

# Optimal Linear Secret Sharing Schemes for Graph Access Structures on Six Participants

Motahhareh Gharahi\*      Shahram Khazaei†

## Abstract

We review the problem of finding the optimal information ratios of graph access structures on six participants. Study of such access structures were initiated by van Dijk [Des. Codes Cryptogr. 15 (1998), 301-321]. Through a sequence of follow up works, exact values of optimal information ratios of nine access structures, out of 18 initially unsolved non-isomorphic ones, were determined. Very recently [O. Farras et al. Cryptology ePrint Archive: Report 2017/919], for each of the remained such cases, the known lower bound on the optimal information ratio of linear secret sharing schemes was improved, establishing the optimal information ratio of linear secret sharing schemes for two of them. Here, for each of the other seven cases, we provide a new upper bound on the optimal information ratio of linear secret sharing schemes; our improved upper bounds match the corresponding recently presented lower bounds. Improved upper bounds are achieved using decomposition techniques. As an additional contribution, we present a new decomposition technique, called  $(\lambda, \omega)$ -weighted decomposition, which is a generalization of all known decomposition techniques.

## 1 Introduction

A *secret sharing scheme* is a method of sharing a secret among a set of participants by distributing shares to them, in such a way that only certain subsets of participants, *qualified subsets*, can reconstruct the secret from their shares. The collection of qualified subsets is called an *access structure*, which is supposed to be *monotone*, i.e., any superset of a qualified subset must be qualified. The basis of an access structure is the collection of all minimal qualified subsets of participant. The notion of access structures was proposed by Ito et al. [16] as an extension of threshold secret sharing, which had been independently introduced by Shamir [24] and Blakley [2] in 1979.

The *information ratio* of a secret sharing scheme is the ratio between the maximum size of the shares and the size of the secret. The (*optimal*) *information ratio* of an access structure  $\Gamma$ , denoted by  $\sigma(\Gamma)$ , is defined as the infimum of the information ratios of all secret sharing schemes that realize it. Determining the exact values of this parameter for a given access structure is one of the main problems in secret sharing area, which has been considered in several papers including [28, 18, 22, 13, 9]).

A secret sharing scheme is said to be *linear* if the secret value and the shares of each participant are vectors over a finite field  $\mathbb{F}$ , and each share is obtained from a linear

---

\*M. Gharahi: e-mail: motahhareh.gharahi@gmail.com, Tel: +98 21 6616 5619, Fax: +98 21 6600 5117, The author has been supported by Iran National Science Foundation (INSF) under postdoc program contract no. 94027246.

†The author has been supported by Sharif Industrial Relation Office (SIRO) under grant no. G931223.

map of the secret and randomly chosen values from  $\mathbb{F}$ . The infimum of the information ratios of all linear secret sharing schemes for an access structure  $\Gamma$  is denoted by  $\lambda(\Gamma)$ .

The access structures with basis composed of minimal qualified subsets of size two is called graph access structure. The optimal information ratios of such access structures have been considered in several cases, for example see, the ones in [5, 28, 10, 11, 9]. The optimal information ratios of the 112 non-isomorphic graph access structures on six participants were studied by van Dijk [28]. In 94 such cases, the exact values of  $\sigma(\Gamma)$  were determined, and for the other ones, upper and lower bounds were provided. A series of works [27, 30, 23, 14, 15] then resulted in determining the exact values of  $\sigma(\Gamma)$  for nine cases out of 18 unsolved ones. Very recently, Farrás et al. [12] have derived a new lower bound on  $\lambda(\Gamma)$  for each of the nine remaining cases. In two cases, improved lower bounds match the corresponding known upper bounds on  $\lambda(\Gamma)$  [29, 20].

In this paper, we consider the remaining seven cases, providing new upper bounds on  $\lambda(\Gamma)$  for each of them. All cases, except one, can be improved by applying  $(\lambda, \omega)$ -decomposition [29] and  $\lambda$ -weighted decomposition [27] techniques, which are the only known extensions of Stinson's  $\lambda$ -decomposition technique [26]. Our hard attempt to tackle the remaining case by resorting to the known decomposition techniques failed. Consequently, we devised a new decomposition technique to handle the excepted case. The new decomposition technique, which is a generalization of each of the aforementioned techniques, is referred to as  $(\lambda, \omega)$ -weighted decomposition. For each case, our improved upper bound on  $\lambda(\Gamma)$  matches the corresponding presented lower bound in [12]. Therefore, our results put an end to the seek for optimal linear secret sharing schemes for these seven cases.

## 2 Secret sharing schemes

In this section, we present some standard definitions related to secret sharing. We refer the reader to [1] for a two-decade survey on the topic and the references there-in, including [25, 19, 7, 8, 4], for historical development of the field.

Let  $\mathcal{P} = \{p_1, \dots, p_n\}$  be a set of participants. The collection  $\Gamma$  of sets in  $2^{\mathcal{P}}$  is called an *access structure* on  $\mathcal{P}$  if  $\Gamma$  is monotone increasing, i.e., for every  $A \in \Gamma$  and  $A \subseteq B$  it holds that  $B \in \Gamma$ . The sets in  $\Gamma$  and  $\Gamma^c$  are called *qualified sets* and *forbidden sets* of the access structure, respectively. A qualified set  $A \in \Gamma$  is called minimal if any proper subset of  $A$  is a forbidden set, and a forbidden set  $B \in \Gamma^c$  is called maximal if  $\{p\} \cup B \in \Gamma$  for all  $p \in \mathcal{P}$ . The collection of all minimal qualified subsets and that of all maximal forbidden sets are denoted by  $\Gamma^-$  and  $\Gamma^+$ , respectively.

Let  $\mathbf{X}$  be a random variable with support  $\mathcal{X} = \{x_1, \dots, x_m\}$  (i.e., the set of values that it accepts with positive probability) and let  $p_i = \Pr[\mathbf{X} = x_i]$ . The Shannon entropy of  $\mathbf{X}$  is defined as  $H(\mathbf{X}) = -\sum_{i=1}^m p_i \log_2 p_i$ . The entropy of  $\mathbf{X}$  conditioned on  $\mathbf{Y}$  is defined as  $H(\mathbf{X}|\mathbf{Y}) = \sum_{y \in \mathcal{Y}} \Pr[\mathbf{Y} = y] H(\mathbf{X}|\mathbf{Y} = y)$ , where  $\mathcal{Y}$  is the support of  $\mathbf{Y}$  and  $H(\mathbf{X}|\mathbf{Y} = y) = \sum_{i=1}^m \Pr[\mathbf{X} = x_i|\mathbf{Y} = y] \log_2 \Pr[\mathbf{X} = x_i|\mathbf{Y} = y]$ . Conventionally,  $0 \log_2 0$  is considered to be 0.

**Definition 2.1** (secret sharing scheme). *A secret sharing scheme on  $\mathcal{P}$  is a triple  $\Sigma = (\mathbf{S}, \mathbf{R}, \Pi)$ , where  $\mathbf{S}$  and  $\mathbf{R}$  are independent random variables with supports  $\mathcal{S}$  and  $\mathcal{R}$ , respectively, satisfying  $H(\mathbf{S}) > 0$ , and  $\Pi : \mathcal{S} \times \mathcal{R} \rightarrow \mathcal{S}_1 \times \dots \times \mathcal{S}_n$  is a map, in which  $\mathcal{S}_i$  is the support of random variable  $\mathbf{S}_i$  induced by  $\Pi(\mathbf{S}, \mathbf{R}) = (\mathbf{S}_1, \dots, \mathbf{S}_n)$ . We refer to  $\Pi$ ,  $\mathcal{S}$  and  $\mathcal{R}$  as the sharing map, secret space and randomness space.*

To share a secret  $s \in \mathcal{S}$ , presumably sampled from  $\mathbf{S}$ , a randomness  $r$  is sampled from  $\mathbf{R}$  and the vector of shares  $\Pi(s, r) = (s_1, \dots, s_n)$  is computed. Then, each share  $s_j$  is privately transmitted to the participant  $p_j$ . For a set  $A \subseteq \mathcal{P}$ , we denote the random variable  $\mathbf{S}_A$  as the restriction of  $\Pi(\mathbf{S}, \mathbf{R})$  to the entries that correspond to the members of  $A$ .

A secret sharing scheme is said to be *linear* if the sets  $\mathcal{S}, \mathcal{R}, \mathcal{S}_1, \dots, \mathcal{S}_n$  are all vector spaces of finite dimension over a finite field  $\mathbb{F}$  and  $\Pi$  is a linear map on  $\mathbb{F}$ .

**Definition 2.2** (realization of an access structure). *Let  $\Sigma$  be a secret sharing scheme and let  $\Gamma$  be an access structure both defined on  $\mathcal{P}$ . We say that  $\Sigma$  is a secret sharing scheme for  $\Gamma$ , or  $\Sigma$  realizes  $\Gamma$ , if the following two hold:*

- (1) *The secret can be reconstructed by qualified sets; that is, for all  $A \in \Gamma$ , it holds that  $H(\mathbf{S}|\mathbf{S}_A) = 0$ .*
- (2) *The secret is remained perfectly hidden from the forbidden sets; that is, for all  $B \notin \Gamma$ , it holds that  $H(\mathbf{S}|\mathbf{S}_B) = H(\mathbf{S})$ .*

Let  $\Sigma$  be a secret sharing scheme on  $\mathcal{P}$ . The *information ratio* of a participant  $p_i \in \mathcal{P}$  in  $\Sigma$ , denoted by  $\sigma_{p_i}(\Sigma)$ , is defined by  $\sigma_{p_i}(\Sigma) = H(\mathbf{S}_i)/H(\mathbf{S})$  and the information ratio of  $\Sigma$  is defined by  $\sigma(\Sigma) = \max_{p \in \mathcal{P}} \sigma_p(\Sigma)$ .

The (*optimal*) *information ratio* of an access structure  $\Gamma$  on  $\mathcal{P}$  is defined by  $\sigma(\Gamma) = \inf \sigma(\Sigma)$ , where the infimum is taken over all secret sharing schemes  $\Sigma$  realizing  $\Gamma$ . When the infimum is only taken over all linear secret sharing schemes for  $\Gamma$ , it is denoted by  $\lambda(\Gamma)$ . A secret sharing scheme  $\Sigma$  with  $\sigma(\Sigma) = 1$  is called *ideal*. An access structure  $\Gamma$  is called *ideal* if it can be realized by an ideal scheme. The *dual* of an access structure  $\Gamma$  on  $\mathcal{P}$ , denoted by  $\Gamma^*$ , is defined by  $\Gamma^* = \{A \subseteq \mathcal{P} : \mathcal{P} \setminus A \notin \Gamma\}$ . It is known [17] that if  $\Sigma$  is a linear secret sharing scheme for  $\Gamma$ , then there exists a linear secret sharing scheme  $\Sigma^*$  for  $\Gamma^*$  such that  $\sigma(\Sigma^*) = \sigma(\Sigma)$ . Consequently  $\lambda(\Gamma^*) = \lambda(\Gamma)$ .

The access structure  $\Gamma$  on  $\mathcal{P}$  is said to be based on a graph  $G$  if the participants are as vertices of  $G$  and the minimal qualified subsets are corresponding to the edges. Such access structures are called *graph access structures*. It is known [6] that an access structure  $\Gamma$  based on a connected graph  $G$  is ideal if and only if  $G$  is a complete multipartite graph.

### 3 Decomposition constructions

Decomposition is a technique for constructing a new secret sharing scheme from a collection of secret sharing schemes. The idea was first proposed by Stinson [26] under the name of  $\lambda$ -decomposition. Below, we first review two known extensions of  $\lambda$ -decomposition. Then, we present a new decomposition technique, as a generalization of each of the mentioned extensions.

#### 3.1 $(\lambda, \omega)$ -decomposition

In this subsection, we review the  $(\lambda, \omega)$ -decomposition technique from [29].

**Definition 3.1** ( $(\lambda, \omega)$ -decomposition). *Let  $\Gamma$  be an access structure on  $\mathcal{P}$ , and let  $\lambda, \omega$  be positive integers such that  $\lambda > \omega$ . A  $(\lambda, \omega)$ -decomposition of  $\Gamma$  consists of a collection  $\{\Gamma^1, \dots, \Gamma^h\}$  of access structures on  $\mathcal{P}$  such that the following requirements are satisfied:*

- (1) If  $A \in \Gamma^-$ , then it holds that  $A \in \Gamma^j$  for at least  $\lambda$  distinct values of  $j \in [h]$ .
- (2) If  $A \in \Gamma^+$ , then it holds that  $A \in \Gamma^j$  for at most  $\omega$  distinct values of  $j \in [h]$ .

**Theorem 3.1.** Let  $\Gamma$  be an access structure on  $\mathcal{P}$  and  $\{\Gamma^1, \dots, \Gamma^h\}$  be a  $(\lambda, \omega)$ -decomposition of  $\Gamma$ . Moreover, suppose that there exists a finite field  $\mathbb{F}$  such that for every  $\Gamma_j$ ,  $j \in [h]$ , there exist a secret sharing scheme with secret space  $\mathbb{F}$  and information ratio  $\sigma_{p,j}$  for  $p \in \mathcal{P}$ . Then, there exists a secret sharing scheme  $\Sigma$  for  $\Gamma$  with information ratio

$$\sigma(\Sigma) = \max_{p \in \mathcal{P}} \left\{ \frac{\sum_{j=1}^h \sigma_{p,j}}{\lambda - \omega} \right\}.$$

### 3.2 $\lambda$ -weighted decomposition

In this subsection, we review the  $\lambda$ -weighted-decomposition technique from [27].

**Definition 3.2** (weighted access structure). A weighted access structure on  $\mathcal{P}$  is a set  $\Gamma^w = \{(A, w) \mid A \in 2^{\mathcal{P}}, w \in \mathbb{Z}^{\geq 0}\}$  such that for every  $(A, w_A), (B, w_B) \in \Gamma^w$ , if  $A \subseteq B$ , then it holds that  $w_A \leq w_B$ . For every  $(A, w) \in \Gamma^w$ ,  $w$  is called the weight of  $A$  in  $\Gamma^w$  and denoted by  $\text{wt}(A; \Gamma^w)$ , or  $w_A$  when there is no confusion. The weight of  $\Gamma^w$  is defined by  $\text{wt}(\Gamma^w) = \max\{w_A : \text{for all } A \in 2^{\mathcal{P}}\}$ .

**Definition 3.3** (realization of a weighted access structure). Let  $\Sigma$  be a secret sharing scheme and let  $\Gamma^w$  be a weighted access structure both defined on  $\mathcal{P}$ . We say that  $\Sigma$  is a secret sharing scheme for  $\Gamma^w$ , or  $\Sigma$  realizes  $\Gamma^w$ , if for all  $A \in 2^{\mathcal{P}}$  it holds that  $H(\mathbf{S}|\mathbf{S}_A) = (1 - w_A/\text{wt}(\Gamma^w))H(\mathbf{S})$ .

**Definition 3.4** ( $\lambda$ -weighted-decomposition). Let  $\Gamma$  be an access structure on  $\mathcal{P}$  and let  $\lambda$  be a positive integer. A  $\lambda$ -weighted-decomposition of  $\Gamma$  consists of a collection  $\{\Gamma_1^w, \dots, \Gamma_h^w\}$  of weighted access structures on  $\mathcal{P}$  if the following hold:

- (1) If  $A \in \Gamma^-$ , then there exists a subset of indexes  $I \subseteq [h]$ , such that we have  $\sum_{j \in I} \text{wt}(A; \Gamma_j^w) \geq \lambda$ .
- (2) If  $A \in \Gamma^+$ , then it holds that  $\text{wt}(A; \Gamma_j^w) = 0$ , for each  $j \in [h]$ .

**Theorem 3.2.** Let  $\Gamma$  be an access structure on  $\mathcal{P}$  and  $\{\Gamma_1^w, \dots, \Gamma_h^w\}$  be a  $\lambda$ -weighted-decomposition of  $\Gamma$ . Suppose that there exists a finite field  $\mathbb{F}$  such that each weighted access structure  $\Gamma_j^w$  with weight  $w_j = \text{wt}(\Gamma_j^w)$ ,  $j \in [h]$ , is realized by a secret sharing scheme with information ratio  $\sigma_{p,j}$  for  $p \in \mathcal{P}$  over secret space  $\mathbb{F}^{w_j}$ . Moreover, assume that any subset  $A \subset \mathcal{P}$  can obtain  $\text{wt}(A; \Gamma_j^w)$  out of the  $w_j$  secrets. Then, there exists a secret sharing scheme  $\Sigma$  for  $\Gamma$  with information ratio

$$\sigma(\Sigma) = \max_{p \in \mathcal{P}} \left\{ \frac{\sum_{j=1}^h w_j \sigma_{p,j}}{\lambda} \right\}.$$

### 3.3 $(\lambda, \omega)$ -weighted decomposition

In this subsection, we introduce the  $(\lambda, \omega)$ -weighted decomposition, which captures the previous two decompositions as its special cases.

**Definition 3.5** ( $(\lambda, \omega)$ -weighted-decomposition). Let  $\Gamma$  be an access structure on  $\mathcal{P}$ , and let  $\lambda, \omega$  be positive integers such that  $\lambda > \omega$ . A  $(\lambda, \omega)$ -weighted-decomposition of  $\Gamma$  consists of a collection  $\{\Gamma_1^w, \dots, \Gamma_h^w\}$  of weighted access structures on  $\mathcal{P}$  such that the following properties are satisfied:

- (1) If  $A \in \Gamma^-$ , then there exists a subset of indexes  $I \subseteq [h]$ , such that we have  $\sum_{j \in I} \text{wt}(A; \Gamma_j^w) \geq \lambda$ .
- (2) If  $A \in \Gamma^+$ , then  $\sum_{j=1}^h \text{wt}(A; \Gamma_j^w) \leq \omega$ .

**Theorem 3.3.** Let  $\Gamma$  be an access structure on  $\mathcal{P}$  and  $\{\Gamma_1^w, \dots, \Gamma_h^w\}$  be a  $(\lambda, \omega)$ -weighted-decomposition of  $\Gamma$ . Suppose that there exists a finite field  $\mathbb{F}$  such that each weighted access structure  $\Gamma_j^w$  with weight  $w_j = \text{wt}(\Gamma_j^w)$ ,  $j \in [h]$ , is realized by a secret sharing scheme with information ratio  $\sigma_{p,j}$  for  $p \in \mathcal{P}$  over secret space  $\mathbb{F}^{w_j}$ . Moreover, assume that any subset  $A \subset \mathcal{P}$  can obtain  $\text{wt}(A; \Gamma_j^w)$  out of the  $w_j$  secrets. Then, there exists a secret sharing scheme  $\Sigma$  for  $\Gamma$  with information ratio

$$\sigma(\Sigma) = \max_{p \in \mathcal{P}} \left\{ \frac{\sum_{j=1}^h w_j \sigma_{p,j}}{\lambda - \omega} \right\}.$$

*Proof.* We construct a secret sharing scheme for  $\Gamma$  over secret space  $\mathbb{F}^{\lambda - \omega}$ . To share a secret  $s = (s_1, \dots, s_{\lambda - \omega}) \in \mathbb{F}^{\lambda - \omega}$ , let

$$f(x) = \sum_{t=0}^{\omega-1} a_t x^t + \sum_{t=\omega}^{\lambda-1} s_{t-\omega+1} x^t,$$

where  $a_0, \dots, a_{\omega-1}$  are chosen randomly from  $\mathbb{F}$ . Let  $N = \sum_{j=1}^h w_j$ . For each  $\ell \in [N]$ , define  $k_\ell = f(\ell)$ . Indeed, we have defined a  $(\lambda, \omega, N)$  ramp secret sharing scheme [3] this way. In such schemes, similar to threshold schemes, the secret  $s$  is shared between  $N$  participant, by giving the share  $k_\ell$  to the  $\ell$ th participant. The secret  $s$  can then be reconstructed from any subset of size at least  $\lambda$  of shares, while no information is leaked about  $s$  from any subset of size at most  $\omega$  of such shares.

In our construction, we then view  $(k_1, \dots, k_N)$  as a block-wise vector  $(K_1, \dots, K_h)$ , where  $K_j \in \mathbb{F}^{w_j}$ ; recall that  $N = \sum_{j=1}^h w_j$ . More precisely, for each  $j \in [h]$  we have  $K_j = (k_{\sum_{t=1}^{j-1} w_t + 1}, \dots, k_{\sum_{t=1}^j w_t})$ . Then, the secret  $K_j$  is shared among the participants  $\mathcal{P}$  using the secret sharing scheme for weighted access structure  $\Gamma_j^w$ . The corresponding secret sharing scheme accepts secrets in  $\mathbb{F}^{w_j}$  and every participant  $p \in \mathcal{P}$  receives a share  $s_{p,j} \in \mathbb{F}^{w_j \sigma_{p,j}}$ . The final share of participant  $p \in \mathcal{P}$  in our constructed scheme will be  $(s_{p,1}, \dots, s_{p,h})$ , i.e., an element of  $\mathbb{F}^{\sum_{j=1}^h w_j \sigma_{p,j}}$ . Thus, as claimed, the information ratio of the constructed secret sharing scheme is

$$\sigma(\Sigma) = \max_{p \in \mathcal{P}} \left\{ \frac{\sum_{j=1}^h w_j \sigma_{p,j}}{\lambda - \omega} \right\}.$$

We continue to show that our scheme realizes  $\Gamma$ . Let  $A \in \Gamma^-$  be a qualified set. By assumption,  $A$  obtains  $\text{wt}(A; \Gamma_j^w)$  elements of  $(k_{\sum_{t=1}^{j-1} w_t + 1}, \dots, k_{\sum_{t=1}^j w_t})$ . Therefore, the qualified set  $A$  obtains a total of  $\sum_{j=1}^h \text{wt}(A; \Gamma_j^w)$  elements of the vector  $(k_1, \dots, k_N)$ . By definition of  $(\lambda, \omega)$ -weighted decomposition,  $\sum_{j=1}^h \text{wt}(A; \Gamma_j^w) \geq \lambda$ .

Therefore, a qualified set obtains at least  $\lambda$  elements of  $(k_1, \dots, k_N)$ . The ramp secret sharing then guarantees that the initial secret  $s$  can be recovered by any qualified set. Similarly, it can be shown that any unqualified set obtains at most  $\omega$  elements of  $(k_1, \dots, k_N)$ , and therefore, it gains no information about the shared secret.  $\square$

## 4 Improved upper bounds

We consider seven graph access structures on six participants, for which determining the exact values of information ratios remained unsolved in [28]. We improve known upper bound for each of them by using decomposition techniques. Taking into account the recently derived lower bounds on  $\lambda(\Gamma)$  in [12], we conclude that our decomposition construction leads to an optimal linear secret sharing schemes for each of them, establishing the exact value of  $\lambda(\Gamma)$ . A summary of our results can be found in Table 1. For the sake of completeness, we have included the other two access structures which have a similar situation. We point out that the graph access structures  $\Gamma_{75}$  and  $\Gamma_{84}$  are isomorphic with the dual of two access structures with four minimal qualified subsets on six participants. Regarding the notations of [21], their corresponding underlying participants sets are  $\{3, 5, 7, A, D, E\}$  and  $\{3, 5, 7, B, D, E\}$ , respectively, with reported upper bounds  $11/6$  and  $5/3$  on  $\lambda(\Gamma)$  in [21]. Our observation shows that for both of them indeed  $\lambda(\Gamma) = 8/5$ .

Table 1: Updated results for the unsolved graph access structures on six participants

Access structure	$\sigma(\Gamma)$ [28, 20]	$\lambda(\Gamma)$ [28, 20, 12]	Current $\sigma(\Gamma)$	Current $\lambda(\Gamma)$
$\Gamma_{55}, \Gamma_{59}, \Gamma_{70},$ $\Gamma_{71}, \Gamma_{75}, \Gamma_{77}, \Gamma_{84}$	$[3/2, 5/3]$	$[8/5, 5/3]$	$[3/2, 8/5]$	$8/5$
$\Gamma_{91}, \Gamma_{93}$	$[3/2, 8/5]$	$8/5$	–	–

Throughout this paper a set  $A = \{i_1, \dots, i_t\}$  is simply represented by  $i_1 \dots i_t$ . The vertices of each graph are labeled in clockwise direction by starting from 1 at the leftmost vertex. The access structure numbers are similar to [28].

In all constructed schemes, the secret is  $s$  (or  $(s_1, s_2)$ ) and the randomness is  $(r_1, \dots, r_5)$  where  $s, s_1, s_2$  and  $r_i$ 's are all from  $GF(q)$  with  $q > 3$ . The share of the participant  $p \in \mathcal{P}$  is denoted by  $s_p$ .

### 4.1 Upper bounds obtained by $(\lambda, \omega)$ -decomposition

We consider three graph access structures  $\Gamma_{59}, \Gamma_{71}$  and  $\Gamma_{84}$ , shown in Fig. 1. By using  $(\lambda, \omega)$ -decomposition technique, we improve known upper bounds on their optimal information ratios.

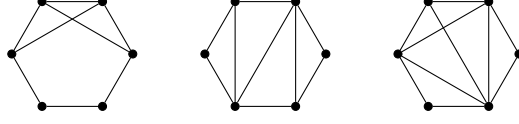


Fig. 1: Graph access structures  $\Gamma_{59}$ ,  $\Gamma_{71}$  and  $\Gamma_{84}$ .

Similar to [30], we use a table for demonstrating the presented  $(\lambda, \omega)$ -decomposition for each of the aforementioned graph access structures.

**Note 4.1** (Description of table entries). Consider an access structure  $\Gamma$  with  $\Gamma^- = \{A_1, \dots, A_m\}$  and  $\Gamma^+ = \{B_1, \dots, B_M\}$ . The first two columns represent the discovered  $(\lambda, \omega)$ -decomposition. First column in table denotes the number of duplications of sub-access structures  $\Gamma^{j^-}$  in the decomposition which is given in the second column. Some sub-access structures are graph access structures, which are represented by their corresponding underlying graph, and others are composed of singleton sets, in which case the minimal subsets are explicitly given. Each bit  $a_i$  of binary string  $a_1 \dots a_m$  in third column indicates if  $A_i$  is a qualified subset of  $\Gamma^j$ ; that is,  $a_i = 1$  iff  $A_i \in \Gamma^{j^-}$ . Each bit  $b_i$  of binary string  $b_1 \dots b_M$  in fourth column indicates if  $B_i$  is a qualified subset of  $\Gamma^{j^-}$ ; that is  $b_i = 1$  iff  $B_i \in \Gamma^{j^-}$ . Fifth column shows the presented secret sharing scheme  $\Sigma^j$  for  $\Gamma^j$ . If a sub-access structure is ideal, we ignore to provide its corresponding sub-scheme. If all sub-access structures are ideal, the fifth column will be removed. Finally, the last column represents the vector of information ratios of participants in the sub-scheme, that is,  $(\sigma_{1,j}, \dots, \sigma_{6,j})$ .

**Result 4.1** (Results for  $\Gamma_{59}$ ,  $\Gamma_{71}$  and  $\Gamma_{84}$ ). We provide new upper bound on the optimal information ratio of each of the graph access structures  $\Gamma_{59}$ ,  $\Gamma_{71}$  and  $\Gamma_{84}$  by applying a  $(6, 1)$ -decomposition. These decompositions are respectively represented in the Table 2, Table 3 and Table 4.

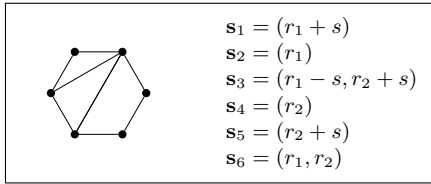


Fig. 2: Scheme  $\Sigma^2$  in Table 2.

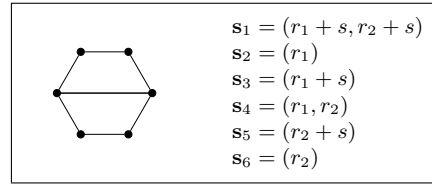




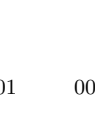



Fig. 3: Scheme  $\Sigma^4$  in Table 3.










Table 2: The (6, 1)-decomposition for  $\Gamma_{59}$ .

#	$\Gamma^{j-}$	$a_1 \dots a_8$	$b_1 \dots b_7$	$\Sigma^j$	$(\sigma_{1,j}, \dots, \sigma_{6,j})$
1	$\{\{1\}, \{4\}\}$	11101110	1100001	ideal	(1, 0, 0, 1, 0, 0)
1		11110111	0000010	$\Sigma^2$	(1, 1, 2, 1, 1, 2)
1		10111111	0010000	$\Sigma^3$	(1, 2, 1, 1, 2, 1)
1		11111011	0001000	$\Sigma^4$	(1, 2, 1, 1, 1, 2)
1		01111111	0000100	$\Sigma^5$	(1, 1, 2, 1, 2, 1)
2		11011100	0000000	ideal	(1, 1, 1, 1, 0, 0)
1		00100001	0000000	ideal	(1, 0, 0, 0, 1, 1)
1		00000011	0000000	ideal	(0, 0, 0, 1, 1, 1)

**Note.** See Note 4.1 for description of table. Here,  $\Gamma_{59}^- = \{12, 13, 16, 23, 24, 34, 45, 56\}$  and  $\Gamma_{59}^+ = \{14, 15, 25, 26, 35, 36, 46\}$ . The scheme  $\Sigma^2$  is presented in Fig. 2. Since the access structures  $\Gamma^3, \Gamma^4$  and  $\Gamma^5$  are all isomorphic with  $\Gamma^2$ , corresponding schemes can be easily constructed from  $\Gamma^2$  in Fig. 2. From Theorem 3.1, this decomposition leads to a scheme  $\Sigma$  with  $\sigma(\Sigma) = 8/5$ .














Table 3: The (6, 1)-decomposition for  $\Gamma_{71}$ .

#	$\Gamma^{j^-}$	$a_1 \dots a_9$	$b_1 \dots b_6$	$\Sigma^j$	$(\sigma_{1,j}, \dots, \sigma_{6,j})$
1	$\{\{3\}\}$	001011100	100000	ideal	(0, 0, 1, 0, 0, 0)
1	$\{\{6\}\}$	010100101	000001	ideal	(0, 0, 0, 0, 0, 1)
1	$\{\{2\}, \{5\}\}$	101101011	001110	ideal	(0, 1, 0, 0, 1, 0)
1		111010011	010000	$\Sigma^4$	(2, 1, 1, 2, 1, 1)
2		111100100	000000	ideal	(1, 1, 1, 0, 0, 1)
2		000011111	000000	ideal	(0, 0, 1, 1, 1, 1)
1		110100000	000000	ideal	(1, 1, 0, 0, 0, 1)
1		000011010	000000	ideal	(0, 0, 1, 1, 1, 0)
1		010100001	000000	ideal	(1, 1, 0, 0, 1, 1)
1		001011000	000000	ideal	(0, 1, 1, 1, 1, 0)
1		100000000	000000	ideal	(1, 1, 0, 0, 0, 0)
1		000000010	000000	ideal	(0, 0, 0, 1, 1, 0)

**Note.** See Note 4.1 for description of table. Here,  $\Gamma_{71}^- = \{12, 16, 23, 26, 34, 35, 36, 45, 56\}$  and  $\Gamma_{71}^+ = \{13, 14, 15, 24, 25, 46\}$ . The scheme  $\Sigma^4$  is presented in Fig. 3. From Theorem 3.1, this decomposition leads to a scheme  $\Sigma$  with  $\sigma(\Sigma) = 8/5$ .

Table 4: The (6, 1)-decomposition for  $\Gamma_{84}$ .

#	$\Gamma^{j-}$	$a_1 \dots a_{10}$	$b_1 \dots b_4$	$(\sigma_{1,j}, \dots, \sigma_{6,j})$
1	$\{\{1\}\}$	1111000000	1000	(1, 0, 0, 0, 0, 0)
1	$\{\{3\}\}$	0100101100	0010	(0, 0, 1, 0, 0, 0)
1	$\{\{5\}\}$	0010010111	0001	(0, 0, 0, 0, 1, 0)
1		1111111111	0100	(1, 1, 1, 1, 1, 1)
1		1011010001	0000	(1, 1, 0, 0, 1, 1)
1		0000111110	0000	(0, 1, 1, 1, 1, 0)
1		1111010101	0000	(1, 1, 1, 0, 1, 1)
1		0110111110	0000	(1, 1, 1, 1, 1, 0)
1		1100100000	0000	(1, 1, 1, 0, 0, 0)
2		0000000011	0000	(0, 0, 0, 0, 1, 1)
1		1001000000	0000	(1, 1, 0, 0, 0, 1)
1		0000101000	0000	(0, 1, 1, 1, 0, 0)
1		0001000000	0000	(1, 0, 0, 0, 0, 1)
1		0000001000	0000	(0, 0, 1, 1, 0, 0)

**Note.** See Note 4.1 for description of table. Here,  $\Gamma_{84}^- = \{12, 13, 15, 16, 23, 25, 34, 35, 45, 56\}$  and  $\Gamma_{84}^+ = \{14, 246, 36, 5\}$ . All sub-access structures are ideal. From Theorem 3.1, this decomposition leads to a scheme  $\Sigma$  with  $\sigma(\Sigma) = 8/5$ .

## 4.2 Upper bounds obtained by $\lambda$ -weighted decomposition

We improve the known upper bounds for each of the three graph access structures  $\Gamma_{55}$ ,  $\Gamma_{70}$  and  $\Gamma_{75}$ , represented in Fig. 4, by using  $\lambda$ -weighted decompositions.

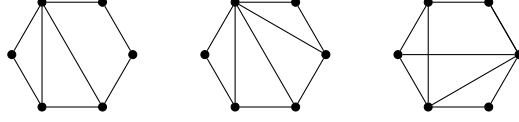


Fig. 4: Graph access structures  $\Gamma_{55}$ ,  $\Gamma_{70}$  and  $\Gamma_{75}$ .

**Result 4.2** (Results for  $\Gamma_{55}$ ,  $\Gamma_{70}$  and  $\Gamma_{75}$ ). *We apply the 5-weighted decomposition construction for each of the graph access structures  $\Gamma_{55}$ ,  $\Gamma_{70}$  and  $\Gamma_{75}$ , resulting in new upper bound on the optimal information ratio for each of them. These decomposition constructions are shown in Table 6.*

**Note 4.2.** *In Tables 5 and 6, a weighted graph indicates a weighted sub-access structures with following considerations: I) the weight of a singleton set is assumed to be zero, II) the weight assigned to each edge indicates the weight of the corresponding subset of size 2 and III) the weight of a larger set is considered to be at least the maximum weight of all its subsets of size 2 and at most the maximum of the weights assigned to graph edges; the exact value is not important.*

Table 5: Schemes for non-ideal sub-access structures in Table 6

Weighted access structure	Secret sharing scheme	Note
	$\mathbf{s}_1 = (r_1 + 2s_1 + s_2, r_2 - r_3, r_4)$ $\mathbf{s}_2 = (r_1, r_3 + s_1, r_2 + r_4 - s_1)$ $\mathbf{s}_3 = (r_3, r_1 + r_2 + r_4 + 2s_1 + s_2)$ $\mathbf{s}_4 = (r_2 + s_1, r_3 + s_1)$ $\mathbf{s}_5 = (r_2, r_4)$ $\mathbf{s}_6 = (r_1 + s_1, r_2 + s_1, r_4 + s_2)$	In Part I of Table 6
	$\mathbf{s}_1 = (r_1 + 2s_1 + s_2, r_2 - r_3, r_4)$ $\mathbf{s}_2 = (r_2 - s_1, r_3 - s_2, r_4 + s_2)$ $\mathbf{s}_3 = (r_2, r_4)$ $\mathbf{s}_4 = (r_2 + s_1, r_3 + s_1)$ $\mathbf{s}_5 = (r_3, r_1 + r_2 + r_4 + 2s_1 + s_2)$ $\mathbf{s}_6 = (r_1, r_3 + s_1, r_2 + r_4)$	In Part II of Table 6
	$\mathbf{s}_1 = (r_1 + 2s_1 + s_2, r_2 - r_3, r_4)$ $\mathbf{s}_2 = (r_1, r_3 + s_1, r_2 + r_4)$ $\mathbf{s}_3 = (r_3, r_1 + r_2 + r_4 + 2s_1 + s_2)$ $\mathbf{s}_4 = (r_2 - s_1, r_3 + s_1)$ $\mathbf{s}_5 = (r_2, r_4)$ $\mathbf{s}_6 = (r_2 + s_1 + s_2, r_3, r_4 + s_2)$	In Part III of Table 6

Table 6: The 5-weighted decompositions for  $\Gamma_{55}$ ,  $\Gamma_{70}$  and  $\Gamma_{75}$ .

I: Weighted decomposition for $\Gamma_{55}$			II: Weighted decomposition for $\Gamma_{70}$			III: Weighted decomposition for $\Gamma_{75}$		
#	$\Gamma_j^w$	$\Sigma^j$ ( $\sigma_{1,j}, \dots, \sigma_{6,j}$ )	#	$\Gamma_j^w$	$\Sigma^j$ ( $\sigma_{1,j}, \dots, \sigma_{6,j}$ )	#	$\Gamma_j^w$	$\Sigma^j$ ( $\sigma_{1,j}, \dots, \sigma_{6,j}$ )
1		$\Sigma^1$ (3, 3, 2, 2, 2, 3)/2	1		$\Sigma^1$ (3, 3, 2, 2, 2, 3)/2	1		$\Sigma^1$ (3, 3, 2, 2, 2, 3)/2
2		(1, 1, 0, 0, 1, 1)	2		(1, 1, 0, 0, 1, 1)	1		(1, 1, 1, 1, 0, 0)
2		(0, 1, 1, 1, 1, 0)	2		(0, 1, 1, 1, 1, 0)	2		(1, 0, 0, 1, 1, 1)
1		(1, 1, 1, 0, 0, 1)	1		(1, 1, 1, 1, 0, 1)	1		(1, 1, 1, 1, 0, 1)
1		(0, 0, 1, 1, 1, 0)	1		(0, 0, 1, 1, 1, 0)	2		(0, 0, 1, 1, 1, 0)
1		(0, 0, 0, 1, 1, 1)	1		(0, 0, 0, 1, 1, 1)	1		(0, 1, 0, 0, 1, 1)
1		(0, 0, 1, 1, 0, 0)	1		(0, 0, 1, 1, 0, 0)	1		(1, 1, 0, 0, 0, 1)
1		(1, 0, 0, 0, 0, 1)	1		(1, 0, 0, 0, 0, 1)	1		(0, 1, 1, 0, 0, 0)

**Note.** See Note 4.2 for description of the wighted sub-access structures. For each decompositions in the table, the scheme  $\Sigma^1$  is presented in Table 5, and if a sub-access structure is ideal, we ignore to provide its corresponding scheme. By Theorem 3.2, each of the 5-weighted decompositions leads to a scheme  $\Sigma$  with  $\sigma(\Sigma) = 8/5$ .

### 4.3 An upper bound obtained by $(\lambda, \omega)$ -weighted decomposition

For the graph access structure  $\Gamma_{77}$ , shown in Fig. 5, we drive a new upper bound on the optimal information ratio by providing a  $(\lambda, \omega)$ -weighted decomposition.

**Result 4.3** (Result for  $\Gamma_{77}$ ). *We provide a new upper bound on the optimal information ratio of the graph access structure  $\Gamma_{77}$ , by applying the  $(6, 1)$ -weighted decomposition technique, shown in Table 7.*

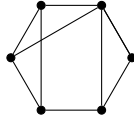


Fig. 5: Graph access structure  $\Gamma_{77}$ .

Table 7: The  $(6, 1)$ -weighted decomposition for  $\Gamma_{77}$ .

#	$\Gamma_j^w$	$a_1 \dots a_9$	$b_1 \dots b_6$	$\Sigma^j$	$(\sigma_{1,j}, \dots, \sigma_{6,j})$
1	$\{\{2\}, \{5\}\}$	100110111	011100	ideal	$(0, 1, 0, 0, 1, 0)$
1	$\{\{3\}\}$	010101100	000010	ideal	$(0, 0, 1, 0, 0, 0)$
1		111101011	100000	$\Sigma^3$	$(2, 1, 1, 2, 1, 1)$
1		222122222	000000	$\Sigma^4$	$(3, 3, 3, 3, 3, 3)/2$
1		101010000	000000	ideal	$(1, 1, 0, 0, 0, 1)$
1		011111101	000001	ideal	$(1, 1, 1, 1, 1, 1)$
1		000001110	000000	ideal	$(0, 0, 1, 1, 1, 0)$
1		111110000	000000	ideal	$(1, 1, 1, 0, 0, 1)$
1		000000011	000000	ideal	$(0, 0, 0, 1, 1, 1)$

**Note.** See Note 7 for description of the weighted sub-access structures. Each element  $a_i$  of the string in third column indicates the weight of  $A_i \in \Gamma^-$  in  $\Gamma_j^w$ . Each element  $b_i$  of the string in fourth column indicates the weight of  $B_i \in \Gamma^+$  in  $\Gamma_j^w$ . Here,  $\Gamma_{77}^- = \{12, 13, 16, 23, 26, 34, 35, 45, 56\}$  and  $\Gamma_{77}^+ = \{14, 15, 24, 25, 36, 46\}$ . The access structures  $\Gamma_3^w$  is isomorphic with  $\Gamma^2$  in Table 2. Therefore,  $\Sigma^3$  can be constructed from the presented scheme in Fig. 2. The scheme  $\Sigma^4$  is presented in Fig. 6. From Theorem 3.3, this decomposition leads to a scheme  $\Sigma$  with  $\sigma(\Sigma) = 8/5$ .

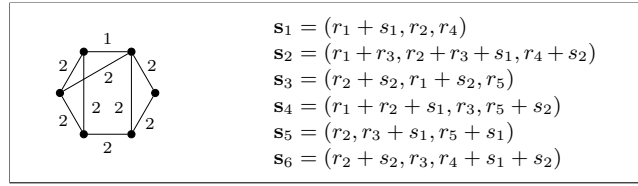


Fig. 6: Scheme  $\Sigma^4$  in Table 7

**Note 4.3.** For the  $(\lambda, \omega)$ -weighted decomposition of Table 7, we have two types of weighted sub-access structures. The weighted graphs indicate weighted sub-access structures as explained in Note 4.2. Here, we also have two sub-access structures for which the weights of all the indicated singleton sets are one but the weight of any other subset is zero.

## 5 Conclusion

The problem of finding the exact value of the optimal information ratios of non-isomorphic graph access structures on six participants has been studied in several papers [28, 27, 30, 23, 14, 15, 20, 12], but the problem has remained unsolved for nine cases. In this paper, we have improved the known upper bounds on the optimal information ratios for seven such access structures, by presenting a linear secret sharing scheme for each of them. For all cases, our improved upper bound matches the recently published lower bound in [12] on the optimal information ratio when the schemes are restricted to be linear. Therefore, our results for these seven cases together with the obtained results in [29, 20, 12] settles the problem of finding optimal linear secret sharing schemes for all nine unsolved graph access structures on six participants. Despite all the research performed to resolve this problem, the exact values of the optimal information ratios for all nine open access structures remains unknown. Further research must be done in order to distinguish between the following two possibilities for each access structure: 1) the optimal linear secret sharing scheme provides the optimal information ratio, in which case the known lower bound needs to be improved or, 2) the optimal secret sharing scheme is non-linear. A summary of our results can be found in Table 1, presented in Section 4.

We point out that we have tried our best to obtain the optimal linear secret sharing scheme using known decomposition techniques for each case. We were successful in six cases but we failed for the last one, for which we had to devise a new decomposition technique, referred to as  $(\lambda, \omega)$ -weighted decomposition. Exploring the true potentials of known techniques, including ours which can be considered as a generalization of all known techniques, deserves further investigations.

## References

- [1] A. Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011.
- [2] G. R. Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference 1979*, 48:313–317, 1979.

- [3] G. R. Blakley and C. Meadows. Security of ramp schemes. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 242–268. Springer, 1984.
- [4] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):107–110, 1997.
- [5] C. Blundo, A. Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology*, 8(1):39–64, 1995.
- [6] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2):123–134, 1991.
- [7] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *Journal of Cryptology*, 5(3):153–166, 1992.
- [8] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology*, 6(3):157–167, 1993.
- [9] L. Csirmaz. Secret sharing on the d-dimensional cube. *Designs, Codes and Cryptography*, 74(3):719–729, 2015.
- [10] L. Csirmaz and P. Ligeti. On an infinite family of graphs with information ratio  $2 - 1/k$ . *Computing*, 85(1):127–136, 2009.
- [11] L. Csirmaz and G. Tardos. Optimal information rate of secret sharing schemes on trees. *IEEE Transactions on Information Theory*, 59(4):2527–2530, 2013.
- [12] O. Farràs, T. Kaced, S. Martin, and C. Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. Cryptology ePrint Archive, Report 2017/919, 2017. <http://eprint.iacr.org/2017/919>.
- [13] O. Farràs, J. R. Metcalf-Burton, C. Padró, and L. Vázquez. On the optimization of bipartite secret sharing schemes. *Designs, Codes and Cryptography*, 63(2):255–271, 2012.
- [14] M. Gharahi and M. Hadian Dehkordi. The complexity of the graph access structures on six participants. *Designs, codes and cryptography*, pages 1–5, 2013.
- [15] M. Gharahi and M. Hadian Dehkordi. Perfect secret sharing schemes for graph access structures on six participants. *Journal of Mathematical Cryptology*, 7(2):143–146, 2013.
- [16] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
- [17] W.-A. Jackson and K. M. Martin. Geometric secret sharing schemes and their duals. *Designs, Codes and Cryptography*, 4(1):83–95, 1994.
- [18] W.-A. Jackson and K. M. Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996.
- [19] E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.

- [20] Q. Li, X. X. Li, X. J. Lai, and K. F. Chen. Optimal assignment schemes for general access structures based on linear programming. *Designs, Codes and Cryptography*, 74(3):623–644, 2015.
- [21] J. Martí-Farré, C. Padró, and L. Vázquez. Optimal complexity of secret sharing schemes with four minimal qualified subsets. *Designs, Codes and Cryptography*, 61(2):167–186, 2011.
- [22] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 46(7):2596–2604, 2000.
- [23] C. Padró, L. Vázquez, and A. Yang. Finding lower bounds on the complexity of secret sharing schemes by linear programming. *Discrete Applied Mathematics*, 161(7):1072–1084, 2013.
- [24] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [25] D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2(4):357–390, 1992.
- [26] D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.
- [27] H.-M. Sun and B.-L. Chen. Weighted decomposition construction for perfect secret sharing schemes. *Computers & Mathematics with Applications*, 43(6):877–887, 2002.
- [28] M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6(2):143–169, 1995.
- [29] M. Van Dijk, W.-A. Jackson, and K. M. Martin. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography*, 15(3):301–321, 1998.
- [30] M. van Dijk, T. Kevenaar, G.-J. Schrijen, and P. Tuyls. Improved constructions of secret sharing schemes by applying  $(\lambda, \omega)$ -decompositions. *Information processing letters*, 99(4):154–157, 2006.