Noname manuscript No.
(will be inserted by the editor)

The complexity of the connected graph access structure on seven participants

Massoud Hadian Dehkordi · Ali Safi

Received: date / Accepted: date

Abstract In this paper, we study an important problem in secret sharing that determines the exact value or bound for the complexity. First, we used induced subgraph complexity of the graph G with access structure Γ to obtain a lower bound on the complexity of the graph G. Secondly, by applying decomposition techniques we obtain an upper bound on the complexity of the graph G. We determine the exact values of the complexity for each of the ten graph access structures on seven participants. Also, we improve the value bound of the complexity for the six graph access structures with seven participants.

Keywords Access structure · Complexity · Secret sharing scheme · Connected graph · Induced subgraph

Mathematics Subject Classification (2000) MSC 68R10 · MSC 94A62

1 Introduction

A secret sharing scheme is a method which allows a secret K to be shared among a set of participants P in such a way that only qualified subsets of participants can recover the secret. The first secret sharing schemes considered by Shamir[1] and Blakley[2], in their schemes any proper subset A of participants set P that$|A| \geq t$ can recover the secret K and for every subset A of P that $|A| < t$ no one can obtain any information about the secret. Such schemes called (t, n) −threshold schemes where t is threshold scheme, and n is the size of participants set P.

Massoud Hadian Dehkordi
Department of Mathematics, Iran University of Science & Technology, Tehran, Iran
Tel.: +98-21-77240540
Fax: +98-21-77240479
E-mail: mhadian@iust.ac.ir

Ali Safi
Department of Mathematics, Iran University of Science & Technology, Tehran, Iran

The access structure Γ of a secret sharing scheme defined on P, with secret K, is the collection Γ of subsets of P that are desired to be able to reconstruct the value of K from their pooled shares. In general an access structure Γ on the set P considered to be monotone. This means that if $A \in \Gamma$ and $A \subseteq A' \subset P$ then $A' \in \Gamma$. A subset of P that belongs to Γ, is called a qualified subset and those that do not belong to Γ known as unqualified subset. A minimal qualified subset $A \in \Gamma$ is a subset of participants such that $A' \notin \Gamma$ for all $A' \subset A$. The basis of Γ is the collection of all minimal qualified subsets of P, which is denoted by $[\Gamma]^-$. We will say that a scheme is a perfect secret sharing scheme realizing the access structure Γ provided the following two properties are satisfied [8]:

1. If a qualified subset of participants $A \subseteq P$ pool their shares, then they can determine the value of K.
2. If an unqualified subset of participants $A \subseteq P$ pool their shares, then they can determine nothing about the value of K.

The efficiency of a perfect secret sharing schemes can be assessed in terms of its *complexity*, which is the ratio between the size of the maximum size of the shares given to any participant in P, and the size of the secret. *The complexity of an access structure* Γ, denoted by $\sigma(\Gamma)$, is defined as the infimum of the complexities of all secret sharing schemes with access structure Γ. A perfect secret sharing scheme is called *ideal* if its complexity is equal to one. The graph access structure, is an access structure that contains only minimal qualified subset of cardinality two. The complexity of the graph access structures have been studied in the literature by several authors since the 90s [3–10, 12]. There have been particular endeavours to determine the most efficient secret sharing schemes for all graphs with a small number of vertices. In line with this, there have been obtained lower bounds based on entropy considerations, as well as upper bounds, using a decomposition or weighted decomposition technique for constructing good schemes.

in [3], Jackson and Martin studied the complexity of connected graph access structures on five participants. Van Dijk studied the complexity of the 112 graph access structures on six participants and in 94 cases, determined the exact values of the complexity [4]. With results obtained in [14–16], the complexity in several cases out of 18 cases of secret sharing schemes which remained unsolved for connecting graphs with six participants were determined. in [9, 10], Song and Wang studied the complexity of connected graph access structures on seven participants with six, seven, eight, nine and ten edges. They determined the exact values of the complexity for 189 cases. Also, Song and et. in [12], studied the complexity of the 272 graph access structures on nine participants with eight and nine edges and in 231 cases, determined the exact values of the complexity.

In [9], the complexity of the 111 connected graph access structures on seven participants with six, seven and eight edges are studied among which the exact value of 91 cases are determined and the other cases provided the upper and lower bound. With results obtained in [11], the complexity in four cases out of 20 cases of secret sharing schemes which remained unsolved for connecting graphs with seven participants were determined. In this paper, we obtain the exact value of the complexity to 10 connected graph access structures from the remaining 16 cases by using the following method. First, a six-vertex graph access structure is reached by removing the vertex appropriate to its edges of the seven-vertex graph access structure. Because the complexity of the most six-vertex graph access structures are determined in [4, 14–16], we obtain the lower bound for complexity of the seven-vertex graph access structure. On the other hand, by using decomposition techniques, we get an upper bound equals to the lower bound. In addition to the above method we improve the value bound of the complexity for the six graph access structures with seven participants.

2 Definitions and basic properties

In this section, we introduce definitions and theorems which are used to determine the exact values of the complexity of the connected graph access strucrure with seven vertices.

Theorem 1 *([4]). Let $G = (V, E)$ be a graph with vertices $a, b \in V$. For $d \in V$, ad is an edge iff bd is an edge. Define G' by deleting vertex a and edges ad for all vertices d. Then $\sigma(\Gamma_G) = \sigma(\Gamma_{G'})$.*

Definition 1 Let G be a graph with vertex set V and edge set E. If $V_1 \subseteq V$, then the *induced subgraph* $G[V_1]$ is defined to have vertex set V_1 and edge set $\{vw \in E(G) : v, w \in V_1\}$.

Definition 2 Let G be a connected graph with vertex set V. Suppose that V can be partitioned into subsets $V_1, \ldots, V_n$ such that the edges in G are defined by all pairs of vertices from different subsets. Then G is called a *complete multipartite graph.*

Theorem 2 *([5]). The access structure Γ based on a connected graph G is ideal if and only if G is a complete multipartite graph.*

Theorem 3 *([6]). If G is not multipartite graph then $\sigma(G) \geq \frac{3}{2}$.*

Theorem 4 *([6]). Suppose G is a graph and G' is an induced subgraph of G. Then $\sigma(\Gamma_{G'}) \leq \sigma(\Gamma_G)$.*

Definition 3 ([8]). Suppose Γ is an access structure having basis $[\Gamma]^-$. Let $\lambda \geq 1$ be an integer. A $\lambda-$ *decomposition* of $[\Gamma]^-$ consists of a collection (i.e. a multiset) $\{\Gamma^1, \ldots, \Gamma^t\}$ such that the following properties are satisfied:

1. $\Gamma^h \subseteq [\Gamma]^-$ for $1 \leq h \leq t$.
2. For each $A \in [\Gamma]^-$, there exist λ indices $1 \leq i_1 < \cdots < i_\lambda \leq t$ such that $A \in \Gamma^{i_j}$ for $1 \leq j \leq \lambda$.

Theorem 5 *([8]). Let $P = \{P_i : 1 \leq i \leq n\}$ be the set of n participants and Γ be an access structure having basis $[\Gamma]^-$. If the collection $\left\{\Gamma^1, \ldots, \Gamma^t\right\}$ be a $\lambda -$ decomposition of $[\Gamma]^-$ such that for $1 \leq h \leq t$, Γ^h is ideal and*

$$R = \max\{|\{h : p_i \in P_h\}| : 1 \leq i \leq n\}$$

then $\sigma(\Gamma) \leq \frac{R}{\lambda}$.

Example 1 The 2-decomposition for the graph Γ_{12} shown in Figure 1. According to Theorem 5, we have $\sigma(\Gamma) \leq \frac{3}{2}$.

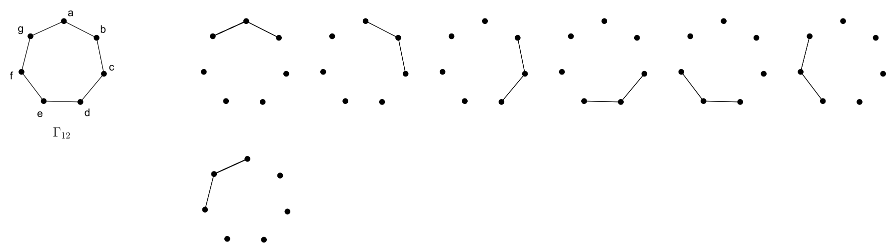


Fig. 1 The 2-decomposition for the graph Γ_{12}.

Definition 4 ([14]) A weighted access structure for a secret sharing scheme, denoted by Γ_w, is a set $\left\{(X, W(X)) |\, W(X) \geq 0, W(X) \in Z, X \in 2^P\right\}$. The weight of Γ_w is defined by $W(\Gamma_w) = max\left\{W(X) |\, X \in 2^P\right\}$.

A secret sharing scheme for a weighted access structure Γ_w is a method which allows $W(\Gamma_w)$ secrets of the same size to be shared among a set of participants P in such a way that each subset of participants, X, can exactly recover $W(X)$ secrets out of the $W(\Gamma_w)$ secrets. It is obvious that if $X \subseteq X' \subseteq P$, then $W(X) \leq W(X')$.

Consider a weighted graph $G(V, E)$ with weights $W_e(G)$ $(W_e(G) \geq 1)$ and $W(G) = \max\{W_e(G) \,|e \in E\}$ for $e \in E$, is a perfect secret shrring scheme which satisfies the following requirements:

1. Any pair of participants corresponding to an edge e of G can obtain $W_e(G)$ secrets out of the $W(G)$ secrets.
2. Any subset of participants containing no edge of G has no information on the $W(G)$ secrets.

Example 2 Consider the weighted graph G that is showen in Figure 2, later on given the perfect secret sharing scheme for it, assume the secret $s = (s_1, s_2)$ is selected randomly from $(GF(q))^2$, where q is a prime number.

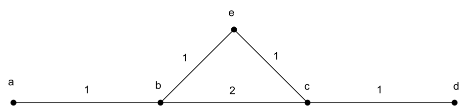


Fig. 2 Graph G.

The shares are given as follows:

$$\begin{aligned} &a : (r_2), \\ &b : (r_2 + s_2, r_1), \\ &c : (r_1 + s_1, r_2), \\ &d : (r_1), \\ &e : (r_1 + r_2), \end{aligned}$$

where r_1 and r_2 are selected randomly from $(GF(q))$ and all operations are calculated at $(GF(q))$. The sets $\{a, b\}, \{c, d\}, \{b, e\}, \{c, e\}$ obtain s_2, s_1, s_2 and s_1 respectively. Also, participants set $\{b, c\}$ can obtain the secrets s_1 and s_2.

Definition 5 ([14]). Suppose Γ is an access structure. A $\lambda-$*weighted decomposition* of Γ consists of a collection $\left\{\Gamma^1, \dots, \Gamma^t\right\}$ such that the following requirements are satisfied.

1. Each Γ^h is a weighted access structure, for $1 \leq h \leq t$.
2. For each $X \in \Gamma$,there exists some indices, say $i_1 < \cdots < i_k$, such that $\sum_{i_j} W\left(X; \Gamma^{i_j}\right) \geq \lambda$, where $W\left(X; \Gamma^{i_j}\right)$ is the weight of X in Γ^{i_j}, for $1 \leq j \leq k$.
3. For each $X \notin \Gamma$, $\sum_{h=1}^{t} W\left(X; \Gamma^h\right) = 0$.

Theorem 6 *([14]). WDC for graph. Let G be a graph of access structure on n participants, and suppose that $\left\{G^1, \dots, G^t\right\}$ is a $\lambda-$weighted decomposition of G. Assume that for each weighted graph G^h, $1 \leq h \leq t$ there exists a perfect secret sharing scheme with complexity σ_{ih} for each $p_i \in P_h$. Then, there exists a perfect secret sharing scheme for G with complexity*

$$\sigma\left(\Sigma\right) = \max\left\{\frac{\sum_{\{h: p_i \in P_h\}} W\left(G^h\right)\sigma_{ih}}{\lambda} : 1 \leq i \leq n\right\}.$$

Example 3 The weighted decomposition construction for the graph Γ_{106} with seven participants is shown in Figure 3.

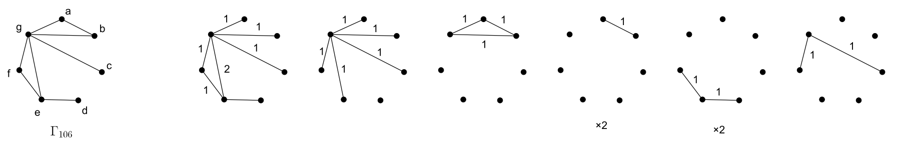


Fig. 3 3-weighted decomposition for the graph Γ_{106}.

So, the secret sharing scheme for Γ_{106} is setup as follows. Let the secret $K = (K_1, K_2, K_3)$ be taken randomly from $(GF(q))^3$, where q is a prime power. Let $f(x) = K_1 + K_2 x + K_3 x^2 \pmod{q}$. The value $y_i s$ computed from $f(x)$ are as follows: $y_i = f(i) \pmod{q}$, for $i = 1, \ldots, 9$. It is clear that given four $y_i s$, $f(x)$ can be determined uniquely, and hence, the secret K can be recovered. On the contrary, one who does not have any knowledge of these $y_i s$ obtains no information on the secret K. The shares for a, b, c, d, e, f, g are assigned as follow:

$$
\begin{aligned}
&S_a : (r_2, r_3, r_4 + y_4, r_5 + y_5, r_6)\\
&S_b : (r_2, r_3, r_4 - y_4, r_5 +, r_6 + y_6)\\
&S_c : (r_2, r_3, r_9)\\
&S_d : (r_1, r_7, r_8)\\
&S_e : (r_1 + y_1, r_2, r_3, r_7 + y_7, r_8 + y_8)\\
&S_f : (r_1 + r_2, r_3, r_7, r_8, r_9)\\
&S_g : (r_1, r_2 + y_2, r_3 + y_3, r_4, r_9 + y_9)
\end{aligned}
$$

Thus,

$$
\begin{aligned}
&\{a, b\} \text{ can recover } y_4, y_5, y_6,\\
&\{a, g\} \text{ can recover } y_2, y_3, y_4,\\
&\{b, g\} \text{ can recover } y_2, y_3, y_4,\\
&\{c, g\} \text{ can recover } y_2, y_3, y_9,\\
&\{d, e\} \text{ can recover } y_1, y_7, y_8,\\
&\{e, f\} \text{ can recover } y_1, y_7, y_8,\\
&\{e, g\} \text{ can recover } y_1, y_2, y_3,\\
&\{f, g\} \text{ can recover } y_2, y_3, y_9,
\end{aligned}
$$

Therefore, all above pairs can obtain three $y_i s$, and they can recover the secret K. On the contrary, no other pair can obtain any information on $y_i s$. It is clear that the complexity for these shares are $\sigma_a = \frac{5}{3}, \sigma_b = \frac{5}{3}, \sigma_c = 1, \sigma_d = 1, \sigma_e = \frac{5}{3}, \sigma_f = \frac{5}{3}$ and $\sigma_g = \frac{5}{3}$. Hence, the complexity for the constructed secret sharing scheme is $\frac{5}{3}$. Thus, According to the definition of the complexity of the access structure, we have $\sigma(\Gamma_{106}) \leq \frac{5}{3}$.

3 The results

The purpose of this section is to determine the exact value of the complexity of the following graph access structures with seven participants $P = \{a, b, c, d, e, f, g\}$:

$[\Gamma_{12}]^- = \{ab, ag, bc, cd, de, ef, fg\}$, $[\Gamma_{43}]^- = \{ab, af, ag, bc, bf, de, ef\}$,
$[\Gamma_{47}]^- = \{ab, af, ag, bf, bc, cd, de, ef\}$, $[\Gamma_{60}]^- = \{ab, af, ag, be, cd, de, ef, fg\}$,
$[\Gamma_{65}]^- = \{ab, ag, bc, bd, bf, df, ef, fg\}$, $[\Gamma_{70}]^- = \{ab, ac, bc, cd, cg, de, ef, fg\}$,
$[\Gamma_{83}]^- = \{ab, ag, cd, de, df, dg, ef, fg\}$, $[\Gamma_{85}]^- = \{ab, bc, cd, cf, cg, de, df, fg\}$,
$[\Gamma_{106}]^- = \{ab, ag, bg, cg, de, ef, eg, fg\}$, $[\Gamma_{108}]^- = \{ab, ad, ag, bc, bd, de, df, ef\}$,

and improve the value bound of the complexity of the following graph access structures with seven participants $P = \{a, b, c, d, e, f, g\}$:

$[\Gamma_{61}]^- = \{ab, ae, ag, bc, be, cd, de, ef\}$, $[\Gamma_{62}]^- = \{ab, af, ag, bc, cd, cf, ef, fg\}$,
$[\Gamma_{63}]^- = \{ab, ag, bc, bg, cd, cf, ef, fg\}$, $[\Gamma_{64}]^- = \{ab, ac, ag, ce, cf, de, ef, fg\}$,
$[\Gamma_{68}]^- = \{ab, af, ag, bc, be, cd, df, ef\}$, $[\Gamma_{94}]^- = \{ab, bc, bg, cd, ce, cg, ef, eg\}$.

The lower bound and upper bound obtained for the complexity of the above graph access structures are listed in table 1. see[9]

Γ_i	$\sigma(\Gamma_i)$	Γ_i	$\sigma(\Gamma_i)$	Γ_i	$\sigma(\Gamma_i)$	Γ_i	$\sigma(\Gamma_i)$
Γ_{12}	$\frac{3}{2} \sim \frac{11}{7}$	Γ_{43}	$\frac{5}{3} \sim 2$	Γ_{47}	$\frac{5}{3} \sim 2$	Γ_{60}	$\frac{5}{3} \sim 2$
Γ_{61}	$\frac{5}{3} \sim 2$	Γ_{62}	$\frac{3}{2} \sim 2$	Γ_{63}	$\frac{5}{3} \sim 2$	Γ_{64}	$\frac{5}{3} \sim 2$
Γ_{65}	$\frac{5}{3} \sim 2$	Γ_{68}	$\frac{3}{2} \sim 2$	Γ_{70}	$\frac{5}{3} \sim 2$	Γ_{83}	$\frac{5}{3} \sim 2$
Γ_{85}	$\frac{5}{3} \sim 2$	Γ_{94}	$\frac{5}{3} \sim 2$	Γ_{106}	$\frac{3}{2} \sim 2$	Γ_{108}	$\frac{5}{3} \sim 2$

Table 1: Upper and lower bounds provided for the complexity of the 16 remaining access structure in [9].

For seven-vertex graph access structure Γ_{12}, from Theorem 3, we can get the lower bound of $\sigma(\Gamma_{12})$ to be $\frac{3}{2}$, and with using 2-decomposition in the provided example 1, we get the upper bound for $\sigma(\Gamma_{12})$ is equal to $\frac{3}{2}$, so $\sigma(\Gamma_{12}) = \frac{3}{2}$.

For the seven-vertex graph access structures Γ_{43} and Γ_{47} by removing the vertex d and edges connected to it, we get the six-vertex graph access structure Γ_9 with the exact value of complexity is $\frac{7}{4}$[14]. Theorem 4, implies that the lower bound of $\sigma(\Gamma_{43})$ and $\sigma(\Gamma_{47})$ are at least $\frac{7}{4}$. Theorem 6 together with 4-weighted decomposition in the appendix, imply the upper bound for $\sigma(\Gamma_{43})$ and $\sigma(\Gamma_{47})$ are equal to $\frac{7}{4}$, then $\sigma(\Gamma_{43}) = \sigma(\Gamma_{47}) = \frac{7}{4}$.

We remark that the result for Γ_{43}, can be obtained by using of the complexity graph access structure with nine-vertex Γ_{257} or Γ_{268} in [12] and Theorem 1. We can see that $\sigma(\Gamma_{43}) = \frac{7}{4}$.

For the seven-vertex graph access structure by removing the vertex c in Γ_{60}, we can obtain the six-vertex graph access structure Γ_{31} that $\sigma(\Gamma_{31}) = \frac{5}{3}$, [4]. For the seven-vertex graph access structure by removing the vertex a in Γ_{70}, we can recived the six-vertex graph access structure Γ_{18} that $\sigma(\Gamma_{18}) = \frac{5}{3}$, [4]. We conclude that the complexity of Γ_{60} and Γ_{70} are at least $\frac{5}{3}$. Using 3-decomposition in the appendix and from Theorem 5, we can get the upper bound for $\sigma(\Gamma_{60})$ and $\sigma(\Gamma_{70})$ are equal to $\frac{5}{3}$, then $\sigma(\Gamma_{60}) = \sigma(\Gamma_{70}) = \frac{5}{3}$.

Removing the vertex c from the seven-vertex graph access structure Γ_{65} and removing the vertex d and its connected edges from Γ_{106}, we get the six-vertex graph access structures Γ_{33} and Γ_{25} respectively, with exact complexity value of $\frac{5}{3}$, [4]. Theorem 4 implies that the lower bound for Γ_{65} and Γ_{106} are $\frac{5}{3}$. Using of the Theorem 6 and 3-weighted decomposition in the appendix and in the provided example 3, we get the upper bound for $\sigma(\Gamma_{65})$ and $\sigma(\Gamma_{106})$ are equal to $\frac{5}{3}$, then $\sigma(\Gamma_{65}) = \sigma(\Gamma_{106}) = \frac{5}{3}$.

For the seven-vertex graph access structure Γ_{83} with removing vertex b and for Γ_{85} removing vertex a and its connected edges, we can get to the six-vertex graph access structure Γ_{22} that $\sigma(\Gamma_{22}) = \frac{7}{4}$. For the seven-vertex graph access structure Γ_{108} with removing vertex e and its connected edges, we can get to the six-vertex graph access structure Γ_9 that $\sigma(\Gamma_9) = \frac{7}{4}$, [14, 15]. From Theorem 4, we conclude that the lower bound for $\sigma(\Gamma_{83})$, $\sigma(\Gamma_{85})$ and $\sigma(\Gamma_{108})$ are $\frac{7}{4}$. With use of the Theorem 6 and 4-weighted decomposition in the appendix, we obtain the upper bound for $\sigma(\Gamma_{83})$, $\sigma(\Gamma_{85})$, $\sigma(\Gamma_{108})$ be $\frac{7}{4}$, then $\sigma(\Gamma_{83}) = \sigma(\Gamma_{85}) = \sigma(\Gamma_{108}) = \frac{7}{4}$.

For the seven-vertex graph access structures by removing the vertex d in Γ_{61} and vertex f in Γ_{94}, we can in order to obtain the six-vertex graph access structures Γ_9 and Γ_{22} that $\sigma(\Gamma_9) = \sigma(\Gamma_{22}) = \frac{7}{4}$, [13,15]. Theorem 4 implies the complexity of Γ_{61} and Γ_{94} are at least $\frac{7}{4}$. Using 8-weighted decomposition in the appendix and from Theorem 6, we can get the upper bound for $\sigma(\Gamma_{61})$ and $\sigma(\Gamma_{94})$ are equal to $\frac{15}{8}$.

Removing the vertex e from the seven-vertex graph access structures Γ_{62} and removing the vertex f and its connected edges from Γ_{68}, we get the six-vertex graph access structures Γ_{31} and Γ_4 respectively, with exact complexity value of $\frac{5}{3}$, [4]. Theorem 4 implies that the lower bound for Γ_{62} and Γ_{68} are $\frac{5}{3}$. Using of the Theorem 6 and 4-weighted decomposition in the appendix for Γ_{62} and Theorem 5 and 4-decomposition in the appendix for Γ_{68}, we get the upper bound for $\sigma(\Gamma_{62})$ and $\sigma(\Gamma_{68})$ are equal to $\frac{7}{4}$.

For the seven-vertex graph access structure by removing the vertex d in Γ_{63}, we can obtain the six-vertex graph access structure Γ_{31} that $\sigma(\Gamma_{31}) = \frac{5}{3}$, [4]. Theorem 4 implies the complexity of Γ_{63} is at least $\frac{5}{3}$. Using 8- decomposition in the appendix and from Theorem 5, we can get the upper bound for $\sigma(\Gamma_{63})$ is equal to $\frac{15}{8}$.

Removing the vertex d from the seven-vertex graph access structure Γ_{64}, we get the six-vertex graph access structure Γ_{31}, with exact complexity value of $\frac{5}{3}$, [4]. Theorem 4 implies that the lower bound for Γ_{64} is equal to $\frac{5}{3}$. Using of the Theorem 6 and 4-weighted decomposition in the appendix for Γ_{64}, we get the upper bound for $\sigma(\Gamma_{64})$ is equal to $\frac{7}{4}$.

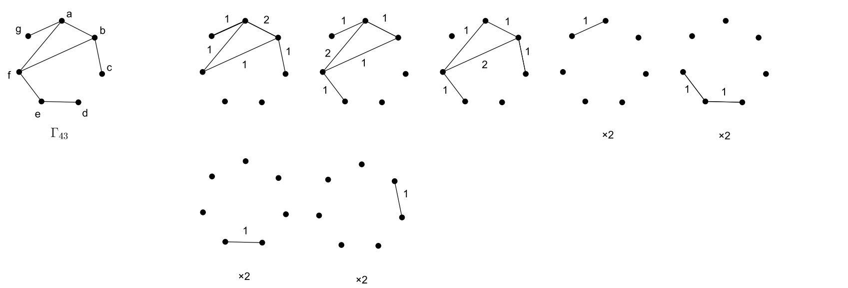
The results are given in Table 2.

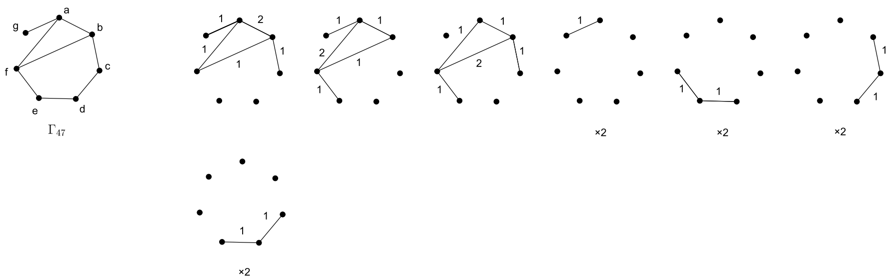
Γ_i	$\sigma(\Gamma_i)$	Γ_i	$\sigma(\Gamma_i)$	Γ_i	$\sigma(\Gamma_i)$	Γ_i	$\sigma(\Gamma_i)$
Γ_{12}	$\frac{3}{2}$	Γ_{43}	$\frac{7}{4}$	Γ_{47}	$\frac{7}{4}$	Γ_{60}	$\frac{5}{3}$
Γ_{61}	$\frac{7}{4} \sim \frac{15}{8}$	Γ_{62}	$\frac{5}{3} \sim \frac{7}{4}$	Γ_{63}	$\frac{5}{3} \sim \frac{15}{8}$	Γ_{64}	$\frac{5}{3} \sim \frac{7}{4}$
Γ_{65}	$\frac{5}{3}$	Γ_{68}	$\frac{5}{3} \sim \frac{7}{4}$	Γ_{70}	$\frac{5}{3}$	Γ_{83}	$\frac{7}{4}$
Γ_{85}	$\frac{7}{4}$	Γ_{94}	$\frac{7}{4} \sim \frac{15}{8}$	Γ_{106}	$\frac{5}{3}$	Γ_{108}	$\frac{7}{4}$

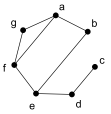
Table 2: The obtained results.

Remark: We point out that our results can be applied for some graph access structures of nine participants with equal or more than 10 edges, by using Theorem 1.

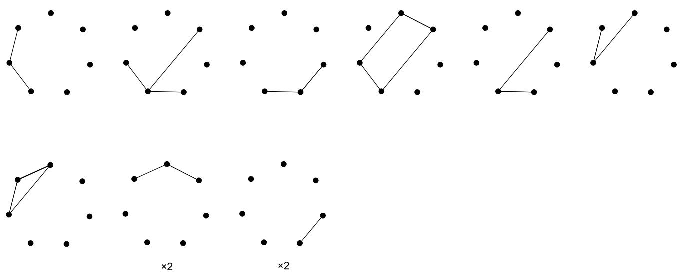
Appendix

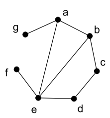




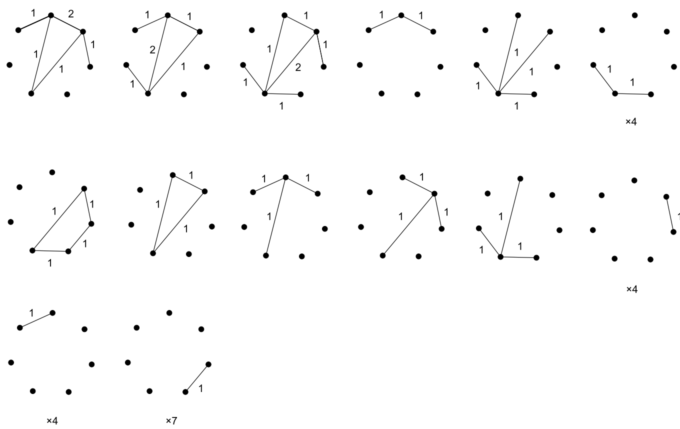


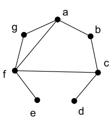
Γ_{60}



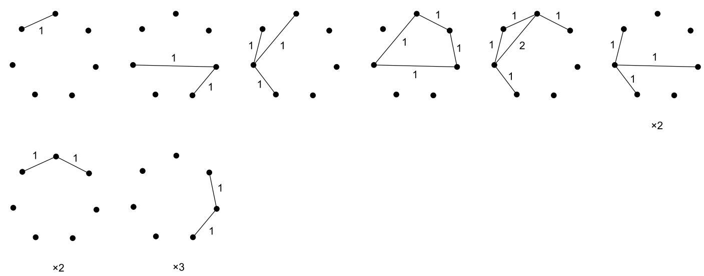


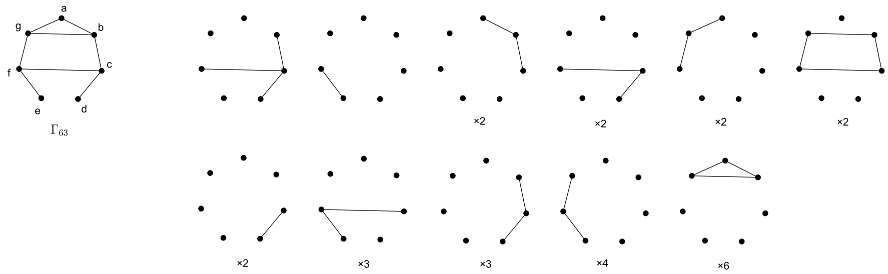
Γ_{61}



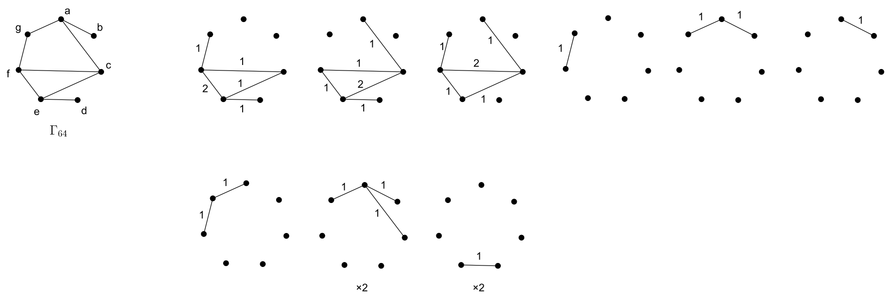


Γ_{62}

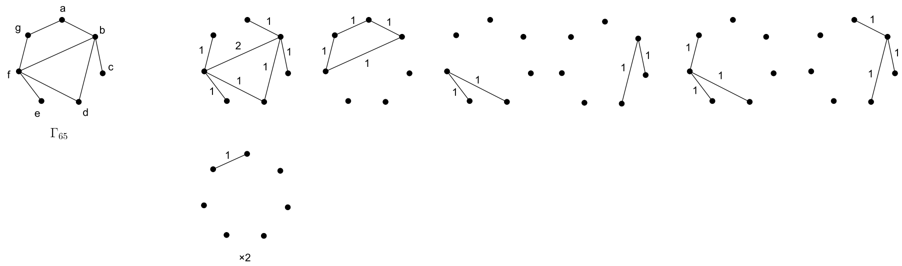




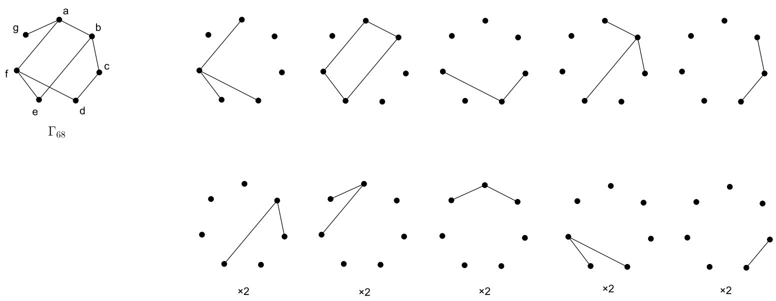
Γ_{63}



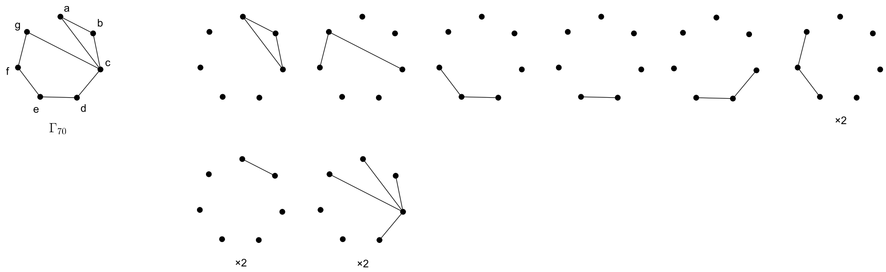
Γ_{64}



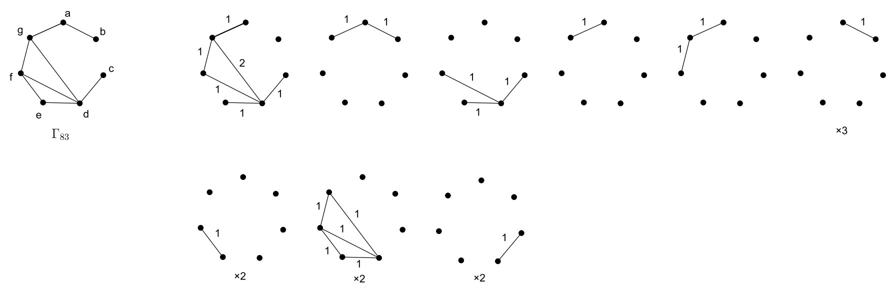
Γ_{65}



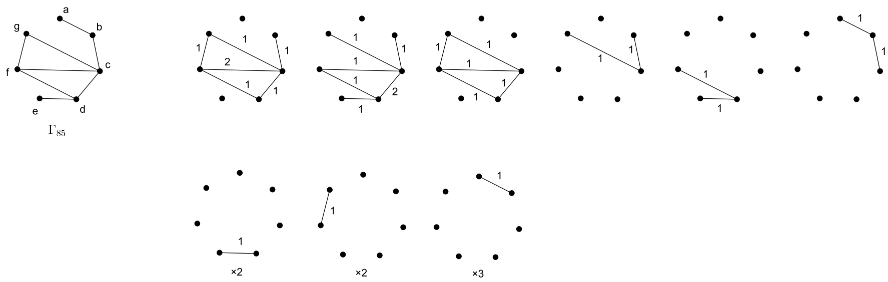
Γ_{68}

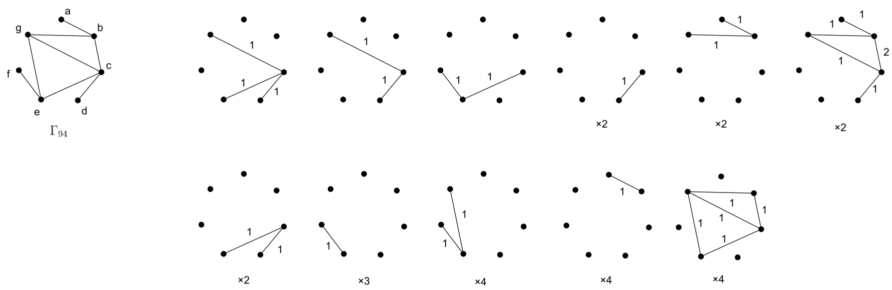


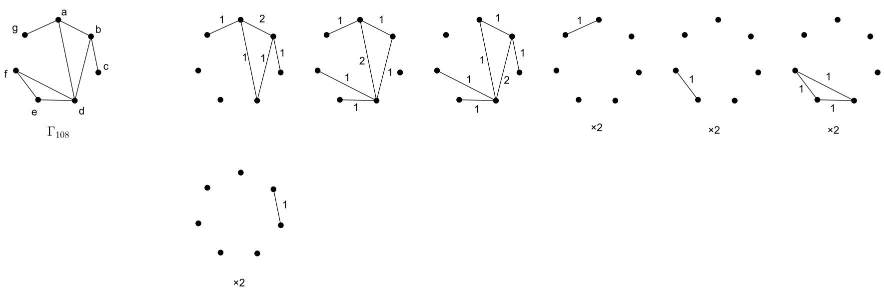
Γ_{70}



Γ_{83}







Acknowledgements The authors would like to thank the anonymous for the enlightening elements.

References

1. A. Shamir, *How to share a secret*, J. Communications of the ACM, **22** (1979), 612–613.
2. G. R. Blakley, *Safeguarding cryptographic keys*, in “Proc. of National Computer Conference”, (1979), 313–317.
3. J. Wen-Ai, K. M. Martin, *Perfect secret sharing schemes on five participants.*, in “ Des. Codes Cryptogr,” **9** no. **3** (1996): 267-286.

4. M. Van Dijk, "Secret key sharing and secret key generation," Ph.D thesis, Eindhoven University of Technology in Eindhoven, (1997).
5. E. F. Brickell, D. M. Davenport, *On the classification of ideal secret sharing schemes*, J. Cryptol, **4** (1991), 123–134.
6. C. Blundo, A. De Santis, D. R. Stinson, U. Vaccaro, *Graph decompositions and secret sharing schemes*, J. Cryptol, **8** (1995), 39–64.
7. E. F. Brickell, D. R. Stinson, *Some improved bounds on the information rate of perfect secret sharing schemes*, J. Cryptol , **5** (1992), 153–166.
8. D. R. Stinson, *Decomposition constructions for secret-sharing schemes*, IEEE Transactions on Information Theory, **40** (1994), 118–125.
9. Y. Song, Z. Li, W. Wang, *The Information Rate of Secret Sharing Schemes on Seven Participants by Connected Graphs*, Lecture Notes in Electrical Engineering, (2012), **40**: 637–645
10. W. Wang, Z. Li, Y. Song *The optimal information rate of perfect secret sharing schemes.*, in: Proceedings of the 2011 International Conference on Business Management and Electronic Information, (2011), 207–212.
11. Z. H. Li, Y. Song, Y. M. Li, *The Optimal Information Rates of the Graph Access Structures on Seven Participants*, Advanced Materials Research, (2014), Vol. **859**, 596–601.
12. Y. Song, Z. Li, Y. Li, R. Xin, *The optimal information rate for graph access structures of nine participants.*, Frontiers of Computer Science, **9** no. **5** (2015): 778-787.
13. L. Csirmaz, *An impossibility result on graph secret sharing*, Des. Codes Cryptogr, **53** (2009), 195–209.
14. H. M. Sun, B. L. Chen, *Weighted decomposition construction for perfect secret sharing schemes*, Comput. Math. Appl, **43** (2002), 877–887.
15. M. Gharahi, M. Hadian Dehkordi, *The complexity of the graph access structures on six participants*, Des. Codes Cryptogr, **67** (2013), 169–173.
16. P. Carles, L. Vzquez, *Finding lower bounds on the complexity of secret sharing schemes by linear programming*, LATIN 2010: Theoretical Informatics, Springer Berlin Heidelberg, (2010), 344–355.