# The complexity of the graph access structures on seven participants

**M. Davarzani**
*Faculty of Mathematics and Computer Science*
*Kharazmi University*
*Tehran*
*Iran*
*mahmood.davarzani@gmail.com*

**Abstract.** In this paper, we deal with determining the values for the complexity of the graph access structures on seven participants. As [10], it was determined exact values of the 91 of the complexities of access structures. In this paper we give simple proof by entropy and shannon inequalities for determining the lower bound of complexity which used for determining of lower bound of the 51 graph access structure. Further, we establish the exact values of the complexity of five graphs, which remained as open problems in [10]. Also we obtain the tight bounds for complexity of five access structures.

**Keywords:** Perfect secret sharing scheme, Complexity, Entropy method, Graph access structures.

## 1. Introduction

A secret sharing scheme is a method for sharing a secret among a set $P$ of participants, by distributing the share relating to the secret among them, in such a way that only certain *qualified subsets* of participants are able to recover the secret from their shares. The secret sharing scheme is called *perfect* if any non-qualified subsets of participants cannot obtain any information about the secret.

The *access structure* $\Gamma$ is the collection of all subsets of $P$ that are qualified to reconstruct the secret. A subset $A \in \Gamma$ is called *minimal qualified subset* of $P$, if for every $B \in \Gamma, B \subseteq A$ implies $B = A$. The collection of all minimal qualified subsets of $P$ is denoted by $[\Gamma^-]$, which is called the basis of $\Gamma$. The *complexity* of secret sharing scheme is the ratio between the maximum size of the shares given to any participant in $P$, and the size of the secret. The complexity of an access structure $\Gamma$, denoted by $\sigma(\Gamma)$, is defined as the infimum of the complexities of all secret sharing schemes with access structure $\Gamma$.

The graph access structure on a set $P$ of participants is an access structure that contains only minimal qualified subsets of cardinality two. The complexity for the graph access structures have been considered in several papers, such as [1, 2, 3, 4, 6, 8, 11, 13, 14]. Van Dijk studied the complexity of the 112 graph access structures on six participants. He determined the exact values of complexity in 94 cases [14]. Subsequently in [13], Sun and Chen improved the known upper bound and in [6], Gharahi and Dehkordi established the exact values of complexity for five the graph access structures which remained unsolved in Van Dijk paper. Recently, Padro and Vazquez presented lower bound of complexity by resorting to linear programming approch [9]. The complexity of the graph access structures on seven participants have been studied in [10]. Yun Song, Zhihui Li and Weicong Wang in [10], compute the complexity of the graph access structures of 111 connected graphs that have six, seven and eight vertices and in 91 cases, determined the exact values of the complexity. In this paper, we give a simple and different proof of their results and obtain the exact values of the complexity of five the graph access structures. We also introduce new decompositions which improves the upper bound of complexity of five the access structures.

## 2. Definitions and basic properties

We give a definition of a perfect secret sharing in terms of *shannon entropy*, as in [4].

Consider two sets of random variables $X$ and $Y$, the shannon entropy function $H$ satisfied the following properties

1. *non-negativity*, i.e., $H(X) \geq 0$,
2. *monotonicity*, i.e., if $X \subseteq Y$ then $H(Y) \geq H(X)$,
3. *submodularity*, i.e., $H(x) + H(Y) \geq H(X \cup Y) + H(X \cap Y)$.

The information inequalities that can be obtained from the above inequalities are called *Shannon inequalities.* In any secret sharing scheme, there is one random variable, denoted by S, for the secret and, for each participant $p \in P$, there is one random variable for the share given to $p$. We denote the joint distribution of the shares given to the participants in $X \subseteq P$ by X. A *perfect secret sharing scheme* with the access structure $\Gamma$ is a sharing of the secrets in $S$ among a set $P$ of participants in such a way that:

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

Let $\Sigma$ is a secret sharing scheme for the access structure $\Gamma$ and the set of secrets $S$. The *complexity* of $\Sigma$ is defined by

$$\sigma(\Sigma) = \frac{\max_{p \in P} H(p)}{H(s)}$$

and the *complexity* of an access structure $\Gamma$ is defined as

$$\sigma(\Gamma) = \inf_{\Sigma} \sigma(\Sigma),$$

where the infimum is taken over all secret sharing schemes realizing $\Gamma$. For each important participant $p \in P$, $H(s) \leq H(p)$ [1], so $\sigma(\Gamma) \geq 1$. The access structure with complexity equal to one is called *ideal*. Throughout this paper only perfect secret sharing schemes are considered. The following thorem is obvious [1].

**Theorem 2.1.** *Let $\Gamma$ be an access structure on $P$ and let $\Gamma'$ be an induced subset of $\Gamma$, i.e., for some subset $P' \subseteq P$*

$$\Gamma' = \{X : X \in \Gamma, X \subseteq P'\}.$$

*Then $\Gamma'$ is an access structure on $P'$. And, if there exists a perfect secret sharing scheme for $\Gamma$ and secret set $S$ with complexity $\sigma$ then this scheme is also a perfect secret sharing scheme for $\Gamma'$ and $S$ having complexity at most equal to $\sigma$.*

In graph access structure all minimal qualified subsets have exactly two different participants. When the access structure $\Gamma$ is based on a connected graph $G$, then the participants and the minimal qualified subsets are corresponding to the vertices and the edges of the graphs $G$, repectively. From 2.1 we immediately obtain:

**Corollary 2.2.** *Suppose $G$ is a graph and $G'$ is an induced subgraph of $G$. Then $\sigma(G) \geq \sigma(G')$.*

**Theorem 2.3** ([3])**.** *The access structure $\Gamma$ based on a connected graph $G$ is ideal if and only if $G$ is a complete multipartite graph.*

From the following theorem as in [14], we can determine the complexity of graph access structures on seven participants by the complexity of graph access structure is known on six participants.

**Theorem 2.4.** *Let $G$ be a graph with vertices $A$ and $B$ such that $AD$ is an edge iff $BD$ is an edge for all vertices $D$. Define $G'$ by deleting edges $AD$, for all vertices $D$, and by deleting vertex $A$. Then $\sigma(G) = \sigma(G')$.*

Since the complexity of graph access structures is known for graphs on six participants [10, 6, 14], we can obtain the exact value of complexity 55 graph with seven participants [10].

## 3. The upper bound of the complexity

To drive the upper bound on the complexity of access structure $\Gamma$, we apply $\lambda$-decomposition technique from [12]. Let $\Gamma$ be an access structure having basis $[\Gamma]^-$ and $\lambda \geq 1$, a $\lambda$-decomposition of $[\Gamma]^-$ consist of set $\{\Gamma^1, \cdots, \Gamma^t\}$ such that the following properties are satisfied:

1. $\Gamma^h \subseteq [\Gamma]^-$ for $1 \leq h \leq t$.

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

For $1 \leq h \leq t$, define $P_h = \bigcup_{B \in \Gamma^h} B$; $P_h$ denotes the set of participants in scheme with access structure $[\Gamma]^-$.

**Theorem 3.1** ([12]). *Let $\Gamma$ be an access structure on $n$ participants, having basis $[\Gamma]^-$ and suppose that $\{\Gamma^1, \cdots, \Gamma^t\}$ is a $\lambda$-deocomposition of $[\Gamma]^-$. Let for every $\Gamma^h (1 \leq h \leq t)$, there exist a secret sharing scheme with complexity $\sigma_{ih}$ that $p_i \in P_h$, then there exist a secret sharing scheme $\Sigma$ with access structure $\Gamma$ where*

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

**Corollary 3.2** ([12]). *Let $\Gamma$ be an access structure on $n$ participants and suppose that $\{\Gamma^1, \cdots, \Gamma^t\}$ is a $\lambda$-decomposition of $[\Gamma]^-$ such that for every $1 \leq h \leq t$, $\Gamma^h$ is ideal. If $R = \max\{|h : p_i \in P_h| : 1 \leq i \leq n\}$ then $\sigma(\Gamma) \leq \frac{R}{\lambda}$.*

## 4. The lower bound of the complexity

To derive the lower bound on the complexity of access structure $\Gamma$, we use entropy method as described in [1]. First, we state the following lemma which will be used in this section.

**Lemma 4.1** ([5]). *Let $\Gamma$ be an access structure on a set $P$ of participants, then*

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

$$H(A) + H(B) \geq H(A \cup B) + H(A \cap B) + H(S).$$

Now we prove the following theorem which will be needed when we obtain the lower bound on the complexity. As in [10], they proved the following theorem by concepts of information theory, but we only use 4.1 and submodularity of $H$.

**Theorem 4.2.** *Let $\Gamma$ be a graph access structure on a set of participants $P = \{a, b, c, d, e, f\}$ such that $ab, bd, de, df, fc \in \Gamma$ and $ef, ec, eb, ea, fb, fa \notin \Gamma$. Then $\sigma(\Gamma) \geq \frac{5}{3}$.*

**Proof.** From 4.1, we obtain

$$\begin{aligned}
H(ed) + H(bd) &\geq H(ebd) + H(d) + H(S)\\
H(ed) + H(df) &\geq H(edf) + H(d) + H(S)\\
H(ebdf) &\geq H(ebf) + H(S)\\
H(efc) &\geq H(ec) + H(S)\\
H(eabf) &\geq H(eaf) + H(S)
\end{aligned}$$

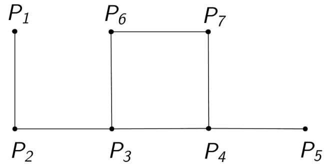
and by the submodularity of $H$, we have

$$\begin{array}{rcl} H(ef)+H(ec) & \geq & H(efc)+H(e) \\ H(ebd)+H(edf) & \geq & H(ebdf)+H(ed) \\ H(ebf)+H(eaf) & \geq & H(eabf)+H(ef) \\ H(e)+H(d) & \geq & H(ed) \\ H(b)+H(d) & \geq & H(bd) \\ H(d)+H(f) & \geq & H(df). \end{array}$$

By adding the above inequalities, we get $H(b)+H(d)+H(f) \geq 5H(S)$. □

From 4.2 and 2.2, we can obtain the lower bound of $\frac{5}{3}$ for 51 graph access structures on seven participants that have six, seven and eight edges, as given in [10].

**Example 4.3.** Suppose $\Gamma_{20}$ is the access structure of the following graph:



By using Theorem 4.2, with $a = P_2, b = P_3, c = P_6, d = P_4, e = P_5, f = P_7$, we conclude that the complexity of $\Gamma_{20}$ is at least $\frac{5}{3}$.

As in [6], we give the following theorem which will be need when we obtain the lower bounds on the complexity.

**Theorem 4.4** ([6])**.** *Let $\Gamma$ be a graph access structure on a set participants $P = \{a, b, c, d, e, f\}$ such that $ab, ac, ad, cd, cf, de \in \Gamma$ and $bc, bd, be, ce, bf, ef \notin \Gamma$ then $\sigma(\Gamma) \geq \frac{7}{4}$.*

In [10], authors calculated the complexity of 111 graph access structures and obtained the exact values of 91 connected graphs. They showed $\frac{5}{3} \leq \sigma(\Gamma_i) \leq 2$ for $i = 44, 79, 80, 83, 85$. Here we consider the problem of determining the exact values for the complexity of the graph access $\Gamma_{44}, \Gamma_{79}, \Gamma_{80}$, $\Gamma_{83}$ and $\Gamma_{85}$.

**Example 4.5.** The complexity is $\frac{7}{4}$ for each of the access structures $\Gamma_{44}, \Gamma_{79}, \Gamma_{80}$, $\Gamma_{83}$ and $\Gamma_{85}$.

**Proof.** We consider the following lables on the access structures of $\Gamma_{44}, \Gamma_{79}, \Gamma_{80}$, $\Gamma_{83}$ and $\Gamma_{85}$.

By using Theorem 4.4 and Corollary 2.2, we have $\sigma(\Gamma_i) \geq \frac{7}{4}$ for $i = 44, 79, 80, 83, 85$. H. Sun and B. Chen, in [13], by weighted decomposition, proved that $\sigma(\Gamma_{44}) \leq \frac{7}{4}$.

For $\Gamma_{79}$, by 2.4, we can delete edge $ag$ and then consider the following 2-decomposition:

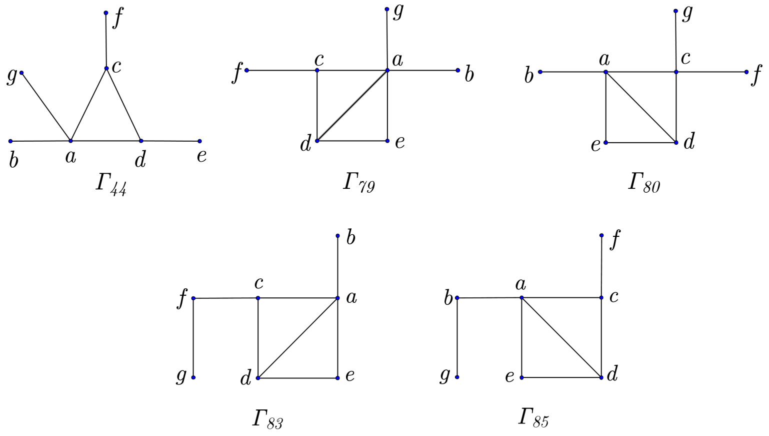


Figure 1: Lables on the access structures

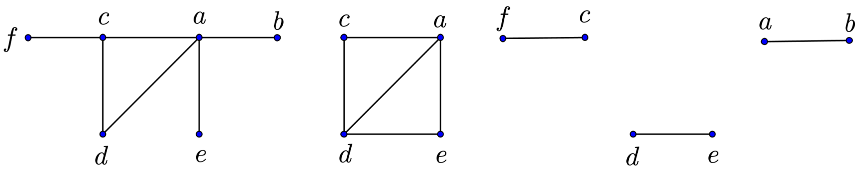


Figure 2: 2− decomposition of $\Gamma_{79}$

Now, by 3.1, we have $\sigma(\Gamma_{79}) \leq \frac{7}{4}$.

For the complexity of $\Gamma_{80}$, by 2.4, we can delete edge $cg$ and then consider the following 2-decomposition:

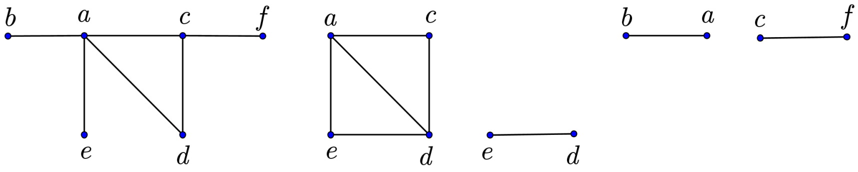


Figure 3: 2− decomposition of $\Gamma_{80}$

And by 3.1, we have $\sigma(\Gamma_{80}) \leq \frac{7}{4}$.

For the complexity of $\Gamma_{83}$ and $\Gamma_{85}$ we consider the following decompositions:

Now, by 3.1, we have $\sigma(\Gamma_i) \leq \frac{7}{4}$ that $i = 83, 85$. □

In [10], authors proved that $\frac{5}{3} \leq \sigma(\Gamma_i) \leq 2$ for $i = 43, 47, 60, 61$ and $93$, which the lower bound was obtained from Theorem 4.2. Here, for each of these access structures, we obtain tight bounds of the complexity.

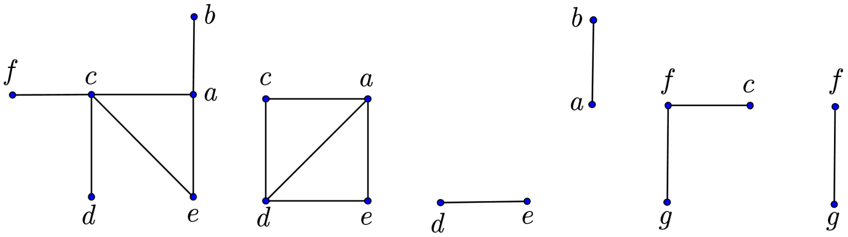


Figure 4: 2− decomposition of $\Gamma_{83}$

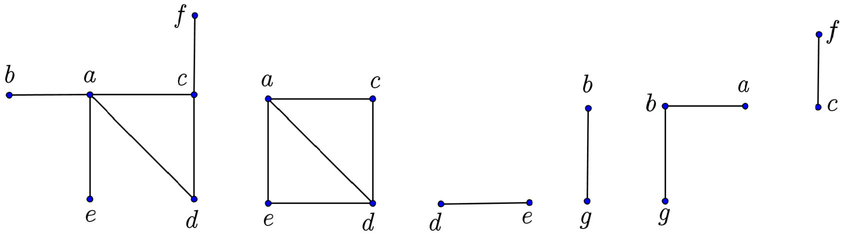


Figure 5: 2− decomposition of $\Gamma_{85}$

**Example 4.6.** The complexity is between $\frac{7}{4}$ and $\frac{15}{8}$ for $\Gamma_i$ that $i = 43, 47, 61$ and 93.

**Proof.** We consider the following lables on the access structures of $\Gamma_{43}, \Gamma_{47}, \Gamma_{61}$, and $\Gamma_{93}$.

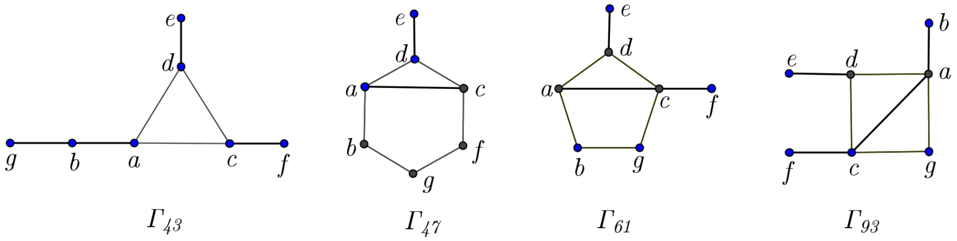


Figure 6: Lables on the access structures

By using 4.4 and 2.2, we have $\sigma(\Gamma_i) \geq \frac{7}{4}$ for $i = 43, 47, 61$ and 93.

For the upper bound of $\Gamma_{43}, \Gamma_{47}, \Gamma_{61}$, and $\Gamma_{93}$ we consider the following decomposition and by 3.1, we have $\sigma(\Gamma_i) \leq \frac{15}{8}$ ; $i = 43, 61$ and 93 and $\sigma(\Gamma_{47}) \leq \frac{11}{6}$. □

## References

[1] C. Blundo, A. De Santis, D.R. Stinson and Ugo Vaccaro, *Graph decompositions and secret sharing schemes,* J. Cryptol., 8 (1995), 39-64.

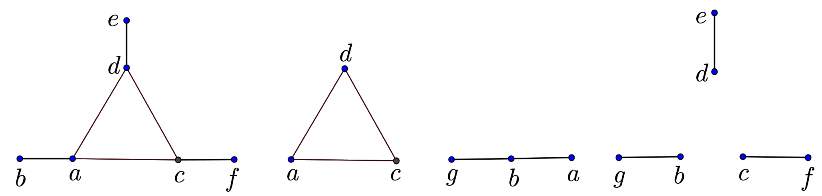


Figure 7: 2− decomposition of $\Gamma_{43}$

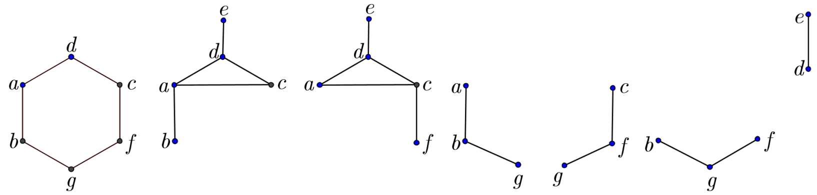


Figure 8: 3− decomposition of $\Gamma_{47}$

[2] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro, *Tight bounds on the information rate of secret sharing schemes*, Des. Codes Cryptogr., 11 (1997), 107-110.

[3] E.F. Brickell and D.M. Davenport, *On the classification of ideal secret sharing schemes*, J. Cryptol., 4 (1991), 123-134.

[4] R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, *On the size of shares for secret sharing schemes*, J. Cryptol., 6 (1993), 157-167.

[5] L. Csirmaz, *The size of a share must be large*, J. Cryptol., 10, no. 4 (1997) 223-231.

[6] M. Gharahi and M.H. Dehkordi, *The complexity of the graph access structures on six participants*, Des. Codes Cryptogr., 67 (2013), 169-173.

[7] H.R. Maimani and Z. Norozi, *Secret sharing based on cartesian product of graphs*, IJMSI, 8 (2013), 31-38.

[8] Z. Norozi and H.R. Maimani, *Secret sharing schemes with five minimal qualified subsets*, Journal of passive defence science and technology, 6 (2013), 45-54.

[9] C. Padró, L. Vázquez and A. Yan, *Finding lower bounds on the complexity of secret sharing schemes by linear programming*, In LATIN 2010: Theoretical Informatics, (2010), 344-355.

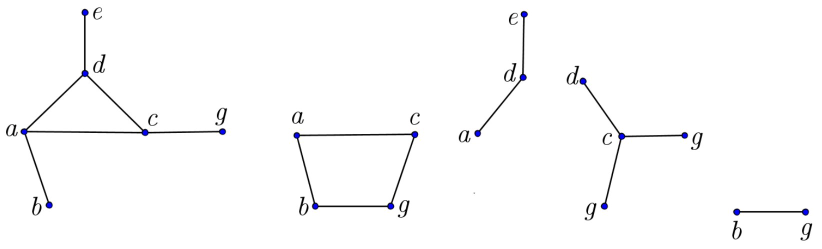


Figure 9: 2− decomposition of $\Gamma_{61}$

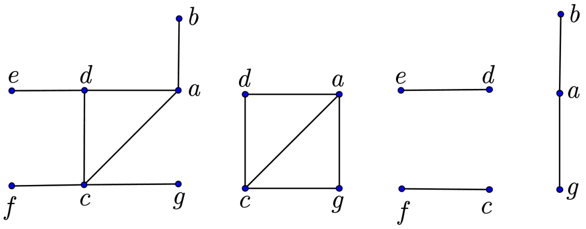


Figure 10: 2− decomposition of $\Gamma_{93}$

[10] Y. Song, Z. Li and W. Wang Song, *The information rate of secret sharing schemes on seven participants by connected graphs*, In Recent Advances in Computer Science and Information Engineering, 127 (2012), 637-645.

[11] D.R. Stinson, *An explication of secret sharing schemes*, Des. Codes Cryptogr., 2 (1992), 357-390.

[12] D.R. Stinson, *Decomposition constructions for secret-sharing schemes*, IEEE Trans. Inf. Theory, 40 (1994), 118-125.

[13] H.M. Sun, and B. Liang Chen, *Weighted decomposition construction for perfect secret sharing schemes*, Comput. Math. Appl., 43 (2002), 877-887.

[14] M. Van Dijk, *On the information rate of perfect secret sharing schemes*, Des. Codes Cryptogr., 6 (1995), 143-169.

Accepted: 16.04.2018