \ldots, t$. Then the core cluster g of G has $|g(IN(G))| \leq |g'(IN(G'))| - l + t + 2$. □

Proposition 1, Lemma 1 and Lemma 2 jointly guarantee the following lemma.

Lemma 3. *Let G' be a graph obtained by $(2l+1)$-subdividing a nonpendant edge e of a simple graph G with $\text{girth}(G) \geq 6$, where $l \geq 3$. If $c^*(G') - d^*(G') = k$, then $c^*(G) - d^*(G) \leq k + r$ provided that e is an edge of type r.*

This lemma gives rise to a bound on $AR(G)$. Let E' be a set of edges of G. If 7-subdividing each edge in E' results in a feasible graph, then E' is called a *feasiblizer* of G. The minimum cardinality of all feasiblizers of G is denoted as $\phi(G)$, called the *feasiblizing number* of G. Let $\Delta(G)$ be the maximum degree of G. If an edge u_0u_1 of G is of type r, then $r \leq \min\{\deg_G(u_0), \deg_G(u_1)\} \leq \Delta(G)$.

Theorem 7. *Let $G = (X, Y)$ with $|X| \geq |Y|$ and $\text{girth}(G) \geq 6$. If E' is a feasiblizer of G in which there are α_r type-r edges and $\alpha = \sum_{r=1}^{\Delta(G)} r\alpha_r$, then $c^*(G) - d^*(G) \leq \alpha$ and $\frac{|V(G)|+in(G)-(\beta(G)+\alpha)}{|V(G)|} \leq AR(G) \leq \frac{|V(G)|+in(G)-\beta(G)}{|V(G)|}$.*

The feasiblizing number is analogous to the decycling number of G. One major difference lies in that we only deal with unfeasible cycles instead of all cycles in G. More importantly, we choose edges as opposed to vertices to destroy unfeasible cycles. This gives a lot more freedom on the choices of edges in a feasiblizer. It should be clarified that choosing common edges of cycles does not necessarily lessen the number of edges needed to feasiblize a graph. For instance, let G be a 16-cycle $(w_0w_1 \cdots w_{15})$ with a chord w_0w_7, then $\phi(G) = 2$ and both edges in a minimum feasiblizer can be chosen to be of type 1. Choosing the common edge w_0w_7 of two cycles does not result in a feasiblizer with lesser edges. For a graph which has a feasiblizer consisting of type-1 edges, the bound of Theorem 7 can be very good.

Corollary 3. *Let $G = (X, Y)$ with $|X| \geq |Y|$ and $\text{girth}(G) \geq 6$. If E' is a feasiblizer consisting of type-1 edges with $|E'| = \phi(G)$, then $c^*(G) - d^*(G) \leq \phi(G)$ and $\frac{|V(G)|+in(G)-(\beta(G)+\phi(G))}{|V(G)|} \leq AR(G) \leq \frac{|V(G)|+in(G)-\beta(G)}{|V(G)|}$.*

This bound is best possible using our $c^*(G)$-and-$d^*(G)$ approach. We show this fact by proposing an infinite class of graphs attaining this bound. Consider the class of connected graphs with the pattern given in Figure 1. The one with k cycles is denoted as $G(k)$. For each $k \in \mathbb{N}$, $\phi(G(k)) = k$ is obviously true. By direct calculation, one can verify that the labeling giving all vertices of the i-th cycle the label i, for all $i = 1, \ldots, k$, is an optimal core cluster, hence $c^*(G(k)) = k$. On the other hand, the covering given in Theorem 5 is an optimal star covering of $G(k)$ and then $d^*(G(k)) = 0$. Therefore, the bound $c^*(G) - d^*(G) \leq \phi(G)$ is attained by each $G(k)$. For the classes of bipartite graphs described in this corollary, our bound on $AR(G)$ is the best possible using our approach.

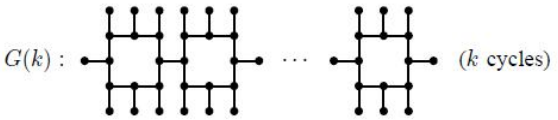

Fig. 1. The family $G(k)$ of bipartite graphs.

IV. Conclusion

In this paper, we have investigated the gap between $c^*(G)$ and $d^*(G)$ for any bipartite graph of girth at least six. and have derived a bound on $c^*(G) - d^*(G)$, which naturally gives rise to a bound on the optimal average information ratio of G. We have also shown that our bound is the best possible using our approach for some infinite classes of graphs. To determine the exact values of the optimal average information ratio for them, new technique must be imposed. Furthermore, the feasiblizing number $\phi(G)$ has not been characterized yet. Having a close examination of the value of $\phi(G)$ will be an interesting problem to consider.

Acknowledgment

This work is supported in part by the National Science Council of Taiwan under Grants NSC 102-2115-M-239-002.

References

[1] G. R. Blakley, "Safeguarding cryptographic keys", in: *Amer. Fed. Inf. Process. Soc. Proc.* 1979, vol.48, pp.313–317.
[2] C. Blundo, A. De Santis, R. De Simone and U. Vaccaro, "Tight bounds on the information rate of secret sharing schemes", *Des. Codes Cryptogr.*, vol.11, pp.107–122, 1997
[3] C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, "On the information rate of secret sharing schemes", *Theor. Comp. Soc.*, vol. 154, pp.283–306, 1996.
[4] C. Blundo, A. De Santis, A. Giorgio Gaggian and U. Vaccaro, "New bounds on the information rate of secret sharing schemes", *IEEE Trans. Inf. Theory*, vol.41, pp.549–554, 1995.
[5] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, "Graph decompositions and secret sharing schemes", *J. Cryptol.*, vol.8, pp.39–64, 1995.
[6] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes", *J. Cryptol.*, vol.4, pp.123–134, 1991.
[7] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes", *J. Cryptol.*, vol.5, pp.153–166, 1992.
[8] L. Csirmaz, "The size of a share must be large", *J. Cryptol.*, vol.10, pp.223-231, 1997.
[9] L. Csirmaz, "An impossibility result on graph secret sharing", *Des. Codes Cryptogr.*, vol.53, pp.195–209, 2009.
[10] L. Csirmaz, "Secret sharing schemes on graphs", *Studia Mathematica Hungarica*, vol.10, pp.297–306, 1997.

[11] L. Csirmaz and P. Ligeti, "On an infinite families of graphs with information ratio $2 - 1/k$", *Computing*, vol.85, pp.127–136, 2009.
[12] L. Csirmaz and G. Tardos, "Exact bounds on tree based secret sharing schemes", *Tatracrypt* 2007, Slovakia.
[13] I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.
[14] M. van Dijk, "On the information rate of perfect secret sharing schemes", *Des. Codes Cryptogr.*, vol.6, pp.143–169, 1995.
[15] W.-A. Jackson and K. M. Martin, "Perfect secret sharing schemes on five participants", *Des. Codes Cryptogr.*, vol.9, pp.267–286, 1996.
[16] H-C Lu and H-L Fu, "The exact values of the average information ratio of perfect secret-sharing schemes for tree-based access structures", *Des. Codes Cryptogr.* DOI 10.1007/s10623-012-9792-1.
[17] H-C Lu and H-L Fu, "The average informaion ratio of perfect secret-sharing schemes for access structures based on sparse bipartite graphs", submitted.
[18] A. Shamir, "How to share a secret", Commun. ACM, vol.22, pp.612–613, 1979.
[19] D. R. Stinson, "An explication of secret sharing schemes", *Des. Codes Cryptogr.*, vol.2, pp.357–390, 1992.
[20] D. R. Stinson, "New general lower bounds on the information rate of perfect secret sharing schemes", in *Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science*, 1993, vol.740, pp.168–182.
[21] D. R. Stinson, "Decomposition constructions for secret sharing schemes", *IEEE Trans. Inf. Theory*, vol.40, pp.118–125, 1994.
[22] D. B. West, *Introduction to graph Theory*, Prentice Hall, 2001.