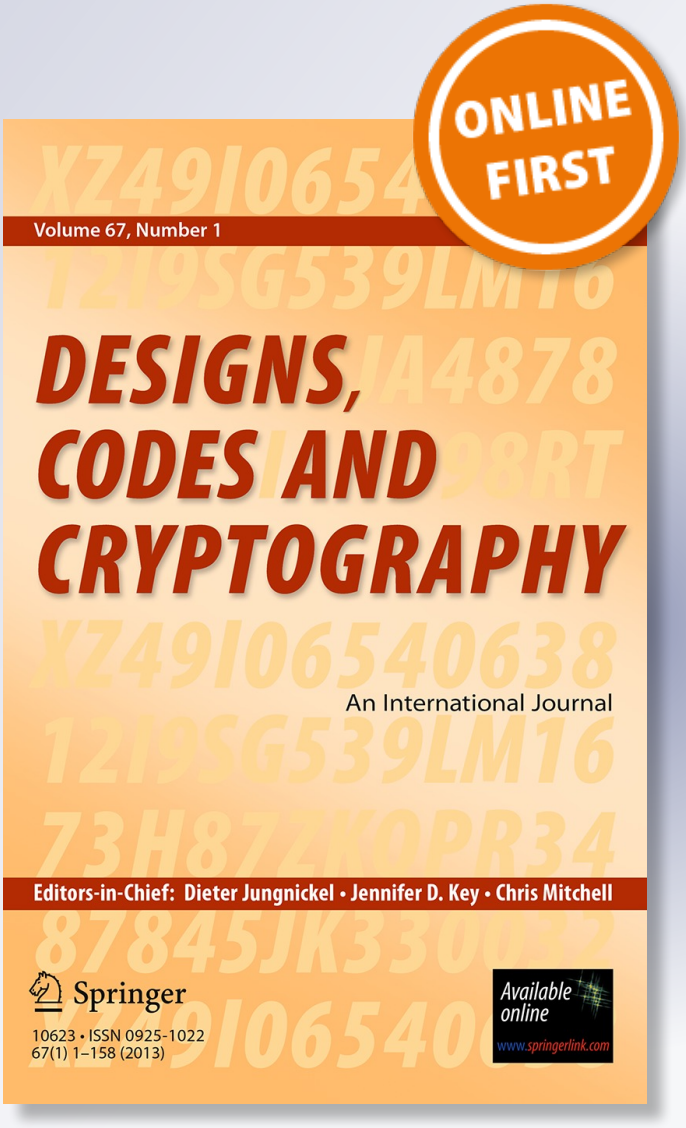
The exact values of the optimal average information ratio of perfect secret-sharing schemes for tree-based access structures

Hui-Chuan Lu & Hung-Lin Fu

Designs, Codes and Cryptography
An International Journal

ISSN 0925-1022

Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9792-1



Springer

Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9792-1

The exact values of the optimal average information ratio of perfect secret-sharing schemes for tree-based access structures

Hui-Chuan Lu · Hung-Lin Fu

Received: 10 February 2012 / Revised: 15 December 2012 / Accepted: 18 December 2012

Abstract A perfect secret-sharing scheme is a method of distributing a secret among a set of participants such that only qualified subsets of participants can recover the secret and the joint shares of the participants in any unqualified subset is statistically independent of the secret. The set of all qualified subsets is called the access structure of the 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 information ratio of a perfect secret-sharing scheme is defined as the ratio between the maximum length of the share given to a participant and the length of the secret. The average information ratio is the ratio between the average length of the shares given to the participants and the length of the secret. The infimum of the (average) information ratios of all possible perfect secret-sharing schemes realizing a given access structure is called the (average) information ratio of the access structure. Very few exact values of the (average) information ratio of infinite families of access structures are known. Csirmaz and Tardos have found the information ratio of all trees. Based on their method, we develop our approach to determining the exact values of the average information ratio of access structures based on trees.

Keywords Secret-sharing scheme · Graph-based access structure · Average information ratio · Entropy · Star covering · Tree

Mathematics Subject Classification (2000) 05C70 · 94A60 · 94A62 · 94A17

Communicated by C. Blundo.

H.-C. Lu (✉)
Center for Basic Required Courses, National United University, Miaoli36003, Taiwan
e-mail: hjlu@nuu.edu.tw; hht0936@seed.net.tw

H.-C. Lu · H.-L. Fu
Department of Applied Mathematics, National Chaio Tung University, Hsinchu30010, Taiwan

Published online: 07 March 2013

1 Introduction

A *secret-sharing scheme* is a method of distributing a secret among a set of participants in such a way that only qualified subsets of participants can recover the secret from the shares they receive. If, in addition, the joint shares of the participants in any unqualified subset is statistically independent of the secret, then the secret-sharing scheme is called *perfect*. Since all secret-sharing schemes considered in this paper are perfect, we will simply use "secret-sharing scheme" for "perfect secret-sharing scheme". The *access structure* of a secret-sharing scheme is the collection of all qualified subsets in this scheme. It is required to be *monotone* which means any subset of participants containing a qualified subset must also be qualified.

There are two major tools for measuring the efficiency of a secret-sharing scheme, namely, the *information ratio* and the *average information ratio*. The information ratio of a secret-sharing scheme is the ratio between the maximum length (in bits) of the share given to a participant and the length of the secret. The average information ratio of a secret-sharing scheme is the ratio between the average length of the shares given to the participants and the length of the secret. These ratios represent the maximum and average number of bits of information the participants must remember for each bit of the secret. The lower the ratios are, the lower storage and communication complexity the scheme has. Therefore, for a given access structure, constructing a secret-sharing scheme with the lowest above-mentioned ratios is one of the main goals of the research. The infimum of the (average) information ratios of all possible secret-sharing schemes realizing a access structure is referred to as the (average) information ratio of that access structure.

In 1979, Shamir [8] and Blakley [2] independently introduced the first kind of secret-sharing schemes called the (t, n)-threshold schemes in which the minimal qualified subsets are the t-subsets of the set of participants of size n. Related problems have then received considerable attention. Secret-sharing schemes for various access structures and many modified versions of secret-sharing schemes with additional capacities were widely studied. The reader is referred to [1,7] and their references for recent developments on secret-sharing problems.

In the present paper, we only consider graph-based access structures. In such a structure, each vertex of a graph G represents a participant and each edge 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 ξ_s and ξ_v for $v \in V(G)$ with a joint distribution such that

(i) ξ_s is the secret and ξ_v is the share of v;
(ii) if $uv \in E(G)$, then ξ_u and ξ_v together determine the value of ξ_s; and
(iii) if $A \subseteq V(G)$ is an independent set, then ξ_s and the collection $\{\xi_v | v \in A\}$ 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

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i),$$

which is a measure of the average uncertainty associated with the random variable X. It is well known that $H(X)$ is a good approximation to the average number of bits needed to represent the elements in X faithfully. Using Shannon entropy, the information ratio of the secret-sharing scheme Σ can be defined as $R_\Sigma = \max_{v \in V(G)}\{H(\xi_v)/H(\xi_s)\}$ and the average information ratio as $AR_\Sigma = \sum_{v \in V(G)} H(\xi_v)/(|V(G)|H(\xi_s))$. For convenience, we use "a secret-sharing scheme on G" for "a secret-sharing scheme for the

access structure based on G". Also, "the information ratio (resp. the average information ratio) of the access structure based on G" is referred to as "the information ratio (resp. the average information ratio) of G", denoted as $R(G)$ (resp. $AR(G)$). As mentioned above, $R(G) = \inf\{R_\Sigma | \Sigma \text{ is a secret-sharing scheme on } G\}$ and $AR(G) = \inf\{AR_\Sigma | \Sigma \text{ is a secret-sharing scheme on } G\}$. It is well known that $R(G) \geq AR(G) \geq 1$ and that $R(G) = 1$ iff $AR(G) = 1$. A secret-sharing scheme Σ with $R_\Sigma = 1$ or $AR_\Sigma = 1$ is then called an *ideal* secret-sharing scheme. An access structure is ideal if there exists an ideal secret-sharing scheme on it. Determining the exact value of $R(G)$ or $AR(G)$ is extremely challenging. It is not easy even for small graphs sometimes. Due to the difficulty, most known results give bounds on $R(G)$ and $AR(G)$. Stinson [10] has shown the important bounds for general graphs: $R(G) \leq \frac{d+1}{2}$ where d is the maximum degree of G and $AR(G) \leq \frac{2m+n}{2n}$ where $n = |V(G)|$ and $m = |E(G)|$. The exact values of $R(G)$ and $AR(G)$ are obtained only for very few specific graphs. Most graphs of order no more than five, and the cycles and paths have known exact values of the average information ratio [3,10]. Most graphs of order no more than six, and the cycles, paths and trees have known exact values of the information ratio [3,6,9–11]. The information ratio of a tree T was determined by Csirmaz and Tardos [6] as $R(T) = 2 - \frac{1}{k}$ where k is the maximum size of a core in T. Based on their method, we develop our approach to the problem of determining the value of $AR(T)$ for any tree T.

This paper is organized as follows. In Sect. 2, some basic known results and definitions are introduced. Our results are presented in Sects. 3, 4 and 5. We derive a lower bound on $AR(T)$ and introduce our approach in Sect. 3. Our main results are shown in Sect. 4. Subsequently, in Sect. 5, two examples are given to demonstrate our systematic way of evaluating $AR(T)$. A concluding remark will be given in the final section.

2 Preliminaries

We introduce some basic known results on graph-based access structures first. The ideal graph-based access structures have been completely characterized by Brickell and Davenport.

Theorem 1 ([4]) *Suppose that G is a connected graph. Then $R(G) = 1$ if and only if G is a complete multipartite graph.*

We introduce the methods of deriving upper bounds and lower bounds on $AR(G)$ for a non-ideal access structure G in what follows. By constructing a secret-sharing scheme Σ on graph G, one can obtain an upper bound AR_Σ on the average information ratio $AR(G)$. Stinson's decomposition construction [10] has been a major tool to do this job. This method enables us to build up secret-sharing schemes for graphs using *complete multipartite coverings*. 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 belongs to at least one subgraph in the collection. The value $\sum_{i=1}^{l} |V(G_i)|$ is crucial for our discussion, we call it the *vertex-number sum of Π*.

Theorem 2 ([10]) *Suppose that $\{G_1, G_2, \ldots, G_l\}$ is a complete multipartite covering of a graph G with $V(G) = \{1, 2, \ldots, n\}$. Let $R_i = |\{j | i \in V(G_j)\}|$ and $R = \max_{1 \leq i \leq n} R_i$. Then there exists a secret-sharing scheme Σ on G with information ratio R_Σ and average information ratio AR_Σ where*

$$R_\Sigma = R \text{ and } AR_\Sigma = \frac{1}{n}\sum_{i=1}^{n} R_i = \frac{1}{n}\sum_{i=1}^{l} |V(G_i)|.$$

The only main tool for establishing lower bounds on $AR(G)$ is the information theoretic approach [5]. Let Σ be a secret-sharing scheme in which ξ_s is the random variable of the secret and each ξ_v is the one of the share of v, $v \in V(G)$. Define a real-valued function f as $f(A) = H(\{\xi_v : v \in A\})/H(\xi_s)$ for each subset $A \subseteq V(G)$, where H is the Shannon entropy. Then, $AR_\Sigma = \frac{1}{n}\sum_{v\in V(G)} f(v)$, where $n = |V(G)|$. Using properties of the entropy function and the definition of a secret-sharing scheme, one can show that f satisfies the following inequalities [5]:

(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 unqualified set and B is not, then $f(A) + 1 \leq f(B)$; and
(e) if neither A nor B is unqualified but $A \cap B$ is, then $f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$.

Csirmaz and Tardos [6] defined a *core* V_0 of a tree T as a subset V_0 of $V(T)$ such that V_0 induces a connected subgraph of T and each vertex in V_0 has a neighbor outside it. They also showed the following theorem.

Theorem 3 ([6]) *Let V_0 be a core of a tree T. If f is defined as above, then $\sum_{v\in V_0} f(v) \geq 2|V_0| - 1$.*

In the next section, we shall derive a lower bound on $AR(T)$ and rewrite Theorem 2 as an upper bound on $AR(T)$ of particular form. Our approach can then be introduced.

3 Lower bound and upper bound on $AR(T)$

Given a tree T, we let $IN(T)$ and $LF(T)$ be the sets of all internal vertices and leaves of T respectively. Denote $|IN(T)|$ as $in(T)$ and $|LF(T)|$ as $lf(T)$. In order to cope with the average information ratio, we extend the idea of a core of T. For $T \neq K_{1,1}$, we define a *core cluster of T of size k* as a partition $\mathcal{C} = \{V_1, V_2, \ldots, V_k\}$ of $IN(T)$ such that each V_i, $i \in \{1, 2, \ldots, k\}$, is a core of T. The size of a core cluster $\mathcal{C}$ is written as $c_\mathcal{C}$. We also denote the minimum size of all core clusters of T as $c^*(T)$, called the *core number* of T. Note that $\bigcup_{i=1}^{k} V_i$ may not be a core of T, if so, then $c^*(T) = 1$ for $T \neq K_{1,1}$. In addition, we naturally define that $c^*(K_{1,1}) = 0$.

The idea of a core cluster helps us establish a lower bound on $AR(T)$.

Theorem 4 *If $T \neq K_{1,1}$ is a tree of order n, then $AR(T) \geq \frac{n+in(T)-c^*(T)}{n}$.*

Proof Suppose that Σ is a secret-sharing scheme on T. Then the function f defined in Sect. 2 by the random variables from Σ satisfies all the properties (a) to (e) and Theorem 3. Let $\mathcal{C} = \{V_1, V_2, \ldots, V_k\}$ be a core cluster of T. By Theorem 3 and the definition of a core cluster, $\sum_{v\in IN(T)} f(v) = \sum_{i=1}^{k}\sum_{v\in V_i} f(v) \geq \sum_{i=1}^{k}(2|V_i| - 1) = 2in(T) - k$. Since T is connected, $f(v) \geq 1$ for all $v \in V(T)$ [5]. $\sum_{v\in V(T)} f(v) = \sum_{v\in IN(T)} f(v) + \sum_{v\in LF(T)} f(v) \geq 2in(T) - k + lf(T) = n + in(T) - k$. Thus we have $AR_\Sigma \geq \frac{1}{n}(n + in(T) - k)$. Since the result holds for any secret-sharing scheme on T, we have $AR(T) \geq \frac{1}{n}(n + in(T) - c^*(T))$. □

On the other hand, as suggested in Theorem 2, in order to construct a secret-sharing scheme with lower average information ratio, we need a complete multipartite covering with the least vertex-number sum. Since we are dealing with trees, and stars are the only complete

multipartite trees, star coverings with the least vertex-number sum are what we are aiming for. For a better description of our approach, given a star covering Π of T with vertex-number sum m, we define the *deduction of* Π, written d_Π, as $d_\Pi = |V(T)| + in(T) - m$. A star covering with the largest deduction gives the least vertex-number sum. The largest value of the deductions over all star coverings of T is called the *deduction of* T and is denoted as $d^*(T)$. The following corollary is simply a rephrasement of Theorem 2 in terms of the deduction of T.

Corollary 5 ([10]) *Let Π be a star covering of a tree T of order n, then*

$$AR(T) \leq \frac{n + in(T) - d^*(T)}{n}.$$

Combining Theorem 4 and Corollary 5, we have the following results.

Theorem 6 *For any star covering Π of T and any core cluster $\mathcal{C}$ of T, $c_\mathcal{C} \geq d_\Pi$. In particular, $c^*(T) \geq d^*(T)$.*

Corollary 7 *If there exists a star covering Π of T and a core cluster $\mathcal{C}$ of T such that $d_\Pi = c_\mathcal{C}$, then $d^*(T) = d_\Pi = c_\mathcal{C} = c^*(T)$.*

As indicated in these results, $c^*(T) = d^*(T)$ makes a criterion for examining whether the upper bound and the lower bound on $AR(T)$ will match. In the next section, we will show that this equality holds for all trees.

4 The main results

Blundo et al. [3] gave an algorithm for producing a star covering of a tree T. We make a slight modification to it and restate it for completeness. Let $N_T(v)$ be the set of all neighbors of v in T and S_v be the star centered at v with $N_T(v)$ as its leaf set.

Algorithm;	
Covering(T)	**Cover**(v)
Let $v \in IN(T)$	$A(v) \leftarrow N_T(v) \cap IN(T)$
$\Pi \leftarrow \phi$	$\Pi \leftarrow \Pi \cup \{S_v\}$
Cover(v)	$E(T) \leftarrow E(T) \backslash E(S_v)$
Output the star covering Π	$V(T) \leftarrow V(T) \backslash ((N_T(v) \cap LF(T)) \cup \{v\})$
	for all $v' \in A(v)$ do Cover(v')

Lemma 8 *Let T be a tree. The star covering Π of T produced by* Covering(T) *has deduction $d_\Pi = 1$ if $T \neq K_{1,1}$ and $d_\Pi = 0$ if $T = K_{1,1}$.*

Proof For $T \neq K_{1,1}$, the initial vertex v and all leaves of T appear in exactly one star in Π. All internal vertices but the initial one appear twice in the covering. So the vertex-number sum $m = lf(T) + 1 + 2(in(T) - 1) = |V(T)| + in(T) - 1$, and we have $d_\Pi = 1$. □

We shall refine this process and obtain star coverings with higher deductions next.

A vertex $v \in IN(T)$ is called a *critical vertex* of T if $N_T(v) \cap LF(T) = \emptyset$. In the structure of a tree T, critical vertices play an important role in our discussion. We use X_T to denote the set of all critical vertices of T. Let K_T be the subgraph induced by X_T and Λ_T (resp. Y_T) be the set of all nontrivial (resp. trivial) components in K_T. The set Y_T is in fact the set of all isolated vertices in K_T. Therefore, Y_T can been seen as a subset of X_T. For any $V' \subseteq V(T)$

and $E' \subseteq E(T)$, the graph $T\backslash V'$ is obtained by removing from T all vertices in V' as well as all edges incident to them. $T\backslash E'$ is resulted from removing all edges in E' from T. Both $T\backslash V'$ and $T\backslash E'$ may contain isolated vertices.

Proposition 9 *Let $T \neq K_{1,1}$ be a tree. If $\Lambda_T = \emptyset$ and $|Y_T| = y \geq 0$, then there exists a star covering Π of T with deduction $d_\Pi = y + 1$.*

Proof Let G be an arbitrary component in $T\backslash Y_T$. If $w_1, \ldots, w_l$ are all of the vertices in Y_T that are adjacent to some vertices in G, then we define $\tilde{G}$ as the subgraph of T induced by $V(G) \cup \{w_1, \ldots, w_l\}$. Let $\mathbb{H} = \{\tilde{G} | G \text{ is a component in } T\backslash Y_T\}$ and $\Pi_{\tilde{G}}$ be the star covering produced by algorithm Covering($\tilde{G}$). By the definition of Y_T, no $\tilde{G}$ is isomorphic to $K_{1,1}$, so $d_{\Pi_{\tilde{G}}} = 1$ by Lemma 8. Since $\bigcup_{\tilde{G}\in\mathbb{H}} E(\tilde{G}) = E(T)$, the covering $\Pi = \bigcup_{\tilde{G}\in\mathbb{H}} \Pi_{\tilde{G}}$ is a star covering of T with vertex-number sum

$$\begin{aligned} m &= \sum_{\tilde{G}\in\mathbb{H}} (|V(\tilde{G})| + in(\tilde{G}) - 1) \\ &= \left(V(T) + \sum_{v\in Y_T} (\deg_T(v) - 1) \right) + (in(T) - y) \\ &\quad - \left(\sum_{v\in Y_T} \deg_T(v) - (y-1) \right) \\ &= V(T) + in(T) - (y+1). \end{aligned}$$

□

Next, we consider the core number of T. For a tree T with $X_T = \emptyset$, $\{IN(T)\}$ is obviously a core cluster of minimum size. The following lemma is straight forward.

Lemma 10 *Let $T \neq K_{1,1}$ be a tree. If $X_T = \emptyset$, then $c^*(T) = 1$.*

Now, we introduce the way we decompose a tree in order to define a core cluster we need. Let $V' \subseteq V(T)$. Given a vertex $\bar{v} \in N_T(v) \cap IN(T)$ for each $v \in V'$, we set $E' = \{v\bar{v} | v \in V'\}$. For each component G in $T\backslash E'$, let G^+ be the subtree of T obtained by attaching to G all edges of the form $v\bar{v}$ if $\bar{v} \in V(G)$, then $G^+ = G$ if G does not contain any $\bar{v}$. We also denote the collection of all G^+'s, where G is a component in $T\backslash E'$, as $\mathbb{H}^+(T, V', E')$. Observe that, if $\deg_T(v) = 2$, then $v \in LF(G^+)$ for exactly two G^+'s in the collection $\mathbb{H}^+(T, V', E')$.

Proposition 11 *Let $T \neq K_{1,1}$ be a tree. If $\Lambda_T = \emptyset$ and $|Y_T| = y \geq 0$, then $c^*(T) = d^*(T) = y + 1$.*

Proof It suffices to show that there is a core cluster of T of size $y + 1$. For each $v \in Y_T$, choose an arbitrary neighbor of v as $\bar{v}$, then $\bar{v} \in IN(T)$. Let $E' = \{v\bar{v} | v \in Y_T\}$. There are $y + 1$ subgraphs in $\mathbb{H}^+(T, Y_T, E')$. Let $\mathbb{H}^+(T, Y_T, E') = \{G_0^+, G_1^+, \ldots, G_y^+\}$ where G_i's, $i = 0, 1, \ldots, y$ are the components in $T\backslash E'$. Note that any two vertices in Y_T have distance at least two, so $IN(G_i^+) \neq \emptyset$. Let $V_i = IN(G_i^+) \cup \{v | v \in V(G_i) \cap Y_T \text{ and } \deg_T(v) = 2\}$. We claim that $\{V_0, V_1, \ldots, V_y\}$ is a core cluster of T. First, each vertex $u \in IN(T)\backslash Y_T$ belongs to exactly one $IN(G_i^+)$ and also exactly one V_i. Each $v \in Y_T$ belongs to exactly two G_i^+'s. If $\deg_T(v) \geq 3$, then v is an internal vertex of one G_i^+ and a leaf of the other.

It belongs to exactly one $IN(G_i^+)$ and hence exactly one V_i. If $\deg_T(v) = 2$, then v is a leaf of exactly one component G_i in $T \backslash E'$ and is a leaf of two subgraphs in $\mathbb{H}^+(T, Y_T, E')$. Hence it belongs to exactly one V_i and none of $IN(G_j^+)$'s, $j = 0, 1, \ldots, y$. This shows that $\{V_0, V_1, \ldots, V_y\}$ is a partition of $IN(T)$. Next, each V_i certainly induces a connected subgraph of T. In addition, each $v \in V_i \cap Y_T$ has a neighbor $\bar{v}$ not in V_i. Each $u \in V_i \backslash Y_T$ has a leaf neighbor in T which does not belongs to V_i. Hence, V_i is a core of T. Since we have a core cluster of size $y + 1$, the result then follows immediately by Proposition 9 and Corollary 7. □

Before literally proving our main theorem, we examine the relation between the deductions of star coverings of subtrees in $\mathbb{H}^+(T, V', E')$ and the deduction of a star covering of T more closely.

Lemma 12 *Let V' be an independent subset of $IN(T)$ and $z = |\{v \in V' | \deg_T(v) \geq 3\}|$. For each $v \in V'$, let $\bar{v}$ be a nonleaf neighbor of v in T and $E' = \{v\bar{v} | v \in V'\}$. If there is a star covering $\Pi_{T'}$ of each $T' \in \mathbb{H}^+(T, V', E')$ with deduction $d_{\Pi_{T'}}$, then $\Pi = \bigcup_{T' \in \mathbb{H}^+(T,V',E')} \Pi_{T'}$ is a star covering of T with deduction $d_\Pi = \sum_{T' \in \mathbb{H}^+(T,V',E')} d_{\Pi_{T'}} - z$.*

Proof Denote $\mathbb{H}^+(T, V', E')$ by $\mathbb{H}^+$ for now. Since $\bigcup_{T' \in \mathbb{H}^+} E(T') = E(T)$, Π is a star covering of T. The vertex-number sum m of Π is

$$\begin{aligned} m &= \sum_{T' \in \mathbb{H}^+} (|V(T')| + in(T') - d_{\Pi_{T'}}) \\ &= |V(T)| + |V'| + in(T) - (|V'| - z) - \sum_{T' \in \mathbb{H}^+} d_{\Pi_{T'}} \\ &= |V(T)| + in(T) - \left(\sum_{T' \in \mathbb{H}^+} d_{\Pi_{T'}} - z \right). \end{aligned}$$

□

Now, we are in a position to present our main theorem.

Theorem 13 *Let T be a tree of order n, then $c^*(T) = d^*(T)$ and*

$$AR(T) = \frac{n + in(T) - c^*(T)}{n}.$$

Proof We prove this result by induction on $|X_T|$.

(1) If $|X_T| = 0$ or 1, then $\Lambda_T = \emptyset$. The result holds by Proposition 11.
(2) Suppose that $|X_T| \geq 2$. By Proposition 11, we may assume that $\Lambda_T \neq \emptyset$.

Choose a vertex $v \in LF(T')$ for some $T' \in \Lambda_T$ and let $\bar{v}$ be the neighbor of v in T'. There are two subtrees G_0^+ and G_1^+ in $\mathbb{H}^+(T, \{v\}, \{v\bar{v}\})$, each of which is not a $K_{1,1}$. Let G_0^+ be the one not containing $\bar{v}$, then $|X_{G_0^+}| < |X_T|$ is obviously true. Since $v \in LF(G_1^+)$, it is no longer a critical vertex of G_1^+, we also have $|X_{G_1^+}| < |X_T|$. By induction hypothesis, there exist a star covering Π_i of G_i^+ and a core cluster $\mathcal{C}_i = \{V_{i1}, V_{i2}, \ldots, V_{ik_i}\}$ with $d_{\Pi_i} = c_{\mathcal{C}_i} = k_i > 0$, $i = 0, 1$. Then $\Pi = \Pi_0 \cup \Pi_1$ is a star covering of T. We construct a core cluster of size d_Π next.

(i) If $\deg_T(v) \geq 3$, then $d_\Pi = k_0 + k_1 - 1$ by Lemma 12. Suppose that $v \in V_{01}$. Since V_{01} is a core of G_0^+, there is a neighbor v' of v in G_0^+ and $v' \notin V_{01}$. v' is an internal vertex

of G_0^+ because v is critical both in T and in G_0^+. We may assume that $v' \in V_{02}$. Now, let $\mathcal{C} = \{V_{01} \cup V_{02}, V_{03}, \ldots, V_{0k_0}, V_{11}, \ldots, V_{1k_1}\}$, then $|\mathcal{C}| = k_0 + k_1 - 1$. We claim that $\mathcal{C}$ is a core cluster of T. First note that $IN(G_0^+) \cup IN(G_1^+) = IN(T)$ and any two sets in $\mathcal{C}$ are disjoint. Each set in $\mathcal{C}\backslash\{V_{01} \cup V_{02}\}$ is a core of G_0^+ or G_1^+, hence a core of T. For $V_{01} \cup V_{02}$, $\bar{v}$ is a neighbor of v in T not in $V_{01} \cup V_{02}$. Since $v \in LF(T')$, v' is not critical and then has a leaf neighbor $v'' \neq v$ in G_0^+ (and in T) not in V_{02}, so $v'' \notin V_{01} \cup V_{02}$ and $V_{01} \cup V_{02}$ is qualified as a core of T. Therefore, $\mathcal{C}$ is a core cluster of T of size d_{Π}.

(ii) If $\deg_T(v) = 2$, then $d_{\Pi} = k_0 + k_1$ by Lemma 12. Since v is a critical vertex of T, the neighbor $v' \neq \bar{v}$ in T is an internal vertex of G_0^+. We may assume that $v' \in V_{01}$. Let $\mathcal{C} = \{V_{01} \cup \{v\}, V_{02}, \ldots, V_{0k_0}, V_{11}, \ldots, V_{1k_1}\}$, then $|\mathcal{C}| = k_0 + k_1$. To show that $\mathcal{C}$ is a core cluster of T, it suffices to show that $V_{01} \cup \{v\}$ is a core of T. Note that v' is not critical in both G_0^+ and T. It has a leaf neighbor $v'' \neq v$ not in $V_{01} \cup \{v\}$. Besides, $\bar{v}$ is a neighbor of v in T not in $V_{01} \cup \{v\}$. $V_{01} \cup \{v\}$ is then a core of T. Therefore, T also has a core cluster of size d_{Π} in this case.

In both cases, we have $c^*(T) = d^*(T)$, which implies that the lower bound and the upper bound of $AR(T)$ coincide. Hence, $AR(T) = \frac{n+in(T)-c^*(T)}{n}$. □

5 Some examples

In this section, we evaluate the average information ratio systematically for two infinite classes of trees using our approach.

The only infinite class of trees which has known average information ratio is the paths. By evaluating the core number, we can easily obtain the known result.

Proposition 14 ([10]) *Let P_n be a path of length n. Then*

$$AR(P_n) = \begin{cases} \frac{3n}{2(n+1)}, & if\ n\ is\ even;\ and \\ \frac{3n+1}{2(n+1)}, & if\ n\ is\ odd. \end{cases}$$

Proof By Proposition 11, we have $c^*(P_1) = 0$, $c^*(P_2) = c^*(P_3) = 1$ and $c^*(P_4) = 2$. Observe that $\Lambda_{P_n} = \{P_{n-4}\}$ for all $n \geq 5$. Since any leaf of the P_{n-4} in Λ_{P_n} has degree two in P_n, from the proof of Theorem 13, we have $c^*(P_n) = c^*(P_{n-4}) + 2$. Recursively, we have

$$c^*(P_n) = \begin{cases} c^*(P_i) + 2k, & \text{if } n = 4k + i,\ i = 1, 2, 3; \text{ and} \\ c^*(P_4) + 2(k-1), & \text{if } n = 4k. \end{cases}$$

$$= \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even; and} \\ \frac{n-1}{2}, & \text{if } n \text{ is odd.} \end{cases}$$

Hence,

$$AR(P_n) = \frac{(n+1) + (n-1) - c^*(P_n)}{n+1} = \begin{cases} \frac{3n}{2(n+1)}, & \text{if } n \text{ is even; and} \\ \frac{3n+1}{2(n+1)}, & \text{if } n \text{ is odd.} \end{cases}$$

□

Next, we evaluate the average information ratio of complete q-ary trees. A complete q-ary tree with k levels is a rooted tree such that each nonleaf vertex has q children and the distance from the root to each leaf is k.

Proposition 15 *Let T_k be a complete q-ary tree with k levels, $q \geq 2$. Then*

$$AR(T_k) = \begin{cases} \frac{q^{k+2}+2q^{k+1}-q^2-2q}{(q+1)(q^{k+1}-1)}, & if\ k\ is\ even;\ and \\ \frac{q^{k+2}+2q^{k+1}-q^2-q-1}{(q+1)(q^{k+1}-1)}, & if\ k\ is\ odd. \end{cases}$$

Proof By Proposition 11, $c^*(T_1) = 1$ and $c^*(T_2) = 2$. Observe that $\Lambda_{T_k} = \{T_{k-2}\}$ and the T_{k-2} has q^{k-2} leaves, each of which has degree $q + 1 \geq 3$ in T_k. Since each leaf of the T_{k-2} and its descendants in T_k compose a T_2, from the proof of Theorem 13, we get $c^*(T_k) = c^*(T_{k-2}) + q^{k-2}(c^*(T_2) - 1) = c^*(T_{k-2}) + q^{k-2}$. Recursively, the core number of T_k can be evaluated as follows.

$$\begin{aligned} c^*(T_k) &= \begin{cases} q^{k-2} + q^{k-4} + \cdots + q^2 + c^*(T_2), & \text{if } k \text{ is even; and} \\ q^{k-2} + q^{k-4} + \cdots + q + c^*(T_1), & \text{if } k \text{ is odd.} \end{cases} \\ &= \begin{cases} \frac{q^k+q^2-2}{q^2-1}, & \text{if } k \text{ is even; and} \\ \frac{q^k+q^2-q-1}{q^2-1}, & \text{if } k \text{ is odd.} \end{cases} \end{aligned}$$

Therefore,

$$\begin{aligned} AR(T_k) &= \frac{\frac{q^{k+1}-1}{q-1} + \frac{q^k-1}{q-1} - c^*(T_k)}{\frac{q^{k+1}-1}{q-1}} \\ &= \begin{cases} \frac{q^{k+2}+2q^{k+1}-q^2-2q}{(q+1)(q^{k+1}-1)}, & \text{if } k \text{ is even; and} \\ \frac{q^{k+2}+2q^{k+1}-q^2-q-1}{(q+1)(q^{k+1}-1)}, & \text{if } k \text{ is odd.} \end{cases} \end{aligned}$$

□

6 Conclusion

We have proposed the idea of the deduction $d^*(T)$ and the core number $c^*(T)$ of a tree and showed that these values are the same, thereby proving the upper bound and the lower bound of the average information ratio of a tree coincide. By doing so, we also present a systematic way of evaluating the core number of a tree. Together with the result by Csirmaz and Tardos [6], we complete the work of evaluating the information ratio and the average information ratio of all trees.

In fact, the notions of the deduction and the core number can be extended to general graphs. The condition $d^*(G) = c^*(G)$ makes a criterion for examining whether the upper bound and the lower bound on $AR(G)$, for any G, will match. The idea formulates a complicated problem of secret-sharing schemes into a problem in graph theory with easy description. "For what kind of graphs will the identity be true?" is indeed an interesting question to investigate. One obvious restriction to set on G is that G must be of larger girth. A star covering generally does not serve as a complete multipartite covering with the least vertex-number sum for a graph of small girth. We have made some progress in the study of bipartite graphs of large girth. Finding a star covering whose deduction matches the size of a core cluster is in general very difficult. However, there have not been any bounds or asymptotic results on the complexity of the problem yet.

Acknowledgments The authors would like to express their deep gratefulness to the reviewers for their detail comments and valuable suggestions which lead to great improvement in the presentation of the paper. The work of Hui-Chuan Lu was supported in part by NSC 100-2115-M-239-001 and the work of Hung-Lin Fu was supported in part by NSC 97-2115-M-009-011-MY3.

References

1. Beimel A.: Secret-sharing schemes: a survey. In: Proceedings of 3rd International Workshop Coding and Cryptology, Lecture Notes in Computer Science, vol. 6639, pp. 11–46 (2011).
2. Blakley G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, 1979. American Federation of Information Processing Societies Proceedings, vol. 48, pp. 313–317 (1979).
3. Blundo C., De Santis A., Stinson D.R., Vaccaro U.: Graph decompositions and secret sharing schemes. J. Cryptol. **8**, 39–64 (1995).
4. Brickell E.F., Davenport D.M.: On the classification of ideal secret sharing schemes. J. Cryptol. **4**, 123–134 (1991).
5. Csirmaz L.: The size of a share must be large. J. Cryptol. **10**, 223–231 (1997).
6. Csirmaz L., Tardos G.: Exact bounds on tree based secret sharing schemes. Tatracrypt, Slovakia (2007).
7. Marti-Farré J., Padró C.: On secret sharing schemes, matroids and polymatroids. J. Math. Cryptol. **4**, 95–120 (2010).
8. Shamir A.: How to share a secret. Commun. ACM **22**, 612–613 (1979).
9. Stinson D.R.: An explication of secret sharing schemes. Des. Codes Cryptogr. **2**, 357–390 (1992).
10. Stinson D.R.: Decomposition constructions for secret sharing schemes. IEEE Trans. Inform. Theory **40**, 118–125 (1994).
11. van Dijk M.: On the information rate of perfect secret sharing schemes. Des. Codes Cryptogr. **6**, 143–169 (1995).