OPTIMAL INFORMATION RATIO OF SECRET SHARING SCHEMES ON DUTCH WINDMILL GRAPHS

BAGHER BAGHERPOUR*, SHAHRROOZ JANBAZ AND ALI ZAGHIAN

Applied Mathematics and Cryptography Department
Malek Ashtar university of technology, Isfahan, Iran

(Communicated by Jens Zumbräegel)

Abstract. One of the basic problems in secret sharing is to determine the exact values of the information ratio of the access structures. This task is important from the practical point of view, since the security of any system degrades as the amount of secret information increases.

A Dutch windmill graph consists of the edge-disjoint cycles such that all of them meet in one vertex. In this paper, we determine the exact information ratio of secret sharing schemes on the Dutch windmill graphs. Furthermore, we determine the exact ratio of some related graph families.

1. Introduction

Let \( P = \{p_1, p_2, \ldots, p_n\} \) be the set of participants among which the dealer wants to share some secret \( s \) in such a way that only the qualified subsets of \( P \) can reconstruct the secret \( s \). A secret sharing scheme is called perfect if the non-qualified subsets of \( P \) can not obtain any information about the secret \( s \). \( 2^P \) denotes the set of all subsets of the set \( P \), and \( \Gamma \) is a collection of subsets of \( P \). We say that \( \Gamma \) is monotone over \( P \) if \( A \in \Gamma \) and \( A \subseteq A' \), then \( A' \in \Gamma \). In the secret sharing schemes, the access structure \( \Gamma \) over \( P \) is a collection of all qualified subsets of \( P \) that is monotone and \( \varnothing \notin \Gamma \). A qualified subset is minimal if it is not a proper subset of any qualified subset. The collection of all minimal qualified subsets is called the basis. Since \( \Gamma \) is monotone, it is fully determined by its basis. The information ratio of a secret sharing scheme is the ratio between the maximum length (in bit) of the shares given to the participants and the length of the secret.

Secret sharing scheme was introduced by Blakley and Shamir [2, 20]. Ito et al. showed that there exists a secret sharing scheme to realize any access structure \( \Gamma \) [15, 16]. Also, for arbitrary monotone access structures, Benaloh and Leichter proposed another construction to realize secret sharing schemes [1]. Perfect secret sharing schemes for graphical access structures have attracted the interest of the scientific community [7, 10, 17, 22, 24]. Stinson introduced the decomposition construction method to obtain an upper bound for the information ratio of graphical access structure [21]. Jackson and Martin in [17] have studied the information ratio of perfect secret sharing schemes on five participants. The information ratio of secret sharing schemes on graphical access structures with six vertices has been studied by Van Dijk in [24]. Sun and Chen proposed the weighted decomposition

2010 Mathematics Subject Classification: Primary: 94A60, 94A62.
Key words and phrases: Secret sharing, information ratio, access structure, Dutch windmill graphs.
* Corresponding author: Bagher Bagherpour.
construction for secret sharing schemes. Csirmaz and Tardos in [9] determined
the exact information ratio for all trees. Csirmaz and Liegti have investigated the
information ratio of an infinite family of graphs in [12].

In this paper, we firstly give some preliminaries and introduce some important
concepts. After that, our main results are introduced in details. In section 3,
we determine the exact information ratio of secret sharing schemes on the Dutch
windmill graphs. Furthermore, the information ratio of secret sharing schemes on
the cone graphs is studied and the information ratio of secret sharing schemes on
some variations of the studied graphs is determined. Finally, we propose some
research problems.

2. Preliminaries

Let \( S \) be the set of all secrets and \( p \in P \) be an arbitrary participant. The
set of all possible shares given to the participant \( p \) is denoted by \( K(p) \). A secret
sharing scheme can be seen as a distribution rule by which the dealer distributes
a secret \( s \in S \), according to some probability distribution, among the participants
in \( P \) by giving a share to each participant of \( P \). Thus, each secret sharing scheme
induces random variables on the sets \( S \) and \( K(p) \), where \( p \in P \). The Shannon
entropy of the random variable taking values in \( S \) is denoted by \( H(S) \). Also, for
each \( A = \{p_1, \ldots, p_r\} \subseteq P \), the Shannon entropy of the random variable taking
values in \( K(A) = K(p_1) \times \cdots \times K(p_r) \) is denoted by \( H(A) \) (for more details see
[3]). Let \( \Gamma \) be an access structure on the set of participants \( P \), and let \( S \) be the set
of secrets. In terms of the entropy, a secret sharing scheme \( \Sigma \) for access structure \( \Gamma \)
and the set of secrets \( S \) is called perfect secret sharing scheme if the two following
conditions hold:

1. \( \forall A \in \Gamma, \ H(S|A) = 0 \)
2. \( \forall A \notin \Gamma, \ H(S|A) = H(S) \).

Suppose \( \Gamma \) is an access structure with the participants set \( P \). Suppose \( \Sigma \) is a
secret sharing scheme to realize \( \Gamma \). The information ratio of a participant \( p \in P \)
in \( \Sigma \), denoted by \( \sigma_p(\Sigma, \Gamma) \), is defined by \( \sigma_p(\Sigma, \Gamma) = H(p)/H(S) \). Also, the
information ratio of the scheme \( \Sigma \) is defined by \( \sigma(\Sigma, \Gamma) = \max_{p \in P} \sigma_p(\Sigma, \Gamma) \).
The optimal information ratio of the access structure \( \Gamma \) is defined as

\[
\sigma(\Gamma) = \inf(\sigma(\Sigma, \Gamma))
\]

where the infimum is taken over all secret sharing schemes \( \Sigma \) for the access structure
\( \Gamma \). A secret sharing scheme for an access structure \( \Gamma \) is ideal if \( \sigma(\Gamma) = 1 \). The
intuition and the basics of the entropy method can be found in here [14, 24]. Lemma
2.1 which was introduced in [9], is a good tool to obtain some lower bounds for the
information ratio of an arbitrary access structure \( \Gamma \).

Lemma 2.1 ([9]). Suppose that \( \Sigma \) is a secret sharing scheme with access structure
\( \Gamma \) on a set of participants \( P \). Let \( S \) be the set of secrets and \( A, B \subseteq P \). Then we have

1) if \( A \subseteq B, B \in \Gamma, \) but \( A \notin \Gamma, \) then \( H(B) \geq H(A) + H(S) \),
2) if \( A, B \in \Gamma \) but \( A \cap B \notin \Gamma, \) then \( H(A) + H(B) \geq H(A \cup B) + H(A \cap B) + H(S) \)

An equivalent form of the second condition of lemma 2.1 is that if \( X, Y, Z \subseteq P, X \cup Z \in \Gamma, Y \cup Z \in \Gamma \) and \( Z \notin \Gamma \), then we have \( I(X; Y|Z) \geq H(S) \). The
following lemma is immediate from \( H(XZ) = H(XZ|Y) + I(X; Y|Z) + I(Y; Z) \).
Lemma 2.2. Suppose that Σ is a secret sharing scheme with access structure Γ on a set of participants P. Let S be the set of secrets and X, Y, Z ⊆ P. If X ∪ Z ⊆ Γ, Y ∪ Z ∈ Γ and Z ∉ Γ, then H(XZ) ≥ H(XZ|Y) + H(S).

M. Van Dijk proved the following property in [24].

Lemma 2.3 ([24], Corollary 2.2, Corollary 2.6). Suppose that Σ is a secret sharing scheme with access structure Γ on a set of participants P. Let S be the set of secrets. Then for all X, Y, Z ⊆ P, if Y ∪ Z ∉ Γ but X ∪ Y ∪ Z ∈ Γ, then H(S) ≤ H(X|Y).

In the above lemma, if we set Z = ∅, then the fact H(S) ≤ H(X) is concluded (for further details see [7]).

A complete graph on n vertices is denoted by K_n, and the n-vertex cycle is C_n. A complete graph on n vertices is denoted by K_{n_1,...,n_k}, where n = ∑_{i=1}^k n_i and |X_i| = n_i for i = 1, ..., k. When necessary, the vertices and edges of a graph G are denoted by V(G) and E(G), respectively. Also, v' ~ v if and only if vv' ∈ E(G). Let G and H be two graphs, with vertices x and y, respectively. If we identify the vertices x and y, the resulting graph is called the coalescence of G and H at x and y (we denote it by C({G,H} : x,y)).

Let F_k = \{G_1, ..., G_k\} be a family of k connected graphs. Let v_1, ..., v_k be the vertices of the graphs G_1, ..., G_k, respectively. By the coalescence over the family F_k we mean that we identify the vertices v_1, ..., v_k of the graphs G_1, ..., G_k, respectively. The resulting coalescence graph over the family F_k is denoted by C(F_k : v_1, ..., v_k).

If every graph of the family F_k is isomorphic to the complete graph K_2, then C(F_k : v_1, ..., v_k) is isomorphic to the star graph K_1,n. Also, C(F_k : v_1, ..., v_k) is called the Dutch Windmill graph (denoted by D_n(k)) if every graph of the family F_k is isomorphic to the cycle graph C_n. We say that C(F_k : v_1, ..., v_k) is the Windmill graph (denoted by W_n(k)) if every graph of the family F_k is isomorphic to the complete graph K_n. In the case n = 3, the graph D_3(n) is quite famous and is called the friendship graph (denoted by F_n) [13]. In the graph G, the length of the shortest induced cycle is called the girth of G, and is denoted by g(G). Suppose that the complete graph K_1 is denoted by a single vertex v. The union of disjoint copies of the graphs G and H is denoted by G ∪ H. The join G ∨ H of (disjoint) graphs G and H is a graph that is obtained from G ∪ H by joining each vertex of G to each vertex of H. The graph v ∨ H is called the cone over H with cone vertex v.

If H is a complete multipartite graph, then v ∨ H is a complete multipartite graph.

The independent sequence method (lemma 2.4) was introduced by Blundo, et al in [4] and was generalized by Padró and Sáez in [18]. Suppose Γ is an access structure with the participants set P. A sequence of subsets \( \emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_k \not\subset \Gamma \) is made independent by a subset A ⊆ P if there exist X_1, X_2, ..., X_k ⊆ A such that for every i ∈ \{1, ..., k\} we have B_i ∪ X_i ∈ Γ and B_{i-1} ∪ X_i ∉ Γ, where B_0 is the empty set.

Lemma 2.4 ([4], Theorem 3.8), ([18], Theorem 2.1)). Let Γ be an access structure on a set of participants P. Let \( \emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_k \not\subset \Gamma \) be a sequence of subsets that is made independent by A ⊆ P. Then
\[
H(A) > \begin{cases} (k + 1)H(S) & \text{if } A \in \Gamma \\ kH(S) & \text{otherwise} \end{cases}
\]

Lemma 2.5 ([12], Lemma 4). Let G be a graphical access structure and A be a connected subset of the vertices of G. Then \( \sum_{v \in A} H(v) \geq H(A) + (|A| - 2)H(S) \).
The following theorem, which was proved in [6], characterizes the information ratio of the realized secret sharing schemes on the complete multipartite graphs.

**Lemma 2.6** ([3], Theorem 2.2). Let $G$ be a connected graph. Then $\sigma(G) = 1$ iff $G$ is a complete multipartite graph.

To find lower bound on the information ratio of the access structures several methods have been introduced. The $\lambda$–decomposition method is one of them, which was introduced by Stinson in [21]. A $\lambda$–decomposition of an access structure $\Gamma$ is the family $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subseteq \Gamma_0$ such that $\Gamma_{0,1} \cup \ldots \cup \Gamma_{0,r} = \Gamma_0$, and every element of $\Gamma_0$ is covered at least $\lambda$ times by the family $\Gamma_{0,1}, \ldots, \Gamma_{0,r}$. The following lemma is a direct consequence of theorem 2.1 of [21].

**Lemma 2.7.** Let $\Gamma$ be an access structure on the set of participants $P$.

Assume that $\Gamma_0$ is the basis of $\Gamma$ and $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subseteq \Gamma_0$ is the $\lambda$–decomposition of $\Gamma$. Suppose that $\Gamma_i$ is the access structure with basis $\Gamma_{0,i}$ and $P_i = \bigcup \mathcal{A} \in \Gamma_{0,i} \mathcal{A}$. Also, suppose that for every $i \in \{1, \ldots, r\}$ there exists a secret sharing scheme $\Sigma_i$ to realize the access structure $\Gamma_i$. Then

$$\sigma(\Gamma) \leq \frac{\max \{\sigma_{P} : p \in P\}}{\lambda},$$

where $\sigma_p = \sum_{(i,p) \in P_i} \sigma_p(\Sigma_i, \Gamma_i)$.

### 3. The Information Ratio of the Dutch Windmill Graphs

In this section we compute the exact information ratio of the secret sharing schemes for Dutch Windmill graphs.

Let $\mathcal{F}_k = \{C_{n_1}, \ldots, C_{n_k}\}$ be a family of $k$ cycles $C_{n_1}, \ldots, C_{n_k}$ of length $n_1, \ldots, n_k$, respectively. For each cycle graph $C_{n_i}$, we denote its vertex set by $V(C_{n_i}) = \{v_1^{i}, \ldots, v_{n_i}^{i}\}$. For simplicity, we denote the coalescence graph $C(\mathcal{F}_k : v_1^1, \ldots, v_k^k)$ briefly by $C(\mathcal{F}_k)$. Also, if we add a pendant (vertex of degree one is called pendant) to the central vertex (vertex with maximum degree) of the graph $C(\mathcal{F}_k)$, then we denote the resulted graph by $C'(\mathcal{F}_k)$. In the following, we determine the exact information ratio of the coalescence graph over the family $\mathcal{F}_k$ whose girth is at least five. We note that the results of the paper [12] does not yield our results.

**Theorem 3.1.** If the girth of the graphs $C(\mathcal{F}_k)$ and $C'(\mathcal{F}_k)$ is at least five, then

$$\sigma(C(\mathcal{F}_k)) = \frac{4k - 1}{2k}, \quad \sigma(C'(\mathcal{F}_k)) = \frac{4k + 1}{2k+1}.$$

**Proof.** We prove that $\sigma(C(\mathcal{F}_k)) = (4k - 1)/2k$. Let us denote the identified vertices $v_1^1, \ldots, v_k^k$ in $C(\mathcal{F}_k)$ by $v_c$ (for the sake of simplicity, we use $V(C_{n_i}) = \{v_1, v_2, \ldots, v_{n_i}\}$ to denote the vertex set of the induced subgraph $C_{n_i}$ of the graph $C(\mathcal{F}_k)$). To determine the lower bound for the information ratio of the graph $C(\mathcal{F}_k)$, it suffices to show

$$H(v_c) + H(v_2^k) + \sum_{i=1}^{k-1} (H(v_2^i) + H(v_1^i)) \geq (4k - 1)H(S).$$

According to lemma 2.5 we have

$$H(v_c) + H(v_2^k) + \sum_{i=1}^{k-1} (H(v_2^i) + H(v_1^i)) \geq H(v_1v_2^{1}v_2^{2} \ldots v_2^{k-1}v_{n_k-1}^{k-1}v_2^{k}) +

(2k - 2)H(S).$$
By Lemma 2.2
\[ H(v_c v_2^v v_1^k \ldots v_{k-1}^v v_{k-1}^k v_{n_{k-1}}^v) \geq H(v_c v_2^v v_1^k \ldots v_{k-1}^v v_{n_{k-1}}^v v_2^k) + H(S). \]
Therefore,
\[
H(v_c) + H(v_2^k) + \sum_{i=1}^{k-1} (H(v_i^v) + H(v_n^i)) \geq H(v_c v_2^v v_1^k \ldots v_{k-1}^v v_{n_{k-1}}^v v_2^k) + (2k-1)H(S).
\]
It can be seen that
\[ H(v_c v_2^v v_1^k \ldots v_{k-1}^v v_{n_{k-1}}^v v_2^k) = H(v_2^k v_n^k) + H(v_{n_{k-1}}^k v_2^k) + \ldots + H(v_c v_2^v v_1^k \ldots v_{n_{k-1}}^v v_2^k). \]
Since the girth of \( C(\mathbb{F}_k) \) is at least five, therefore for every vertex (say \( v \)) of \( \{v_1^v v_1^v \ldots v_{k-1}^v v_{k-1}^v \} \), there exists a vertex (say \( v' \)) of the graph \( C(\mathbb{F}_k) \) such that \( v' \sim v \) and \( v' \) is not adjacent to any vertex of the set \( \{v_1^v v_1^v \ldots v_{k-1}^v v_{k-1}^v \}/v \). Besides, \( \{v_1^v v_1^v \ldots v_{k-1}^v v_{k-1}^v \} \) is not a qualified subset, while \( \{v_1^v v_1^v \ldots v_{k-1}^v v_{k-1}^v \} \) is a qualified subset. Therefore, lemma 2.3 implies
\[
H(v_c v_2^v v_1^k \ldots v_{n_{k-1}}^v v_2^k) \geq 2kH(S).
\]
Substituting (2) into the inequality (1) yields
\[
H(v_c) + H(v_2^k) + \sum_{i=1}^{k-1} (H(v_i^v) + H(v_n^i)) \geq 2kH(S) + (2k-1)H(S) = (4k-1)H(S).
\]
To prove the upper bound for the information ratio of the graph \( C(\mathbb{F}_k) \), we give a covering set for \( C(\mathbb{F}_k) \) which is a trivial decomposition. Consider the subgraphs of the graph \( C(\mathbb{F}_k) \) which are introduced in the table 1. We know that in the path

**Table 1.** Subgraphs of the graph \( C(\mathbb{F}_k) \)

| \( G \) | \( V \) | \( \Pi_1 = (2k-1) \times S_1(V) \) |
|---|---|---|
| \( S_1(V) \) | \( \{v_c, v_2^v, v_1^k, \ldots, v_{n-1}^k, v_{n_k}^k\} \) | \( \Pi_2 = \{1 \times S_1(V) : i \in \{1, \ldots, k\}\} \) |
| \( S_1^i(V) \) | \( \{v_c, v_2^v, v_3^v\} \) | \( \Pi_3 = \{1 \times S_1(V) : i \in \{1, \ldots, k\}\} \) |
| \( S_2^i(V) \) | \( \{v_c, v_2^v, v_{n-1}^v\} \) | \( \Pi_4 = \{1 \times S_1(V) : i \in \{1, \ldots, k\}\} \) |
| \( P_1^i(V) \) | \( \{v_2^v, v_3^v, \ldots, v_{n-1}^v\} \) | \( \Pi_5 = \{1 \times P_2(V) : i \in \{1, \ldots, k\}\} \) |
| \( P_2^i(V) \) | \( \{v_3^v, v_4^v, \ldots, v_{n-1}^v\} \) | \( \Pi_6 = \{1 \times P_2(V) : i \in \{1, \ldots, k\}\} \) |

graph of length at least 4, the initial and last vertices have information ratio 1, and the mid vertices have information ratio 3/2. Therefore, \( \Pi = \{\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5\} \), is a 2k-decomposition of \( C(\mathbb{F}_k) \) (we note that the path \( P_2^i \) is maybe star or only one edge). Thus, by lemma 2.7 we have \( \sigma(C(\mathbb{F}_k)) \leq (4k-1)/2k \).

Now, we prove that \( \sigma(C'(\mathbb{F}_k)) = (4k+1)(2k+1) \). Suppose \( v' \) is a pendant which has been added to the vertex \( v_c \). Firstly, we show that the information ratio
of the graph \( C'(\mathcal{F}_k) \) is lower bounded by \((4k + 1)/(2k + 1)\). By similar argument, which was used in the proof of the information ratio of the graph \( C(\mathcal{F}_k) \), we have

\[
H(v_c) + \sum_{i=1}^{k} (H(v^i_2) + H(v^i_{n_i})) \geq (4k + 1)H(S).
\]

Therefore, \( \sigma(C'(\mathcal{F}_k)) \geq (4k + 1)/(2k + 1) \). To prove the upper bound, consider the subgraphs of the graph \( C'(\mathcal{F}_k) \) which are introduced in the table 2. Let \( \Pi = \{ \Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5, \Pi_6 \} \). It can be seen that \( \Pi \) is a \((2k+1)\)-decomposition of \( C'(\mathcal{F}_k) \) (we note that the path \( P_2 \) is maybe star or only one edge). Thus, by lemma 2.7 we have \( \sigma(C'(\mathcal{F}_k)) \leq (4k + 1)/(2k + 1) \).

Let \( \mathcal{F}_k = \{ C_{n_1}, \ldots, C_{n_k} \} \) be a family of cycle graphs. If all cycles in the set \( \mathcal{F}_k \) are isomorphic to the cycle graph \( C_n \), then the coalescence graph \( C(\mathcal{F}_k) \) is isomorphic to the Dutch windmill graph \( D_n^{(k)} \). Therefore, by using the theorem 3.1, the exact information ratio of the graph \( D_n^{(k)} \) (where \( n \geq 5 \)) is \((4k - 1)/(2k)\). Also, if we add a pendant to the identified vertex \( v_c \) in \( D_n^{(k)} \), then the exact information ratio of the resulted graph is \((4k + 1)/(2k + 1)\). Hitherto, we have determined the exact information ratio of secret sharing schemes on Dutch windmill graphs with girth at least 5. In the sequel of this section, we determine the exact information ratio of secret sharing schemes on Dutch windmill graphs with girth three and four.

**Theorem 3.2.** Let \( G \) be a connected graph. Suppose \( v_c \in V(G) \) and \( H_1, \ldots, H_k \) are the edge-disjoint connected subgraphs of \( G \) such that \( V(H_i) \geq 2 \) for each \( i \in \{ 1, \ldots, k \} \). Suppose for each \( i \in \{ 1, \ldots, k \} \) there exist at least two vertices \( v_{i,1}, v_{i,2} \in H_i \) such that \( v_{i,1}v_{i,1}, v_{i,1}v_{i,2} \in E(G) \) (note that we may have \( v_{i,2}v_{i,2} \in E(G) \)). Then

\[
\sigma(G) \geq \frac{2k-1}{k}, \quad \sigma(G') \geq \frac{2k+1}{k+1},
\]

where \( G' \) is the graph \( G \) when a pendant has been added to the vertex \( v_c \).

**Proof.** Let \( A = \{ v_{c,1}, v_{2,1}, \ldots, v_{k,1} \} \) and \( B = \{ v_{1,1}, v_{2,2}, v_{3,2}, \ldots, v_{k,2} \} \). To prove \( \sigma(G) \geq (2k-1)/k \), it suffices to show

\[
\sum_{v \in A} H(v) \geq (2k-1)H(S).
\]

Table 2. Subgraphs of the graph \( C'(\mathcal{F}_k) \)

| \( G \) | \( V \) | \( \Pi \) |
|---|---|---|
| \( S_1(V) \) | \( \{ v_c, v'_1, v_{i,1}^1, \ldots, v_{i,k}^1 \} \) | \( \Pi_1 = \{ (2k) \times S_1(V) \} \) |
| \( S_1'(V) \) | \( \{ v_c, v'_1, v_{i,1}^1 \} \) | \( \Pi_2 = \{ 1 \times S_1'(V) : i \in \{ 1, \ldots, k \} \} \) |
| \( S_2'(V) \) | \( \{ v_c, v_{i,1}, v_{i,n-1} \} \) | \( \Pi_3 = \{ 1 \times S_2'(V) : i \in \{ 1, \ldots, k \} \} \) |
| \( S'(V) \) | \( \{ v_c v' \} \) | \( \Pi_4 = \{ 1 \times S'(V) \} \) |
| \( P_1'(V) \) | \( \{ v'_{2,1}, v'_{3,2}, \ldots, v'_{n_i} \} \) | \( \Pi_5 = \{ 2k \times P_1'(V) : i \in \{ 1, \ldots, k \} \} \) |
| \( P_2'(V) \) | \( \{ v'_{3,1}, \ldots, v'_{i,n-1} \} \) | \( \Pi_6 = \{ 1 \times P_2'(V) : i \in \{ 1, \ldots, k \} \} \) |
Since $A$ is a connected subset of the vertices of $G$, lemma 2.5 implies
\[ \sum_{v \in A} H(v) \geq H(A) + (k - 2)H(S). \]

Let $B_1 = \{v_{1,1}\}$ and $B_i = B_{i-1} \cup \{v_{i,2}\}$, where $i \in \{2, \ldots, k\}$. It can be seen that the sequence $B_1 \subset B_2 \subset \cdots \subset B_k$ is made independent by $A$. Therefore, lemma 2.4 implies
\[ \sum_{v \in A} H(v) \geq (2k - 1)H(S). \]

Now, we prove $\sigma(G') \geq (2k + 1)/(k + 1)$. Suppose $v'$ is a pendant which has been added to the vertex $v_c$. Let $A = \{v_c, v_{1,1}, v_{2,1}, v_{3,1}, \ldots, v_{k,1}\}$ and $B = \{v', v_{1,2}, v_{2,2}, v_{3,2}, \ldots, v_{k,2}\}$. By similar argument, which was used in the proof of $\sigma(G) \geq (2k - 1)/k$, we have
\[ \sum_{v \in A} H(v) \geq (2k + 1)H(S). \]

Therefore, $\sigma(G') \geq (2k + 1)/(k + 1)$.

Consider the graph $D_4^{(k)}$ with labelling, which is introduced in figure 1. The vertex $v_c$ is the central vertex of the graph $D_4^{(k)}$. We use $D_4^{(k)}$ to denote the graph $D_4^{(k)}$ when a pendant is added to the vertex $v_c$. In theorem 3.3, we determine the exact information ratio of the graphs $D_4^{(k)}$ and $D_4^{(k)}$.

**Theorem 3.3.** Let $k$ be a positive integer. Then
\[ \sigma(D_4^{(k)}) = \frac{2k - 1}{k}, \quad \sigma(D_4^{(k)}) = \frac{2k + 1}{k+1}. \]

**Proof.** We prove that $\sigma(D_4^{(k)}) = (2k - 1)/k$. Suppose that $V(D_4^{(k)}) = \{v_c, v_1, v_2, v_3, \ldots, v_{3k}\}$ denotes the vertex set of $D_4^{(k)}$. By the labelling, which is introduced in Figure 1, the edge set of the graph $D_4^{(k)}$ is
\[ E(D_4^{(k)}) = \{v_i v_{i+1}, v_{i+1} v_{i+2}, v_c v_i, v_c v_{i+2} : i \in \{1, 4, \ldots, 3(k-1) - 2, 3k - 2\}\}. \]

Consider the subgraphs of the graph $D_4^{(k)}$, which are introduced in the table 3. Let
\[ \Pi_1 = \{(k-1) \times G_1\}, \quad \Pi_2 = \{G_i : i \in \{2, 3, \cdots, k+1\}\}, \quad \Pi_3 = \{(k-1) \times G_i : i \in \{k+1\}\}. \]
Table 3. Subgraphs of the graph $D_4^{(k)}$

| $G$            | $V(G)$                           | $E(G)$                              |
|----------------|----------------------------------|-------------------------------------|
| $G_1$          | $\{v_c, v_1, v_3, \ldots, v_{3k-2}, v_{3k}\}$ | $\{v_cv_j, vcv_{j+2} : j \in \{1, 4, \ldots, 3k-2\}\}$ |
| $G_{1+(i+2)/3}$ | $\{v_c, v_i, v_{i+1}, v_{i+2}\}$ | $\{v_iv_i, v_i v_{i+2}, v_i v_{i+1}, v_{i+1} v_{i+2}\}$ |
| $G_{k+1+(i+2)/3}$ | $\{v_i, v_{i+1}, v_{i+2}\}$ | $\{v_i v_{i+1}, v_{i+1} v_{i+2}\}$ |

2, \ldots, 2k+1}, and $\Pi = \{\Pi_1, \Pi_2, \Pi_3\}$. It can be seen that $\Pi$ is a $k$-decomposition of $D_4^{(k)}$. Therefore, by lemma 2.7 we have $\sigma(D_4^{(k)}) \leq (2k - 1)/k$. By using the theorem 3.2, it can be said that $\sigma(D_4^{(k)}) \geq (2k - 1)/k$. Thus, $\sigma(D_4^{(k)}) = (2k - 1)/k.$

Now, we prove that $\sigma(D_4^{(k)}) = (2k + 1)/(k + 1)$. Suppose $v'$ is a pendant which has been added to the vertex $v_c$. To prove the upper bound for the information ratio of the graph $D_4^{(k)}$, consider the subgraphs of the graph $D_4^{(k)}$ as introduced in table 4.

Table 4. Subgraphs of the graph $D_4^{(k)}$

| $G$            | $V(G)$                           | $E(G)$                              |
|----------------|----------------------------------|-------------------------------------|
| $G_1$          | $\{v_c, v_1, v_3, \ldots, v_{3k-2}, v_{3k}\}$ | $\{v_cv_j, vcv_{j+2}, vcv' : j \in \{1, 4, \ldots, 3k-2\}\}$ |
| $G_{1+(i+2)/3}$ | $\{v_c, v_i, v_{i+1}, v_{i+2}\}$ | $\{v_iv_i, v_i v_{i+2}, v_i v_{i+1}, v_{i+1} v_{i+2}\}$ |
| $G_{k+2}$      | $\{v_c, v'\}$                   | $\{v'v\}$                           |
| $G_{k+2+(i+2)/3}$ | $\{v_i, v_{i+1}, v_{i+2}\}$ | $\{v_i v_{i+1}, v_{i+1} v_{i+2}\}$ |

Let $\Pi_1 = \{k \times G_1\}, \Pi_2 = \{G_i : i \in \{2, 3, \ldots, k + 1\}\}, \Pi_3 = \{G_{k+2}\}, \Pi_4 = \{k \times G_i : i \in \{k + 3, k + 4, \ldots, 2k + 2\}\}$, and $\Pi = \{\Pi_1, \Pi_2, \Pi_3, \Pi_4\}$. It can be seen that $\Pi$ is a $(k+1)$-decomposition of $D_4^{(k)}$. Therefore, by lemma 2.7 we have $\sigma(D_4^{(k)}) \leq (2k + 1)/(k + 1)$. By using the theorem 3.2, it can be said that $\sigma(D_4^{(k)}) \geq (2k + 1)/(k + 1)$. Thus, $\sigma(D_4^{(k)}) = (2k + 1)/(k + 1)$.

Let $F_k = \{H_1, \ldots, H_k\}$ be a family of graphs and $v\nabla F_k$ be a cone graph over $H_1 \cup \cdots \cup H_k$ with cone vertex $v$. We denote by $v\nabla F'_k$ the graph $v\nabla F_k$ when a pendant is added to the cone vertex of the graph $v\nabla F_k$.

Theorem 3.4. Let $F_k = \{H_1, \ldots, H_k\}$ be a family of complete multipartite graphs with at least two vertices. Then

$$\sigma(v\nabla F_k) = \frac{2k-1}{k}, \quad \sigma(v\nabla F'_k) = \frac{2k+1}{k+1}.$$ 

Proof. We prove that $\sigma(v\nabla F_k) = (2k - 1)/k$. To prove the upper bound for the information ratio of the graph $v\nabla F_k$, consider the subgraphs of $v\nabla F_k$ as introduced in table 5.

Let $\Pi_1 = \{(k-1) \times G_1\}, \Pi_2 = \{G_i : i \in \{2, 3, \ldots, k+1\}\}$ and $\Pi_3 = \{(k-1) \times G_i : i \in \{k+2, k+3, \ldots, 2k+1\}\}$. It can be seen that $\Pi = \{\Pi_1, \Pi_2, \Pi_3\}$ is a $k$-decomposition of $v\nabla F_k$. Therefore, by lemma 2.7 we have $\sigma(v\nabla F_k) \leq (2k-1)/k.$
By using the theorem 3.2, it can be said that $\sigma(v\nabla F_k) \geq (2k-1)/k$. Thus, $\sigma(v\nabla F_k) = (2k-1)/k$.

Now, we prove that $\sigma(v\nabla F'_k) = (2k+1)/(k+1)$. Suppose $v'$ is a pendant which has been added to the cone vertex $v$. To obtain the upper bound for the information ratio of the graph $v\nabla F'_k$, consider the subgraphs of $v\nabla F'_k$ as introduced in table 6. Let $\Pi_1 = \{k \times G_1\}$, $\Pi_2 = \{G_i : i \in \{2,\ldots,k+1\}\}$.

| $G$     | $V(G)$                        | $E(G)$                        |
|---------|-------------------------------|-------------------------------|
| $G_1$   | $\{v, V(H_1), V(H_2), \ldots , V(H_k)\}$ | $\{vw : w \in \{V(H_1), \ldots , V(H_k)\}\}$ |
| $G_{1+i}$, $i \in \{1, \ldots , k\}$ | $\{v, V(H_i)\}$ | $\{E(H_i), vw : w \in V(H_i)\}$ |
| $G_{k+1+i}$, $i \in \{1, \ldots , k\}$ | $V(H_i)$ | $E(H_i)$ |

$\Pi_3 = \{G_{k+2}\}$ and $\Pi_4 = \{k \times G_i : i \in \{k+2, \ldots , 2k+2\}\}$. It can be seen that $\Pi = \{\Pi_1, \Pi_2, \Pi_3, \Pi_4\}$ is a $(k+1)$-decomposition of $v\nabla F'_k$. Therefore, by lemma 2.7 we have $\sigma(v\nabla F'_k) \leq (2k+1)/(k+1)$. By using the theorem 3.2, it can be said that $\sigma(v\nabla F'_k) \geq (2k+1)/(k+1)$. Thus, $\sigma(v\nabla F'_k) = (2k+1)/(k+1)$.

In the cone graph $v\nabla F_k$ if each graph of the family $\mathcal{F}_k$ is isomorphic to the graph $K_2$, then $v\nabla F_k$ is isomorphic to the friendship graph $F_k$ (see Figure 2). Therefore, as a direct consequence of the theorem 3.4, we have $\sigma(F_k) = (2k-1)/k$ and $\sigma(F'_k) = (2k+1)/(k+1)$, where $F'_k$ is a friendship graph when a pendant is added to the dominating vertex (a vertex that is adjacent to all other vertices) of the graph $F_k$. Furthermore, the exact information ratio of the windmill graph $W_n^{(k)}$ is $(2k-1)/k$.

Let $\mathcal{F}_k = \{G_1, \ldots , G_n\}$ be a family of graphs. In this paper, we determined the information ratio of the coalescence graph over $\mathcal{F}_k$ in some special cases. An interesting research problem can be as follows:

**Problem.** For special family of $\mathcal{F}_k = \{G_1, \ldots , G_n\}$, determine the information ratio of the coalescence graph over $\mathcal{F}_k$.

The friendship graph $F_k$ is a cone graph over the $k$ complete graphs $K_2$. We calculated the exact information ratio of this graph. The below question can be studied for future work:

**Problem.** Let $G$ be an arbitrary graph and $v\nabla G$ denotes the cone graph over $G$. Determine the exact information ratio of the graph $v\nabla G$. 
Figure 2. The friendship graph $F_k$ with predefined labelling

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers whose valuable suggestions increased the readability and quality of the current paper.

REFERENCES

[1] J. C. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, Advances in Cryptology-Crypto 88 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 403 (1990), 27–35.
[2] G. R. Blakley, Safeguarding Cryptographic Keys, in AFIPS Conference Proceedings, 48 (1979), 313–317.
[3] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, Advances in Cryptology-Proceeding of Eurocrypt 92, Lecture Notes in Computer Sci, 658 (1993), 1–24.
[4] C. Blundo, A. De Santis and U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, Designs Codes and Cryptography, 11 (1997), 107–122.
[5] C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, On the classification of ideal secret sharing schemes, Journal of Cryptology, 4 (1993), 157–167.
[6] R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, Journal of Cryptology, 6 (1993), 157–169.
[7] T. M. Cover and J.A. Thomas, Elements of Information Theory, 2nd edition, John Wiley and Sons, Inc., Hoboken, New Jersey, 2006.
[8] L. Csirmaz, The size of a share must be large, Journal of Cryptology, 10 (1997), 223–231.
[9] L. Csirmaz, An impossibility result on graph secret sharing, Designs Codes and Cryptography, 53 (2009), 195–209.
[10] L. Csirmaz and G. Tardos, Optimal information rate of secret sharing schemes on trees, IEEE Transaction on Information Theory, 59 (2013), 2527–2530.
[11] L. Csirmaz and P. Ligeti, On an infinite family of graphs with information ratio $1 - \frac{2}{k}$, Computing, 85 (2009), 127–136.
[12] P. Erdős, A. Réyi and V. T. Sós, On a problem of graph theory, Studia Sci. Math. Hungar, 1 (1966), 215–235.
[13] R. G. Gallager, Information Theory and Reliable Communications, John Wiley, New York, 1986.
[14] M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, Proc. IEEE Globecorn, Tokyo, 87 (1987), 99–102.
[15] M. Ito, A. Saito and T. Nishizeki, Multiple assignment scheme for sharing secret, Journal of Cryptology, 6 (1993), 15–20.
[16] W. Jackson and Keith M. Martin, Perfect secret sharing schemes on five participants, Designs. Codes and Cryptography, 9 (1996), 267–286.
[17] C. Padró and G. Sáez, Secret sharing with bipartite access structure, IEEE Transaction on Information Theory, 46 (2000), 2596–2604.
[19] C. Padró, L. Vazquez, Finding lower bounds on the complexity of secret sharing schemes by linear programming, Ninth Latin American Theoretical Informatics Symposium, LATIN 2010, Lecture Notes in Computer Science, 6034 (2010), 344–355.

[20] A. Shamir, How to share a secret, Communication of the ACM, 22 (1979), 612–613.

[21] D. R. Stinson, Decomposition constructions for secret sharing schemes, IEEE Transaction on Information Theory, 40 (1994), 118–125.

[22] D. R. Stinson, An explication of secret sharing schemes, Designs Codes and Cryptography, 2 (1992), 357–390.

[23] H. M. Sun and B. L. Chen, Weighted decomposition construction for perfect secret sharing schemes, Compute Math. Appl., 43 (2002), 877–887.

[24] M. Van dijk, On the information rate of perfect secret sharing schemes, Designs, Codes and Cryptography, 6 (1995), 143–169.

Received April 2018; revised July 2018.

E-mail address: bagher.bagherpour@mut-es.ac.ir
E-mail address: shjanbaz@mut-es.ac.ir
E-mail address: a_zaghian@mut-es.ac.ir