www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 10 No. 2 (2021), pp. 107-120.
© 2021 University of Isfahan

www.ui.ac.ir

IDEAL SECRET SHARING SCHEMES ON GRAPH-BASED 3-HOMOGENEOUS ACCESS STRUCTURES

SHAHROOZ JANBAZ*, ALI ZAGHIAN AND BAGHER BAGHERPOUR

Abstract. The characterization of the ideal access structures is one of the main open problems in secret sharing and is important from both practical and theoretical points of views. A *graph-based* $3-$*homogeneous access structure* is an access structure in which the participants are the vertices of a connected graph and every subset of the vertices is a minimal qualified subset if it has three vertices and induces a connected graph. In this paper, we introduce the graph-based $3-$homogeneous access structures and characterize the ideal graph-based 3-homogeneous access structures. We prove that for every non-ideal graph-based 3-homogeneous access structure over the graph G with the maximum degree d there exists a secret sharing scheme with an information rate $\frac{1}{d+1}$. Furthermore, we mention three forbidden configurations that are useful in characterizing other families of ideal access structures.

1. Introduction

Secret sharing schemes were introduced by Shamir [16] and Blakley [2]. A *perfect secret sharing scheme* is a method of sharing a secret among a set of participants P in such a way that only pre-specified subsets of P are able to reconstruct the secret by pooling their shares and the other subsets of P are unable to obtain any information about the secret in an information theoretical sense. A subset of P is called *qualified* if is able to reconstruct the secret. The collection of all qualified subsets of P is called *access structure* and is denoted by Γ. If $A \notin \Gamma$, then A is called a *non-qualified subset.* Assume that 2^P denotes the all subsets of P. A qualified subset $A \in \Gamma$ is a *minimal qualified subset*

Communicated by Dianhua Wu.

Manuscript Type: Research Paper.

MSC(2010): Primary: 94A60; Secondary: 94A62.

Keywords: Cryptography, Secret sharing, Ideal access structures, Graph-based access structures, 3-homogeneous access structures.

Received: 23 June 2020, Accepted: 26 January 2021.

∗Corresponding author.

http://dx.doi.org/10.22108/toc.2021.123661.1739

.

if for all $B \in 2^P$ with $B \subset A$, it holds $B \notin \Gamma$. The collection of all minimal qualified subsets of P is called the *basis* of Γ and is denoted by Γ_0. In general, access structures have the *monotone increasing* property, that is, every superset of a qualified subset is a qualified subset. A non-qualified subset $B \in 2^P$ is called *maximal non-qualified* if for all $B' \in 2^P$ with $B \subset B'$, it holds $B' \in \Gamma$. The *information rate* of a secret sharing scheme is the ratio between the length (in bit) of the secret and the maximum length (in bit) of the shares given to the participants. A secret sharing scheme is *ideal* if its information rate is equal to one. Also, an access structure is *ideal* if there exists an ideal secret sharing scheme to realize it.

An *r-homogeneous access structure* is an access structure in which every minimal qualified subset has exactly r participants. The graph-based access structures (those in which the participants set and the basis of the access structure are the vertex set and the edge set of a graph G, respectively) are one of the famous r-homogeneous access structures by which the ideal 2-homogeneous access structures have been exactly characterized [6, 17]. Nevertheless, the characterization of the ideal access structures is one of the long standing open problems in secret sharing. Due to the difficulty of this problem, the ideality of the several particular classes of access structures has been studied. Martí-Farré and Padró characterized all ideal $3-$homogeneous access structures in which the number of minimal qualified subsets contained in any set of four participants is not equal to three [9, 12]. The ideal secret sharing schemes on the access structures with three or four minimal qualified subsets were characterized in [8]. In [10], the authors studied the ideality of the rank-three access structures (those in which every minimal qualified subset has at most three participants) and characterized the ideal rank-three access structures in some cases. In [19], the authors gave an ideal secret sharing scheme to realize the compartmented access structures by using the bivariate interpolation.

1.1. Motivation and Contribution.

Graphs are important tools in secret sharing and they have been used in characterizing the ideal 2-homogeneous access structures and computing information rate of non-ideal 2-homogeneous access structures [1]. Unfortunately, the graphs have not been used in studying the 3-homogeneous access structures, while the graphs may facilitate the problem of characterizing the ideal 3-homogeneous access structures. This motivated us to study the 3-homogeneous access structure using the graph-based 3-homogeneous access structures. We say that an access structure is the *graph-based* $3-$*homogeneous access structure* (briefly GB-3h access structure) on a graph G if the participants set is the vertex set $V(G)$ and the basis of the access structure is the set of the subsets $A \subseteq V(G)$ such that $|A| = 3$ and the induced subgraph of G over A is connected. The GB-3h access structure and its basis are denoted by $G|_3$ and $\Gamma_0(G|_3)$, respectively. In this study, we completely characterize the ideal GB-3h access structures. We give a general lower bound for the information rate of the non-ideal GB-3h access structures and present three forbidden configurations for GB-3h access structures to be ideal. These forbidden configurations can be useful in characterizing other families of ideal access structures. We stress that the GB-3h access structures have not been studied by now and this work is the first work that characterizes the ideal GB-3h access structures.

http://dx.doi.org/10.22108/toc.2021.123661.1739

1.2. **Paper organization.** The rest of the paper is organized as the follows: Some definitions and general results are expressed in section 2. Section 3 is devoted to our results. Section 4 concludes the paper.

2. Preliminary

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 $A = \{p_{i_1}, \dots, p_{i_r}\} \subseteq P$, the Shannon entropy of the random variable taking values in $K(A) = K(p_{i_1}) \times \cdots \times K(p_{i_r})$ is denoted by $H(A)$ (for more details see [3]). If Γ is an access structure, $p_1 \cdots p_k \in \Gamma$ means $\{p_1, \dots, p_k\} \in \Gamma$. In terms of the entropy, a perfect secret sharing scheme for an access structure Γ must verify the following properties:

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

The information rate of a secret sharing scheme Σ, for an access structure Γ and the set of the secrets S, is defined as

$$\rho(\Sigma, \Gamma, S) = \frac{H(S)}{max_{p \in P} H(p)}.$$

When the probability distributions on S and $K(p)$ are uniform, the information rate is

$$\rho(\Sigma, \Gamma, S) = \frac{\log |S|}{max_{p \in P} \log |K(p)|}.$$

The optimal information rate of Γ is defined as $\rho(\Gamma) = \sup\ \rho(\Sigma, \Gamma, S)$, where the suprmum is taken over all secret sharing schemes and all possible sets of the secrets $|S| \geq 2$. The *dual* of the access structure Γ is equal to the access structure $\Gamma^* = \{A \subset P : P \setminus A \notin \Gamma\}$. Given an access structure Γ, it holds $\rho(\Gamma) = \rho(\Gamma^*)$ [7]. A $(t, n)-$*threshold* access structure is an access structure whose basis consists of all subsets with t participants of a set of n participants.

Definition 2.1. *Let P be a set of participants that is compartmented into the disjoint subsets $C_1, \dots, C_m$. For $i = 1, \dots, m$, let a_i and a are the positive integers for which $\sum_{i=1}^m a_i \geq a$. An access structure Γ is called the compartmented access structure with upper bounds (in briefly CAS-UP access structure) on the participants set P if Γ_0 consists of all subsets $A \subseteq P$ such that $|A| = a$ and for each $i \in \{1, \dots, m\}$ it holds $|A \cap C_i| \leq a_i$.*

Both the threshold and the CAS-UP access structures are ideal [19]. Let Γ be an access structure on the participants set P and $A \subset P$. The *restriction* of Γ at A (is denoted by $\Gamma(A)$) is an access

http://dx.doi.org/10.22108/toc.2021.123661.1739

structure on A such that for every $B \subset A$ we have $B \in \Gamma(A)$ if and only if $B \in \Gamma$. The *contraction* of Γ at A (is denoted by $\Gamma.A$) is an access structure on $P \setminus A$ such that for every $B \subset P \setminus A$ we have $B \in \Gamma.A$ if and only if $B \cup A \in \Gamma$.

Proposition 2.2. [7, Theorems 6 and 7] *Let Γ be an access structure on the set of participants P and $A \subset P$. Then $\rho(\Gamma(A)) \geq \rho(\Gamma)$ and $\rho(\Gamma.A) \geq \rho(\Gamma)$.*

To find lower bound on the information rate of the access structures several methods have been introduced. The $\lambda-$decomposition method is one of them, which was introduced by Stinson in [18]. A $\lambda-$decomposition of an access structure Γ is the family $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subset \Gamma_0$ such that $\Gamma_{0,1} \cup \cdots \cup \Gamma_{0,r} = \Gamma_0$, and every element of Γ_0 is covered at least λ times by the family $\Gamma_{0,1}, \ldots, \Gamma_{0,r}$. The following proposition is a direct consequence of theorem 2.1 of [18].

Proposition 2.3. [18, Theorem 2.1] *Let Γ be an access structure on the set of participants P. Assume that Γ_0 is the basis of Γ and $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subset \Gamma_0$ is the $\lambda-$decomposition of Γ. Suppose that Γ_i is the access structure with basis $\Gamma_{0,i}$ and $P_i = \bigcup_{A \in \Gamma_{0,i}} A$. Also suppose that for every $i \in \{1, \ldots, r\}$ we have $\rho(\Gamma_i) = 1$. Then*

$$\rho(\Gamma) \geq \frac{\lambda}{max\{r_p : p \in P\}},$$

where $r_p = |\{i \in \{1, \ldots, r\} : p \in P_i\}|$.

Given a graph G, the *degree* of the vertex v (denoted by $deg(v)$) is the number of the vertices of the graph G which are adjacent to v. The *maximum degree* of the graph G is denoted by $\Delta(G)$. For a graph G, the set $N(v)$ (*neighbours* of v), consists of the all vertices $w \in V(G)$ such that $vw \in E(G)$.

Definition 2.4. *Let $\{G_1, \ldots, G_n\}$ be a set of connected graphs with disjoint vertex sets. We say that the graph G is the union of the graphs $G_1, \ldots, G_n$ (denoted by $G = G_1 \sqcup \cdots \sqcup G_n$) if the following conditions hold:*

(1) $V(G) = \cup_{i=1}^{n} V(G_i)$,
(2) for each $vv' \in E(G)$, if there exists $i \in \{1, \ldots, n\}$ such that $v, v' \in V(G_i)$, then $vv' \in E(G_i)$.

Definition 2.5. *Suppose Γ is an access structure with basis Γ_0 and the participants set P. The access structure Γ is called the star access structure if there exists $B \subset P$ such that for every $A_1, A_2 \in \Gamma_0$ it holds $A_1 \cap A_2 = B$. Given a star access structure Γ with $A_1 \cap A_2 = B$ for each $A_1, A_2 \in \Gamma_0$, the elements of B are called central elements and each $p \notin B$ is called a marginal element.*

Definition 2.6. *Let us denote by $|A|$ the number of elements of $A \subseteq P$. Suppose Γ is a $r-$homogeneous access structure with basis Γ_0 and the participants set P. We say that the access structure Γ is semi-star if there exists $A \subset P$ such that for every $A_1, A_2 \in \Gamma_0$ it holds $A \subseteq A_1 \cap A_2$ and the access structure $\Gamma(P \setminus A)$ is isomorphic to the $(r - |A|, |P| - |A|)-$threshold access structure.*

http://dx.doi.org/10.22108/toc.2021.123661.1739

It can be easily seen that the semi-star access structures and threshold access structures are a family of the CAS-UP access structures. Therefore, the semi-star access structures are ideal. The graph G in which $V(G) = \{v_c, v_1, \ldots, v_n\}$ and

$$E(G) = \{v_c v_i : i \in \{1, \ldots, n\}\} \cup \{v_{j-1}v_j : \text{for some } j \in \{2, \ldots, n\}$$
$$\text{such that } \{v_{j-1}v_j, v_j v_{j+1}\} \nsubseteq E(G)\}$$

is a large family of the graphs (say the semi-star graphs) whose GB-3h access structures are the semi-star access structure. In Figure 2, the graphs G'_1, G_5 and G_7 are semi-star. If the graph G has at most four vertices, then $G|_3$ is ideal. In Figure 2, we state the optimal information rate of the GB-3h access structures on the non-complete multipartite graphs with five vertices. Using the lemmas 3.1, 3.2 and 3.3 and the results of the paper [7], it can be concluded that if a non-complete multipartite graph G with $V(G)| = 5$, is isomorphic to the one of the graphs of $\mathbf{Z} = \{G_{11}, G_{10}, G_7, G_5\}$, then $G|_3$ is ideal, otherwise $G|_3$ is not ideal.

3. Our results

In lemmas 3.1, 3.2 and 3.3, we mention three forbidden configurations for GB-3h access structures to be ideal. These forbidden configurations will be used in the proof of our main results.

Lemma 3.1. *Let G be a connected graph and $|V(G)| \geq 5$. If the graph G has at least one connected induced subgraph isomorphic to P_4, then the access structure $G|_3$ is not ideal.*

Proof. Without loss of generality suppose that F is a connected induced subgraph of the graph $G, V(F) = \{v_1, \ldots, v_4\}$ and $E(F) = \{v_1v_2, v_2v_3, v_3v_4\}$. Since the graph G has at least five vertices, it can be said that there exists a vertex (say v_5) such that v_5 is adjacent to some vertices of $V(F)$. Let us denote the induced subgraph of G over the set $\{v_1, \ldots, v_5\}$ by F'. To prove the lemma we distinguish some cases:

(1) Vertex v_5 is adjacent to one vertex of $V(F)$. By symmetry it suffices to consider two cases: If $v_4v_5 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_2v_3v_4, v_3v_4v_5\}.$$

The basis of access structure $F'|_3 .\{v_3\}$ is equal to $\{v_1v_2, v_2v_4, v_4v_5\}$. Since $\rho(F'|_3 .\{v_3\}) \leq 2/3$, proposition 2.2 implies that $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_1, therefore the access structure $G_1|_3$ is not ideal, see Figure 2). If $v_5v_3 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_2v_3v_4, v_2v_3v_5, v_3v_4v_5\}.$$

The basis of access structure $F'|_3 .\{v_3\}$ is $\{v_1v_2, v_2v_4, v_2v_5, v_4v_5\}$. Since $\rho(F'|_3 .\{v_3\}) \leq 2/3$, proposition 2.2 implies that $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_2, therefore the access structure $G_2|_3$ is not ideal, see Figure 2).

http://dx.doi.org/10.22108/toc.2021.123661.1739

(2) Vertex v_5 is adjacent to two vertices of $V(F)$. By symmetry, it suffices to consider the following cases: If $v_5v_4, v_5v_3 \in E(G)$, then $\Gamma_0(F'|_3)$ is equal to $\{v_1v_2v_3, v_2v_3v_4, v_2v_3v_5, v_3v_4v_5\}$. We proved that in this case the access structure $G|_3$ is not ideal (in this case, F' is isomorphic to the graph G_4, therefore the access structure $G_4|_3$ is not ideal, see Figure 2). If $v_4v_5, v_2v_5 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_1v_2v_5, v_2v_3v_4, v_2v_3v_5, v_3v_4v_5, v_2v_4v_5\}.$$

The basis of access structure $F'|_3 .\{v_3\}$ is $\{v_1v_2, v_2v_4, v_5v_4, v_2v_5\}$. Since $\rho(F'|_3 .\{v_3\}) \leq 2/3$, proposition 2.2 implies that $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_3, therefore the access structure $G_3|_3$ is not ideal, see Figure 2). If $v_4v_5, v_1v_5 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_2v_3v_4, v_3v_4v_5, v_4v_5v_1, v_5v_1v_2\}.$$

The basis of access structure $F'|_3 .\{v_2\}$ is $\{v_1v_3, v_1v_5, v_3v_4\}$. Obviously, $\rho(F'|_3 .\{v_2\}) \leq 2/3$ and proposition 2.2 implies that $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_{12}, therefore the access structure $G_{12}|_3$ is not ideal, see Figure 2). Finally, suppose $v_5v_3, v_2v_5 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_1v_2v_5, v_2v_3v_4, v_3v_4v_5, v_2v_3v_5\}.$$

The basis of access structure $F'|_3 .\{v_2\}$ is $\{v_1v_3, v_1v_5, v_3v_4, v_3v_5\}$, therefore $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_{13}, therefore the access structure $G_{13}|_3$ is not ideal, see Figure 2).

(3) Vertex v_5 is adjacent to three vertices of $V(F)$. By symmetry, it suffices to consider two cases: If $v_4v_5, v_3v_5, v_5v_2 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_1v_2v_5, v_2v_3v_4, v_3v_4v_5, v_2v_3v_5, v_2v_4v_5\}.$$

The basis of the access structure $F'|_3 .\{v_5\}$ is $\{v_1v_2, v_2v_3, v_2v_4, v_3v_4\}$. Since $\rho(F'|_3 .\{v_5\}) \leq 2/3$, proposition 2.2 implies that $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_8, therefore the access structure $G_8|_3$ is not ideal, see Figure 2). If $v_4v_5, v_3v_5, v_5v_1 \in E(G)$, then

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_1v_2v_5, v_1v_5v_3, v_1v_4v_5, v_2v_3v_4, v_3v_4v_5, v_2v_3v_5\}.$$

The basis of the access structure $F'|_3 .\{v_1\}$ is $\{v_5v_3, v_4v_5, v_2v_3, v_2v_5\}$. Since $\rho(F'|_3 .\{v_1\}) \leq 2/3$, proposition 2.2 implies that $G|_3$ is a non-ideal access structure (in this case, F' is isomorphic to the graph G_{14}, therefore the access structure $G_{14}|_3$ is not ideal, see Figure 2).

(4) Finally, suppose v_5 is adjacent to all vertices of $V(F)$. In this case

$$\Gamma_0(F'|_3) = \{v_1v_2v_3, v_1v_2v_5, v_1v_5v_3, v_1v_4v_5, v_2v_3v_4, v_3v_4v_5, v_2v_3v_5, v_2v_4v_5\}.$$

The basis of the access structure $F'|_3 .\{v_1\}$ is $\{v_5v_3, v_4v_5, v_2v_3, v_2v_5\}$. Since the access structure $F'|_3 .\{v_1\}$ is not ideal, the access structure $G|_3$ is not ideal (in this case, F' is isomorphic to the graph G_{15}, therefore $G_{15}|_3$ is not ideal, see Figure 2).

Thus, if a connected graph G has at least one induced subgraph isomorphic to P_4 and $|V(G)| \geq 5$, then the access structure $G|_3$ can not be ideal. □

Lemma 3.2. *Let G be a connected graph and $|V(G)| \geq 5$. If the graph G has at least one subgraph (say G_f) isomorphic to P_3 and a vertex which is not adjacent to any vertex of G_f, then the access structure $G|_3$ is not ideal.*

Proof. Suppose $V(G_f) = \{v_1, v_2, v_3\}$. Let v_4 be the last vertex on the path which is not connected to any vertex of the set $V(G_f)$. Let $v_4v_5 \in E(G)$, where v_5 is adjacent to some vertices of the set $V(G_f)$. Suppose F is the induced subgraph of the graph G over the vertex set $\{v_1, v_2, v_3, v_4, v_5\}$. We distinguish two cases: (1) the induced subgraph G_f is isomoprhic to P_3, (2) the induced subgraph G_f is isomorphic to K_3 (i.e.; the complete graph with three vertices). First, we consider $E(G_f) = \{v_1v_2, v_2v_3\}$. For this cases, we distinguish two cases:

(1) If v_5 is adjacent to at most two vertices of G_f, then there exists an induced subgraph of F such that it is isomorphic to P_4. By lemma 3.1, the access structure $G|_3$ is not ideal.

(2) If v_5 is adjacent to all vertices of G_f, then

$$\Gamma_0(G|_3 (F)) = \{v_5v_4v_1, v_5v_4v_3, v_5v_1v_3, v_5v_1v_2, v_5v_2v_3, v_1v_2v_3, v_5v_2v_4\}.$$

The basis of access structure $F|_3 .\{v_1\}$ is $\{v_2v_3, v_5v_2, v_5v_3, v_5v_4\}$, therefore $G|_3$ is not ideal (in this case, the graph F is isomorphic to the graph G_6, therefore the access structure $G_6|_3$ is not ideal, see Figure 2).

Now, suppose G_f is isomorphic to K_3. The proof of this case is similar to the proof of the previous case (in this case, the graph F is isomorphic to the graph G_9, therefore the access structure $G_9|_3$ is not ideal, see Figure 2). Hence, if G has at least one subgraph (say G_f) isomorphic to P_3 and $G|_3$ is ideal, then each vertex of $V(G) \setminus V(G_f)$ must be adjacent to some vertices of G_f. □

The following lemma can easily be proved using the lemmas 3.1 and 3.2.

Lemma 3.3. *Let G be a connected graph, $|V(G)| \geq 5$, and $G|_3$ be an ideal access structure. Suppose $A \subseteq V(G), |A| = 5$, and induced subgraph of the graph G over A is connected. If $G|_3 (A)$ is not semi-star, then the basis of the access structure $G|_3 (A)$ has at least nine elements.*

Remark 3.4. *The mentioned forbidden configurations (the lemmas 3.1, 3.2* and 3.3) not only are useful in characterizing the ideal GB-3h access structures but also can be useful in characterizing other families of ideal access structures. For example, consider the access structure Γ with the participants set $P = \{p_1, \ldots, p_6\}$ and the basis

$$\Gamma_0 = \{p_1p_2p_3, p_2p_3p_4, p_1p_2p_4, p_2p_4p_5, p_6p_2\}.$$

Let $A = \{p_1, \ldots, p_5\}$. The basis of the access structure $\Gamma(A)$ is equal to the following set

$$\{p_1p_2p_3, p_2p_3p_4, p_1p_2p_4, p_2p_4p_5\}.$$

The access structure $\Gamma(A)$ is isomorphic to the access structure $G|_3$, where $V(G) = \{v_1, \ldots, v_5\}$ and $E(G) = \{v_2v_1, v_2v_3, v_2v_4, v_4v_5\}$. Since in the graph G the vertex v_5 is not adjacent to any vertex of $\{v_1, v_2, v_3\}$ and the subgraph of G over the set $\{v_1, v_2, v_3\}$ is isomorphic to P_3, lemma 3.2 implies that $G|_3$ is not ideal. Therefore, Γ is not ideal.

A sufficient condition for the GB-3h access structures to be threshold is expressed in lemma 3.5.

Lemma 3.5. *Let G be a connected graph with n vertices and $n \geq 3$. The access structure $G|_3$ is a $(3, n)$-threshold access structure if and only if G is isomorphic to a complete multipartite graph with partition sets of size at most two.*

Proof. Suppose the access structure $G|_3$ is a $(3, n)$-threshold access structure. We show that G is isomorphic to a complete multipartite graph with partition sets of size at most two. Otherwise, there exists $\{v_1, v_2, v_3\} \subset V(G)$ such that the induced subgraph of G over $\{v_1, v_2, v_3\}$ is not connected. Thus, $G|_3$ is not a $(3, n)$-threshold access structure, a contradiction. Now, since G is a complete multipartite graph with partition sets (say V_i, where $i = 1 \ldots, m$) of size at most two, for every $A \subset V(G)$ with $|A| = 3$, there exists a connected induced subgraph of G with three vertices over A. Therefore, the access structure $G|_3$ is a $(3, n)$-threshold access structure. □

Lemma 3.6. *Let G be the complete multipartite graph with $|V(G)| = n \geq 3$. Then the access structure $G|_3$ is ideal.*

Proof. Without loss of generality suppose $V_1, \ldots, V_{m-1}$, and V_m are the partition sets of the complete multipartite graph G. Let $A \subset V(G)$ and $|A| = 3$. If for every $i \in \{1, \ldots, m\}$ it holds $A \nsubseteq V_i$, then the induced subgraph of G over A is connected and we have $A \in G|_3$. Evidently, if there exists $i \in \{1, \ldots, m\}$ such that $B \subseteq V_i$ and $|B| \geq 3$, then $B \notin G|_3$. Therefore, $\Gamma_0(G|_3)$ is equal to $\{A \subseteq V(G) : |A| = 3, |A \cap C_i| \leq 2, i = 1, \ldots, m\}$, where $C_i = V_i$ for $i = 1, \ldots, m$. Hence, $G|_3$ is isomorphic to the CAS-UP access structure and is ideal. □

In theorem 3.7, we present a full characterization of the ideal GB-3h access structures. In the proof of theorem 3.7, we assume that the access structure $G|_3$ is not semi-star and $|V(G)| \geq 5$.

Theorem 3.7. *Let G be a connected graph and $\overline{G}$ be the complement graph of G. Then the access structure $G|_3$ is ideal if and only if the following conditions hold:*

(1) There exist suitable graphs $G_1, \ldots, G_m$ such that $\overline{G} = G_1 \sqcup \cdots \sqcup G_m$ and for each $i \in \{1, \ldots, m\}$ the induced subgraph of $\overline{G}$ over $V(G_i)$ is isomorphic to the complete multipartite graph with partition sets of size at most two,

(2) for every $\{v, v', v''\} \subset V(\overline{G})$, if there exist at least two integers $i, j \in \{1, \ldots, m\}$ such that $\{v, v', v''\} \cap V(G_i) \neq \emptyset$ and $\{v, v', v''\} \cap V(G_j) \neq \emptyset$, then the induced subgraph of $\overline{G}$ over the vertex set $\{v, v', v''\}$ is not connected.

Proof. We prove that if the graph G satisfies the expressed conditions, then the access structure $G|_3$ is isomorphic to the CAS-UP access structure. To this end, we compartment the vertices of G as $C_1, \ldots, C_m$, where for each $i \in \{1, \ldots, m\}$ it holds $C_i = V(G_i)$ and G_i is a suitable graph which satisfies the conditions 1 and 2. First, we show that for every $A \subset V(G)$ with $|A| \geq 3$, if there exists a compartment C_j such that $A \subseteq C_j$, then the induced subgraph of G over A is not connected. Since $A \subseteq C_j$, so in the graph $\overline{G}$ we have $A \subseteq V(G_j)$. For each $i \in \{1, \ldots, m\}$, the induced subgraph of the graph $\overline{G}$ over $V(G_i)$ is a complete multipartite graph with partition sets of size at most two, by lemma 3.5 it can be said that the induced subgraph of $\overline{G}$ over A is connected. Therefore, the induced subgraph of G over A is not connected.

Now, by condition 2, it can be easily seen that for each subset $B \subset V(G)$ with $|B| = 3$, if there exist at least two compartments C_{i_1} and C_{i_2} such that $B \cap C_{i_1} \neq \emptyset$ and $B \cap C_{i_2} \neq \emptyset$, then the induced subgraph of G over B is connected. Thus, it can be inferred that $\Gamma_0(G|_3)$ is equal to the following set

$$\{A \subset P : |A| = 3, |A \cap C_i| \leq 2, i \in \{1, \ldots, m\}\}.$$

In the other words, the access structure $G|_3$ is isomorphic to the CAS-UP access structure in which $a = 3$ and $a_i \leq 2$ for $i = 1, \ldots, m$. Therefore, $G|_3$ is an ideal access structure.

At the follows, we prove that if $G|_3$ is an ideal access structure, then the graph G must satisfy the conditions 1 and 2. Let us consider the condition 1. Suppose to the contrary that G does not satisfy the condition 1. For this condition, we distinguish two cases:

(1) There exists at least one $j \in \{1, \ldots, m\}$ such that the induced subgraph of the graph $\overline{G}$ over $V(G_j)$ is not a complete multipartite graph. Then, there exists $\{v_1, \ldots, v_4\} \subset V(G_j)$ such that the induced subgraph of the graph $\overline{G}$ over the set $\{v_1, \ldots, v_4\}$ (say F) is isomorphic to a non-complete multipartite graph. It can be said that F is isomorphic to P_4 or without loss of generality we can assume $E(F) = \{v_1v_2, v_1v_3, v_1v_4, v_3v_4\}$. Suppose F is isomorphic to P_4. Without loss of generality, suppose $E(F) = \{v_1v_2, v_2v_3, v_3v_4\}$. Then, in the graph G we have $\{v_1v_3, v_1v_4, v_2v_4\} \subset E(G)$. Since G is connected and $|V(G)| \geq 5$, lemma 3.1 implies that access structure $G|_3$ is not ideal, a contradiction. If $E(F) = \{v_1v_2, v_1v_3, v_1v_4, v_3v_4\}$, then in the graph G, the vertex v_1 is not adjacent to any vertex of the set $\{v_2, v_3, v_4\}$ and $\{v_2v_3, v_2v_4\} \subset E(G)$. By lemma 3.2 it can be said that the access structure $G|_3$ is not ideal, a contradiction.

(2) There exists at least one $j \in \{1, \ldots, m\}$ such that the induced subgraph of the graph $\overline{G}$ over $V(G_j)$ is a complete multipartite graph but G_j has at least one partition set of size at least three. Since G_j is a complete multipartite graph and has at least one partition set of size at least three, there exists $\{v_1, v_2, v_3\} \subset V(G_j)$ such that in the graph $\overline{G}$ there does not exist any edge between

http://dx.doi.org/10.22108/toc.2021.123661.1739

the vertices of the set $\{v_1, v_2, v_3\}$. Therefore, $\{v_1v_2, v_2v_3, v_3v_1\} \subset E(G)$. Since G_j has at least two partition sets in the graph $\overline{G}$, it can be said that there exists at least one vertex (say v_4) such that in the graph G the vertex v_4 is not adjacent to any vertex of the set $\{v_1, v_2, v_3\}$. Therefore the lemma 3.2 implies that the access structure $G|_3$ is not ideal. This is a contradiction.

Now, we consider the condition 2. If G is a complete multipartite graph, then the lemma 3.6 implies that $G|_3$ is isomorphic to the CAS-UP access structure. Therefore, the graph G satisfies the condition 2. Let G be a non-complete multipartite graph. Suppose to the contrary that there exists an induced subgraph, with the vertex set $A = \{v_1, v_2, v_3\}$, of $\overline{G}$ such that it satisfies the condition 2 but it is connected. Then the induced subgraph of G over A is not connected. Now, we distinguish two cases:

(1) There exist two integers $i, j \in \{1, \dots, m\}$ such that $A \cap V(G_i) \neq \emptyset$ and $A \cap V(G_j) \neq \emptyset$. Without loss of generality, suppose $A \cap V(G_i) = \{v_1, v_2\}$ and $A \cap V(G_j) = \{v_3\}$. For this case, we distinguish two cases:

Case 1) There exists at least one $k \in \{i, j\}$ such that $|V(G_k)| \geq 3$. Without loss of generality suppose $|V(G_i)| \geq 3$ and $v_4 \in V(G_i)$. Since $\{v_1, v_2, v_4\} \notin \Gamma_0(G|_3)$ and $A \notin \Gamma_0(G|_3)$, there exists at least one $A' \subset \{v_1, \dots, v_4\}$ such that $A' \in \Gamma_0(G|_3)$ (otherwise the vertices of the set $\{v_1, \dots, v_4\}$ can be compartmented as $C' = \{v_1, \dots, v_4\}$ in the access structure $G|_3$ and this is a contradiction, because we assumed that the vertices of the graph G are compartmented as $C_i = V(G_i)$, where $i = 1, \dots, m$). Suppose the induced subgraph of G over $\{v_1, \dots, v_4\}$ is connected. Since $V(G) \geq 5$ and the graph G is connected, there exists at least one vertex $v_5 \in V(G)$ such that v_5 is adjacent to some vertices of the set $\{v_1, \dots, v_4\}$. Let $W = \{v_1, \dots, v_5\}$. The induced subgraph of G over W is connected and $A, \{v_1, v_2, v_4\} \notin \Gamma_0(G|_3)$, lemma 3.3 implies that $G|_3$ is not ideal. This gives a contradiction. Now, suppose that the induced subgraph of G over $\{v_1, \dots, v_4\}$ is not connected. Since $A' \in \Gamma_0(G|_3)$, the induced subgraph of G over A' is connected. The induced subgraph of G over $\{v_1, \dots, v_4\}$ is not connected, therefore there exists a vertex of $\{v_1, \dots, v_4\}$ such that it is not adjacent to any vertex of the set A' in the graph G. Since G is a connected graph and $V(G) \geq 5$, lemma 3.2 implies that the access structure $G|_3$ is not ideal, a contradiction.

Case 2) For each $k \in \{i, j\}$ it holds $|V(G_k)| = 2$. Note that if $|V(G_j)| = 1$ and $|V(G_i)| = 2$, then the vertices of the set $V(G_i) \cup V(G_j)$ can be compartmented as $C' = V(G_i) \cup V(G_j)$ in the access structure $G|_3$ and this is a contradiction, because we assumed that the vertices of the graph G are compartmented as $C_i = V(G_i)$, where $i = 1, \dots, m$. Let $v_4 \in V(G_j)$. Then, there exist two subsets $D, D' \subset V(G_i) \cup V(G_j)$ such that D is a minimal qualified subset while $D' \notin G|_3$ and $|D'| = 3$ (otherwise the vertices $v_1, \dots, v_4$ can be partitioned as $C_i = \{v_1, v_2, v_3\}, C_j = \{v_4\}$ in the access structure $G|_3$ and this is a contradiction, because we assumed the vertices of the set $\{v_1, \dots, v_4\}$ are compartmented as $C_i = V(G_i), C_j = V(G_j)$ in the access structure $G|_3$). Suppose the induced subgraph of the graph G over $\{v_1, \dots, v_4\}$ is connected. The graph G is connected and $|V(G)| \geq 5$, therefore there exists a vertex $v_5 \in V(G)$ such that v_5 is adjacent to

http://dx.doi.org/10.22108/toc.2021.123661.1739

some vertices of the set $\{v_1, \dots, v_4\}$ in the graph G. Since $D', A \notin \Gamma_0(G|_3)$, lemma 3.3 implies that the access structure $G|_3$ is not ideal and this gives a contradiction. Now, suppose the induced subgraph of the graph G over $\{v_1, \dots, v_4\}$ is not connected. $D \in \Gamma_0(G|_3)$, therefore the induced subgraph of G over D is connected. The induced subgraph of G over $\{v_1, \dots, v_4\}$ is not connected, thus there exists a vertex of $\{v_1, \dots, v_4\}$ such that it is not adjacent to any vertex of the set D in the graph G. Since G is the connected graph and $V(G) \geq 5$, lemma 3.2 implies that the access structure $G|_3$ is not ideal, a contradiction.

(2) There exist three integers $i, j, k \in \{1, \dots, m\}$ such that $A \cap V(G_i) \neq \emptyset, A \cap V(G_j) \neq \emptyset$ and $A \cap V(G_k) \neq \emptyset$. The proof of this case is similar to the proof of the previous case.

Hence, every GB-3h access structure with at least five elements is ideal if and only if it satisfies the conditions 1 and 2. □

Remark 3.8. *Since the semi-star access structures are a family of the CAS-UP access structures, using the theorem* 3.7 it can be concluded that the ideal GB-3h access structures are isomorphic to the CAS-UP access structures.

Remark 3.9. *Using the theorem* 3.7, it can be said that the access structures $G_{10}|_3$ and $G_{11}|_3$ (see Figure 2) are ideal. This shows that there are non-complete multipartite graphs whose GB-3h access structures are ideal.

In Figure 1, we present a non-complete multipartite graph (say G_s) in which each vertex of the set $\{v_8, v_9, v_{10}, v_{11}\}$ is adjacent to all vertices of $\{v_1, \dots, v_7\}$. It can be verified that $\overline{G_s} = G_1 \sqcup G_2 \sqcup G_3 \sqcup G_4$, where

$$V(G_1) = \{v_1, v_3, v_4, v_6\}, E(G_1) = \{v_1v_3, v_1v_4, v_3v_6, v_4v_6\},$$
$$V(G_2) = \{v_2, v_5, v_7\}, E(G_1) = \{v_2v_7, v_5v_7, v_2v_5\},$$
$$V(G_3) = \{v_9, v_{11}\}, E(G_1) = \{v_9v_{11}\},$$
$$V(G_4) = \{v_{10}, v_8\}, E(G_1) = \{v_{10}v_8\}.$$

The access structure $G_s|_3$ satisfies the theorem 3.7, therefore $G_s|_3$ is an ideal GB-3h access structure with basis

$$\{A \subseteq V(G_s) : |A| = 3, |A \cap C_i| \leq 2, i = 1, \dots, 4\},$$

where $C_i = V(G_i)$ for $i = 1, \dots, 4$.

In theorem 3.10, we present a general lower bound for the information rate of the non-ideal GB-3h access structures.

Theorem 3.10. *Let G be a connected graph and $\Delta(G) = d$. If the access structure $G|_3$ is not ideal, then there exists a secret sharing scheme for $G|_3$ with information rate $1/(d+1)$.*

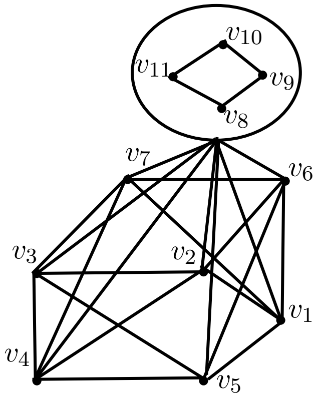


Figure 1. A simple example of GB-3h access structures

Proof. We give a covering set (say Π') for $G|_3$ such that each element of $\Gamma_0(G|_3)$ is covered at least one time by Π'. For each vertex $v \in V(G)$ (assume $deg(v) = l$ and $l \leq d$), suppose $k^v_{1,l}$ is the induced star subgraph of G such that $V(k^v_{1,l}) = N(v) \cup \{v\}$ and $deg(v) = l$. For every $v \in V(G)$, we consider $\Gamma_0(k^v_{1,l}\Big|_3)$ one time in the set Π'. Clearly, the covering set Π' has $|V(G)|$ elements and each element of $\Gamma_0(G|_3)$ is covered at least one time by the covering set Π'. Since $\Delta(G) = d$, each vertex of the graph G appears at most $d + 1$ times in the covering set Π'. By proposition 2.3, it can be said that there exists a secret sharing scheme with information rate $1/(d + 1)$ for the access structure $G|_3$. □

4. Conclusion

In this paper, we introduced the GB-3h access structures and characterized the ideal GB-3h access structures. We presented a general lower bound for the information rate of non-ideal GB-3h access structures and mentioned three forbidden configurations for GB-3h access structures to be ideal. These forbidden configurations can be useful in characterizing other families of ideal access structures.

We say that an access structure is a *graph-based $r-$homogeneous access structure* on a graph G if the participants set is the vertex set $V(G)$ and the basis of the access structure is the set of subsets $A \subseteq V(G)$ such that $|A| = r$ and the induced subgraph of G over A is connected. When $r = 2$, the graph-based 2-homogeneous access structures are isomorphic to the famous graph-based access structures and their ideal cases have exactly been characterized. For $r = 3$, we exactly characterized the ideal graph-based 3-homogeneous access structures in this paper. However, for $r \geq 4$, the characterization of ideal graph-based r-homogeneous access structures is an interesting problem which can be followed by the researchers.

http://dx.doi.org/10.22108/toc.2021.123661.1739

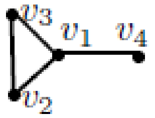
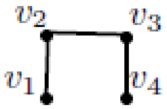
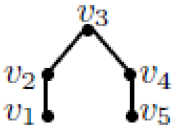
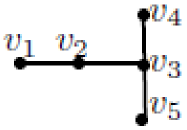
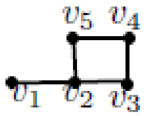
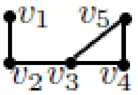
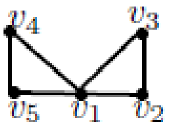
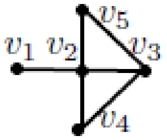
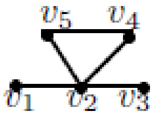
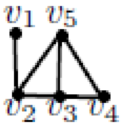
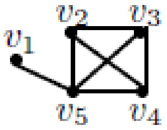
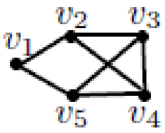
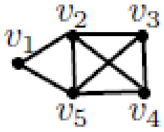
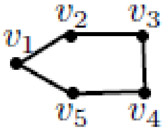
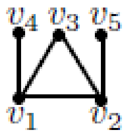
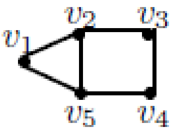
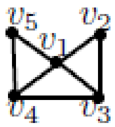
G	graphs	$\rho(G\|_3)$	G	graphs	$\rho(G\|_3)$
G'_1		1	G'_2		1
G_1		2/3	G_2		2/3
G_3		2/3	G_4		2/3
G_5		1	G_6		2/3
G_7		1	G_8		2/3
G_9		2/3	G_{10}		1
G_{11}		1	G_{12}		2/3
G_{13}		$< 2/3$	G_{14}		2/3
G_{15}		2/3			

Figure 2. The optimal information rate of the GB-3h access structures on the connected non-complete multipartite graphs with four and five vertices

References

[1] B. Bagherpour, S. Janbaz and A. Zaghian, Optimal information ratio of secret sharing schemes on Dutch Windmill graphs, *Adv. Math. Commun.*, **13** (2019) 88–99.

[2] G. R. Blakley, Safeguarding cryptographic keys, *In proceeding of the AFIPS conference*, **48** (1979) 313–317.

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

[4] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, Graph decomposition and secret sharing schemes, *J. Cryptology*, **8** (1998) 39–64.

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

[6] L. Csirmas and G. Tardos, Optimal information rate of the secret sharing schemes on trees, *IEEE Transaction on information theory*, **59** (2013).

[7] W. Jackson and K. M. Martin, Perfect secret sharing schemes on five participants, *Des. Codes Cryptogr.*, **9** (1996) 267–286.

[8] J. Martí-Farré and C. Padró, Secret sharing schemes with three or four minimal qualified subsets, *Des. Codes Cryptogr.*, **34** (2005) 17–34.

[9] J. Martí-Farré, A note on secret sharing schemes with three homogeneous access structure, *Inform. Process. Lett.*, **102** (2007) 133–137.

[10] J. Martí-Farré and C. Padró, Ideal secret sharing scheme whose minimal qualified subsets have at most three participants, *Des. Codes Cryptogr.*, **52** (2009) 1–14.

[11] J. Martí-Farré and C. Padró, Secret sharing schemes on access structures with intersection number equal to one, *Discrete Appl. Math.*, **154** (2006) 552–563.

[12] J. Martí-Farré and C. Padró, Secret sharing schemes on sparse homogeneous access structures with rank three, *Electron. J. Combin.*, **11** (2004) 16 pp.

[13] M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing any access structure, *Proc. IEEE Globecom*, **87** (1987) 99–102.

[14] C. Padró and G. Sáez, Secret sharing with bipartite access structure, *IEEE Trans. Inform. Theory*, **46** (2000) 2596–2604.

[15] C. Padró and G. Sáez, Lower bounds on the information rate of secret sharing schemes with homogeneous access structure, *Inform. Process. Lett.*, **83** (2002) 345-351.

[16] A. Shamir, How to share a secret, *Comm. ACM*, **22** (1979) 612–613.

[17] D. R. Stinson, An explanation of secret sharing scheme, *Designs, Codes and Cryptography*, (1992) 157–390.

[18] D. R. Stinson, Decomposition construction for secret sharing schemes, *IEEE Trans. Inform. Theory*, **40** (1994) 118125.

[19] T. Tassa and N. Dyn, Multipartite secret sharing by bivariate interpolation, *J. Cryptology*, 22 (2009) 227258.

[20] T. Tassa, Hierarchical Threshold Secret Sharing, *J. Cryptology*, **20** (2007) 237264.

Shahrooz Janbaz

Electrical and computer faculty, Malek Ashtar University of Technology, Tehran, Iran.

Email: shjanbaz@mut-es.ac.ir

http://dx.doi.org/10.22108/toc.2021.123661.1739

Ali Zaghian

Department of Mathematics and Cryptography, Malek Ashtar University of Technology, Isfahan, Iran.

Email: a_zaghian@mut-es.ac.ir

Bagher Bagherpour

Department of Mathematics and Cryptography, Malek Ashtar University of Technology, Isfahan, Iran.

Email: bagher.bagherpour@mut-es.ac.ir

http://dx.doi.org/10.22108/toc.2021.123661.1739