Optimal Complexity of Secret Sharing Schemes with Four Minimal Qualified Subsets*

Jaume Martí-Farré Carles Padró Leonor Vázquez

October 10, 2010

Abstract

The complexity of a secret sharing scheme is defined as the ratio between the maximum length of the shares and the length of the secret. This paper deals with the open problem of optimizing this parameter for secret sharing schemes with general access structures. Specifically, our objective is to determine the optimal complexity of the access structures with exactly four minimal qualified subsets. Lower bounds on the optimal complexity are obtained by using the known polymatroid technique in combination with linear programming. Upper bounds are derived from decomposition constructions of linear secret sharing schemes. In this way, the exact value of the optimal complexity is determined for several access structures in that family. For the other ones, we present the best known lower and upper bounds.

Key words: Secret sharing, Optimization of secret sharing schemes for general access structures.

1 Introduction

A *secret sharing scheme* is a method to distribute a *secret value* into *shares* among a set of *participants* in such a way that only some *qualified subsets* of participants can recover the secret value from their shares. Secret sharing was introduced independently in 1979 by Blakley [5] and Shamir [35], and it is a very important cryptographic primitive that is used as a building block in many different cryptographic protocols. In this work we consider only *unconditionally secure perfect* secret sharing schemes, that is, the shares of the participants in a non-qualified subset must not provide any information at all about the secret.

The qualified subsets form the *access structure* of the secret sharing scheme, which is a monotone increasing family of subsets of participants. That is, any superset of a qualified subset is also qualified. Then an access structure is determined by the collection of its *minimal qualified subsets.*

Ito, Saito and Nishizeki [24] proved, in a constructive way, that every access structure admits a secret sharing scheme. Another general construction was given by Benaloh and Leichter [4]. In those schemes, the shares are much larger than the secret value. Actually, the length of the shares grows exponentially with the number of participants. This is not desirable because the security and efficiency of a system depends on the amount of information that must be kept secret.

[*] This work was partially supported by the Spanish Ministry of Education and Science under projects TIC 2003-00866 and TSI2006-02731.

The *complexity* $\sigma(\Sigma)$ of a secret sharing scheme Σ is defined as the ratio between the maximum length of the shares and the length of the secret. Optimizing this parameter for every given access structure is one of the main open problems in secret sharing. The *optimal complexity* $\sigma(\Gamma)$ of an access structure Γ is defined as the infimum of the complexities of all secret sharing schemes for Γ. Very little is known about the values of $\sigma(\Gamma)$, and there is a huge gap between the best known general lower and upper bounds. Its asymptotic behavior with respect to the number of participants is also unknown.

In a secret sharing scheme, the length of every share is at least the length of the secret [27]. The secret sharing schemes such that all shares have the same length as the secret are said to be *ideal*, and their access structures are called *ideal* as well. The characterization of ideal access structures is another important open problem in secret sharing.

Due to the difficulty of finding general results, both open problems have been studied for several families of access structures as, for instance, access structures with at most five participants [26, 36], the ones defined by graphs [6, 7, 8, 10, 11, 12, 38], bipartite [32] and tripartite [20] access structures, access structures with intersection number equal to one [29], weighted threshold access structures [2], and hierarchical access structures [22]. The ideal access structures in these families have been completely characterized and, for some of them, bounds on the optimal complexity have been given. For instance, the optimal complexity have been determined for all access structures on four participants [36] and for most of the ones on five participants [26]. In addition, the optimal complexity has been determined as well for most of the access structures on six participants defined by graphs [17, 19]. Finally, a great achievement has been obtained recently by Csirmaz and Tardos [16] by determining the optimal complexity of all access structures defined by trees.

Most of the known lower bounds on the optimal complexity have been found by implicitly or explicitly using a combinatorial method based on polymatroids. The parameter $\kappa(\Gamma)$ was introduced in [30] to denote the best lower bound on $\sigma(\Gamma)$ that can be obtained by this method. Most of the upper bounds are derived from constructions of *linear* secret sharing schemes, and hence they are upper bounds on $\lambda(\Gamma)$, that is, the optimal complexity of the linear secret sharing schemes for Γ. More information about the known results on the parameters κ, σ, and λ can be found in [30].

In this work, we try to optimize the complexity of secret sharing schemes for the access structures that have exactly four minimal qualified subsets. The characterization of the ideal access structures in that family was given in [28]. By introducing a reduced form for the access structures, we prove in Section 3 that it is enough to consider sets of at most $2^k - 2$ participants when trying to determine the optimal complexity of the access structures with at most k minimal qualified subsets. Because of that, in this work we study access structures with four minimal qualified subsets on sets with at most 14 participants. We summarize in Section 4.1 the main results from [28] about those access structures. Some constructions of linear secret sharing schemes providing upper bounds on $\lambda(\Gamma)$ for the access with four minimal qualified subsets are presented in Section 4.2. We present in Section 4.3 a linear programming approach to compute $\kappa(\Gamma)$ that has been used as well in other works [14, 15, 21, 34]. By using it, we have been able to determine the value of this parameter for all such access structures on at most nine participants. We implemented a computer program that explored all non-isomorphic reduced access structures with four minimal qualified subsets and found the best lower and upper bounds on $\sigma(\Gamma)$ that can be derived from those results. For several such access structures, the exact value of $\sigma(\Gamma)$ has been determined in this way. For the other ones, upper and lower bounds have been found. The obtained results are summarized in Section 5, where several tables with these values are presented.

2 Preliminaries

2.1 The Complexity of Secret Sharing Schemes

An *access structure* Γ on a set P of *participants* is a monotone increasing family of subsets of P. The subsets in Γ are said to be *qualified*. An access structure is determined by the family $\min \Gamma$ of its minimal qualified subsets. The *redundant* participants in an access structure are those that are not in any minimal qualified subset. An access structure is said to be *connected* if all participants are non-redundant. From now on, all access structures are assumed to be *non-trivial*, that is, to have at least a non-redundant participant.

Let Q be a finite set with a distinguished element $p_0 \in Q$ called *dealer*, and let $P = Q - \{p_0\}$ be the set of participants. Consider a finite set E with a probability distribution on it. For every $p \in Q$, consider a finite set E_p and a surjective mapping $\pi_p \colon E \to E_p$. We notate $E_0 = E_{p_0}$ and $\pi_0 = \pi_{p_0}$. Those mappings induce random variables on the sets E_p. Let $H(E_p)$ denote the Shannon entropy of one of these random variables. For a subset $A = \{p_1, \dots, p_r\} \subseteq Q$, we write $H(E_A)$ for the joint entropy $H(E_{p_1} \dots E_{p_r})$, and a similar convention is used for conditional entropies as, for instance, in $H(E_p|E_A) = H(E_p|E_{p_1} \dots E_{p_r})$.

The mappings π_i define a *secret sharing scheme* Σ with *access structure* Γ on the set P of participants if $H(E_0|E_A) = 0$ if $A \in \Gamma$ while $H(E_0|E_A) = H(E_0)$ if $A \notin \Gamma$. In this situation, every random choice of an element $\mathbf{x} \in E$, according to the given probability distribution, results in a *distribution of shares* $((s_p)_{p \in P}, s_0)$, where $s_p = \pi_p(\mathbf{x}) \in E_p$ is the *share* of the participant $p \in P$ and $s_0 = \pi_0(\mathbf{x}) \in E_0$ is the *shared secret value*.

Since the security of a system decreases with the amount of information that must be kept secret, the length of the shares is an important parameter in secret sharing, whose optimization is the main object of this work. We define the *complexity* of a secret sharing scheme Σ as $\sigma(\Sigma) = \max_{p \in P} H(E_p)/H(E_0)$, that is, the maximum length of the shares in relation to the length of the secret. The value $\rho(\Sigma) = 1/\sigma(\Sigma)$ is called the *information rate* of the scheme. The *optimal complexity* $\sigma(\Gamma)$ of an access structure Γ is defined as the infimum of the complexities $\sigma(\Sigma)$ of the secret sharing schemes Σ for Γ. It is not difficult to check that $H(E_p) \geq H(E_0)$ for every non-redundant participant $p \in P$, and hence $\sigma(\Sigma) \geq 1$. Secret sharing schemes with $\sigma(\Sigma) = 1$ are said to be *ideal* and their access structures are called *ideal* as well.

For a finite field $\mathbb{K}$, a secret sharing scheme Σ is said to be $\mathbb{K}$*-linear* if the sets E and E_p are vector spaces over $\mathbb{K}$, the mappings π_p are $\mathbb{K}$-linear mappings, and the uniform probability distribution is considered in E. By using basic linear algebra, one can check that $\bigcap_{p \in A} \ker \pi_p \subseteq \ker \pi_0$ for every qualified subset $A \in \Gamma$, while $\ker \pi_0 + \bigcap_{p \in A} \ker \pi_p = E$ if $A \notin \Gamma$.

Since all random variables involved in linear secret sharing schemes are uniformly distributed, $H(E_p) = \dim(E_p) \log |\mathbb{K}|$ for every $p \in Q$. Therefore, the complexity of a linear secret sharing scheme Σ is $\sigma(\Sigma) = \max_{p \in P} \dim E_p / \dim E_0$. As a consequence of the general construction in [24], every access structure admits a linear secret sharing scheme. For an access structure Γ, we notate $\lambda(\Gamma)$ for the infimum of the complexities of the linear secret sharing schemes for Γ. Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$.

2.2 Combinatorial Lower Bounds on the Optimal Complexity

Csirmaz [13] pointed out that the lower bounds on the optimal complexity that are derived from the basic properties of Shannon entropy, as the ones in [7, 6, 26] and other works, can be obtained by using polymatroids. This is a consequence of the results by Fujishige [23], who proved that the joint entropies of a family of random variables define a polymatroid. In particular, for a secret sharing scheme Σ on a set P of participants, the mapping $h \colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(A) = H(E_A)/H(E_0)$ satisfies the following properties.

1. $h(\emptyset) = 0$.

2. h is *monotone increasing*: if $A \subseteq B \subseteq Q$, then $h(A) \leq h(B)$.

3. h is *submodular*: $h(A \cup B) + h(A \cap B) \leq h(A) + h(B)$ for every $A, B \subseteq Q$.

4. For every $A \subseteq Q$, either $h(A \cup \{p_0\}) = h(A)$ or $h(A \cup \{p_0\}) = h(A) + 1$.

The first three properties imply that the pair $\mathcal{S}(\Sigma) = (Q, h)$ is a *polymatroid* with *ground set Q* and *rank function h*. The fourth property implies that the dealer p_0 is an *atomic point* of $\mathcal{S}$. For a polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$, we define on the set $P = Q - \{p_0\}$ the access structure

$$\Gamma = \Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P \,:\, h(A \cup \{p_0\}) = h(A)\}.$$

In this situation, we say that $\mathcal{S}$ is a Γ-polymatroid. The access structure Γ of a secret sharing scheme Σ is determined by the associated polymatroid $\mathcal{S} = \mathcal{S}(\Sigma)$ because $\Gamma = \Gamma_{p_0}(\mathcal{S})$. We define as well $\sigma_{p_0}(\mathcal{S}) = \max\{h(\{x\}) \,:\, x \in P\}$. Observe that $\sigma_{p_0}(\mathcal{S}) = \sigma(\Sigma)$ if $\mathcal{S}$ is the polymatroid associated to the secret sharing scheme Σ. For every access structure Γ, we consider the value

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Gamma\text{-polymatroid with } \Gamma = \Gamma_{p_0}(\mathcal{S})\}.$$

This parameter was introduced in [30]. Observe that $\sigma(\Sigma) = \sigma_{p_0}(\mathcal{S}(\Sigma)) \geq \kappa(\Gamma)$ for every secret sharing scheme Σ with access structure Γ, and hence $\kappa(\Gamma) \leq \sigma(\Gamma)$. Every lower bound on the optimal complexity $\sigma(\Gamma)$ that can be obtained by using the so-called Shannon inequalities on the entropy function is in fact a lower bound on $\kappa(\Gamma)$.

2.3 Constructive Upper Bounds on the Optimal Complexity

Upper bounds on the optimal complexity $\sigma(\Gamma)$ are obtained by presenting explicit constructions of secret sharing schemes for Γ. Several *decomposition methods* to combine some given secret sharing schemes into a new one have been presented in [11, 19, 26, 33, 37, 38]. The most efficient schemes that are obtained by these methods are in most cases linear. Therefore, upper bounds on $\lambda(\Gamma)$ are obtained.

The constructions that are used in this paper to find upper bounds on $\sigma(\Gamma)$ are obtained by using the decomposition method presented by Stinson in [38], which is described in the following. Let Γ be an access structure on a set P of participants. A collection $(\Gamma_1, \ldots, \Gamma_s)$ of (not necessarily different) access structures on P is an *ℓ-decomposition* of Γ if $\Gamma = \bigcup_{i=1}^{s} \Gamma_i$ and

$$\ell = \min_{A \in \min \Gamma} |\{i \,:\, A \in \min \Gamma_i\}| \,.$$

For every $i = 1, \ldots, s$, consider a $\mathbb{K}$-linear secret sharing scheme Σ_i with access structure Γ_i and set of secrets $E_{i,0} = \mathbb{K}^{r_i}$. Let $\mathcal{S}_i = \mathcal{S}(\Sigma_i) = (Q, h_i)$ be the polymatroid associated to the secret sharing scheme Σ_i. We assume that $h_i(\{p\}) = 0$ if p is a redundant participant of Γ_i. As a consequence of [38, Theorem 2.1], there exists a $\mathbb{K}$-linear secret sharing scheme Σ with access structure Γ, set of secrets $E_0 = \mathbb{K}^{\ell r}$, where $r = \operatorname{lcm}\{r_1, \ldots, r_s\}$, and complexity

$$\sigma(\Sigma) = \frac{1}{\ell} \max_{p \in P} \left(\sum_{i=1}^{s} h_i(\{p\}) \right).$$

Nevertheless, these decompositions method do not provide in general *optimal* linear secret sharing schemes, that is, with complexity equal to $\lambda(\Gamma)$. There exists the possibility that some of the upper bounds that we present here could be improved by using the algorithm to construct linear secret sharing schemes proposed by van Dijk [18], but this has not been explored in this work.

3 Reduced Access Structures

We present in this section a reduction procedure that can be applied to any given access structure. The parameters κ, σ, and λ that are studied here are invariant under this reduction, and hence it is enough to study them on reduced access structures. Several general properties about duality and minors of access structures, and also about different kinds of special participants, are needed to prove the results in this section.

Let Γ be an access structure on a set P. The access structure $\Gamma^* = \{A \subseteq P \,:\, P - A \notin \Gamma\}$ is called the *dual access structure of* Γ. If Σ is a $\mathbb{K}$-linear secret sharing scheme with access structure Γ, then there exists a $\mathbb{K}$-linear scheme Σ^* with access structure Γ^* and complexity $\sigma(\Sigma^*) = \sigma(\Sigma)$ [25]. This implies that $\lambda(\Gamma^*) = \lambda(\Gamma)$. Actually, Σ can be seen as a linear code, and the linear scheme Σ^* is the one constructed from the dual code. In addition, it was proved in [30] that $\kappa(\Gamma^*) = \kappa(\Gamma)$. On the other hand, no relation between the values of $\sigma(\Gamma)$ and $\sigma(\Gamma^*)$ is known.

For an access structure Γ on a set P and a subset $Z \subseteq P$, we define the access structures $\Gamma \backslash Z$ and Γ / Z on the set $P - Z$ by $\Gamma \backslash Z = \{A \subseteq P - Z \,:\, A \in \Gamma\}$ and $\Gamma / Z = \{A \subseteq P - Z \,:\, A \cup Z \in \Gamma\}$. Every access structure that can be obtained from Γ by repeatedly applying the operations $\backslash$ and $/$ is called a *minor of the access structure* Γ. If Z_1 and Z_2 are disjoint subsets then $(\Gamma \setminus Z_1)/Z_2 = (\Gamma/Z_2) \setminus Z_1$, and $(\Gamma \setminus Z_1) \setminus Z_2 = \Gamma \setminus (Z_1 \cup Z_2)$, and $(\Gamma/Z_1)/Z_2 = \Gamma/(Z_1 \cup Z_2)$. Therefore, every minor of Γ is of the form $(\Gamma \setminus Z_1)/Z_2$ for some disjoint subsets $Z_1, Z_2 \subseteq P$. In addition, $(\Gamma \setminus Z)^* = \Gamma^*/Z$ and $(\Gamma/Z)^* = \Gamma^* \setminus Z$.

Proposition 3.1 ([30])**.** *The minors of an ideal access structure are ideal as well. In addition, if* Γ' *is a minor of* Γ*, then* $\lambda(\Gamma') \leq \lambda(\Gamma)$*, and* $\sigma(\Gamma') \leq \sigma(\Gamma)$*, and* $\kappa(\Gamma') \leq \kappa(\Gamma)$*.*

A *privileged* participant for the access structure Γ is a participant $p \in P$ with $\{p\} \in \Gamma$. The *co-privileged* participants are those that are privileged for the dual access structure. Clearly, a participant $p \in P$ is co-privileged if and only if $p \in A$ for every $A \in \min \Gamma$. Two participants $p, q \in P$ are said to be *equivalent* for the access structure Γ if $\{p, q\} \not\subseteq A$ for every $A \in \min \Gamma$, and $A \cup \{p\} \in \min \Gamma$ if and only if $A \cup \{q\} \in \min \Gamma$ for every $A \subseteq P - \{p, q\}$. Two participants are *co-equivalent* for Γ if they are equivalent for the dual access structure Γ^*. It is not difficult to check that $p, q \in P$ are co-equivalent for Γ if and only if, for every $A \in \min \Gamma$, either $\{p, q\} \subseteq A$ or $\{p, q\} \cap A = \emptyset$, that is, if and only if the minimal qualified sets containing p coincide with those containing q.

Proposition 3.2. *Let* Γ *be an access structure on a set* P *and let* $p \in P$ *be a privileged participant for* Γ*. Then* $\sigma(\Gamma \setminus \{p\}) = \sigma(\Gamma)$ *and* $\sigma(\Gamma^*/\{p\}) = \sigma(\Gamma^*)$*. The same equalities apply for the parameters* κ *and* λ*.*

Proof. By Proposition 3.1, $\sigma(\Gamma \setminus \{p\}) \leq \sigma(\Gamma)$ and $\sigma(\Gamma^*/\{p\}) \leq \sigma(\Gamma^*)$, and the same applies for the parameters κ and λ. In a (linear) secret sharing scheme for Γ, the participant p can receive the secret value as its share. Therefore, $\sigma(\Gamma \setminus \{p\}) = \sigma(\Gamma)$ and $\lambda(\Gamma \setminus \{p\}) = \lambda(\Gamma)$. Given a (linear) secret sharing scheme Σ' for $\Gamma^*/\{p\}$, a (linear) secret sharing scheme Σ for Γ^* is constructed as follows. We can suppose that E_0 is a commutative group. To share a secret value $s \in E_0$, a random value $s_1 \in E_0$ is distributed into shares among the participants in $P - \{p\}$ according to Σ' and the participant p receives $s_2 = s - s_1 \in E_0$ as its share. This implies that $\sigma(\Gamma^*/\{p\}) = \sigma(\Gamma^*)$ and $\lambda(\Gamma^*/\{p\}) = \lambda(\Gamma^*)$.

Consider a special participant $p_0 \notin P$ (the dealer) and $Q = P \cup \{p_0\}$. Let $\mathcal{S}' = (Q - \{p\}, h')$ be a $(\Gamma \setminus \{p\})$-polymatroid. Consider the polymatroid $\mathcal{S} = (Q, h)$ defined by $h(A) = h'(A)$ and $h(A \cup \{p\}) = h'(A \cup \{p_0\})$ for every $A \subseteq Q - \{p\}$. Clearly, $\mathcal{S}$ is a Γ-polymatroid, and hence $\kappa(\Gamma \setminus \{p\}) = \kappa(\Gamma)$. Finally, by the duality properties of this parameter, $\kappa(\Gamma^*/\{p\}) = \kappa((\Gamma \setminus \{p\})^*) = \kappa(\Gamma \setminus \{p\}) = \kappa(\Gamma) = \kappa(\Gamma^*)$. □

Lemma 3.3. *Let Γ be an access structure on a set P. Consider a participant $p \in P$ and let $Z \subseteq P - \{p\}$ be the set of the participants different from p that are co-equivalent to p for Γ. Then $\sigma(\Gamma/Z) = \sigma(\Gamma)$.*

Proof. By Proposition 3.1, $\sigma(\Gamma/Z) \le \sigma(\Gamma)$. Let Σ' be a secret sharing scheme for Γ/Z. A secret sharing scheme Σ for Γ can be constructed from Σ' as follows. First, a collection of shares for the secret value according to Σ' is obtained. Every participant in $P - \{p\}$ receives the same share in Σ as in Σ', while the share corresponding to p according to Σ' is distributed among the participants in $Z \cup \{p\}$ by using an (m, m)-threshold scheme, where $m = |Z| + 1$. Specifically, we can assume that the set E_p is a commutative group and the share s_p for p according to Σ' is split by taking random values $u_q \in E_p$ with $s_p = \sum_{q \in Z \cup \{p\}} u_q$. Clearly, $\sigma(\Sigma) = \sigma(\Sigma')$ and this implies that $\sigma(\Gamma) = \sigma(\Gamma/Z)$. □

Proposition 3.4. *Let Γ be an access structure on a set P and let $p, q \in P$ be two equivalent participants for Γ. Then $\sigma(\Gamma \setminus \{q\}) = \sigma(\Gamma)$ and $\sigma(\Gamma^*/\{q\}) = \sigma(\Gamma^*)$. The same equalities apply for the parameters κ and λ.*

Proof. By Proposition 3.1, $\sigma(\Gamma \setminus \{q\}) \le \sigma(\Gamma)$ and $\sigma(\Gamma^*/\{q\}) \le \sigma(\Gamma^*)$, and the same applies for the parameters κ and λ. If Σ' is a secret sharing scheme for $\Gamma \setminus \{q\}$, a secret sharing scheme Σ for Γ with $\sigma(\Sigma) = \sigma(\Sigma')$ is obtained by giving to q the same share as the one received by p. Clearly, Σ is linear if Σ' is so. Therefore, $\sigma(\Gamma \setminus \{q\}) = \sigma(\Gamma)$ and $\lambda(\Gamma \setminus \{q\}) = \lambda(\Gamma)$. Let $\mathcal{S}' = (Q - \{q\}, h')$ be a $(\Gamma \setminus \{q\})$-polymatroid, and consider the polymatroid $\mathcal{S} = (Q, h)$ such that $h(A) = h'(A)$ and $h(A \cup \{q\}) = h'(A \cup \{p\})$ for every $A \subseteq Q - \{q\}$. Clearly, $\mathcal{S}$ is a Γ-polymatroid, and this implies that $\kappa(\Gamma \setminus \{q\}) = \kappa(\Gamma)$. By duality, $\lambda(\Gamma^*/\{q\}) = \lambda(\Gamma^*)$ and $\kappa(\Gamma^*/\{q\}) = \kappa(\Gamma^*)$. The corresponding equality for the parameter σ is a direct consequence of Lemma 3.3. □

At this point, we proceed to introduce the reduction procedure for access structures (Definition 3.5) and to prove that the parameters κ, σ, and λ are invariant under it (Proposition 3.6). Some notation is needed.

For every positive integer k, consider the set

$$\mathcal{U}_k = \{b_{k-1} \dots b_1 b_0 \,:\, b_i \in \{0,1\}\} - \{0 \dots 0, 1 \dots 1\},$$

which has $2^k - 2$ elements, and, for $i = 0, \dots, k-1$, consider

$$\mathcal{U}_k^i = \{b_{k-1} \dots b_1 b_0 \in \mathcal{U}_k \,:\, b_i = 1\} \subseteq \mathcal{U}_k.$$

For a subset $U \subseteq \mathcal{U}_k$, we define the access structure $\Gamma_k(U)$ on U by

$$\Gamma_k(U) = \{A \subseteq U \,:\, U \cap \mathcal{U}_k^i \subseteq A \text{ for some } i = 0, \dots, k-1\}.$$

Every minimal qualified subset of $\Gamma_k(U)$ is of the form $U \cap \mathcal{U}_k^i$ for some $i = 0, \dots, k-1$. Therefore, the number of minimal qualified subsets of $\Gamma_k(U)$ is at most k, and in some cases it is less than k. For instance, the access structure $\Gamma_k(\mathcal{U}_k^i)$ has exactly $k-1$ minimal qualified subsets.

In order to illustrate the use of this notation, we analyze in more detail the case $k = 4$, which is actually the one that is mainly considered in this paper. For a more compact presentation, we identify the elements in $\mathcal{U}_4$ with the integers that have the corresponding binary representations, and we write them in the hexadecimal system. That is,

$$\mathcal{U}_4 = \{0001_2, \dots, 1110_2\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, \mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D}, \mathsf{E}\}.$$

Then the subsets $\mathcal{U}_4^i$ can be written as

- $\mathcal{U}_4^0 = \{1,3,5,7,9,\mathsf{B},\mathsf{D}\}$,
- $\mathcal{U}_4^1 = \{2,3,6,7,\mathsf{A},\mathsf{B},\mathsf{E}\}$,
- $\mathcal{U}_4^2 = \{4,5,6,7,\mathsf{C},\mathsf{D},\mathsf{E}\}$, and
- $\mathcal{U}_4^3 = \{8,9,\mathsf{A},\mathsf{B},\mathsf{C},\mathsf{D},\mathsf{E}\}$.

For instance, for $U = \{3,5,6,9,\mathsf{A},\mathsf{C}\} \subseteq \mathcal{U}_4$, the minimal qualified subsets of the access structure $\Gamma_4(U)$ are $U \cap \mathcal{U}_4^0 = \{3,5,9\}$, $U \cap \mathcal{U}_4^1 = \{3,6,\mathsf{A}\}$, $U \cap \mathcal{U}_4^2 = \{5,6,\mathsf{C}\}$, and $U \cap \mathcal{U}_4^3 = \{9,\mathsf{A},\mathsf{C}\}$.

Let Γ be an access structure on a set P with exactly k minimal qualified subsets $\min\Gamma = \{A_0, A_1, \dots, A_{k-1}\}$. The *incidence vector* of a participant $p \in P$ is the bit sequence $\chi(p,\Gamma) = b_{k-1}\dots b_1 b_0$, where $b_i = 1$ if $p \in A_i$ and $b_i = 0$ otherwise. The *weight* $w(p)$ of the participant $p \in P$ in Γ is defined as the Hamming weight of its incidence vector. Observe that a participant with $\chi(p,\Gamma) = 1\dots1$ is co-privileged for Γ, and that two participants are co-equivalent for Γ if they have the same incidence vector. In addition, every participant with $\chi(p,\Gamma) = 0\dots0$ is redundant. Therefore, if Γ has neither co-privileged nor redundant participants and every two different participants are not co-equivalent, we can identify every participant to its incidence vector, and hence the set of participants can be identified to a subset of $\mathcal{U}_k$. This leads us to the following definition.

Definition 3.5. Let Γ be an access structure on a set P of participants with exactly k minimal qualified subsets $\min\Gamma = \{A_0, A_1, \dots, A_{k-1}\}$. Consider the set

$$\chi(P,\Gamma) = \{\chi(p,\Gamma) \,:\, p \in P\} - \{0\dots00, 1\dots11\} \subseteq \mathcal{U}_k.$$

Then the access structure $\Gamma_k(\chi(P,\Gamma))$ on the set $\chi(P,\Gamma)$ is called the *reduced form* of Γ. We say that Γ is a *reduced* access structure if $\Gamma_k(\chi(P,\Gamma))$ is isomorphic to Γ.

Observe that a reduced access structure has neither co-privileged nor redundant participants and every two different participants are not co-equivalent.

Proposition 3.6. *Let Γ be an access structure on a set P with exactly k minimal qualified subsets and let $\Gamma' = \Gamma_k(\chi(P,\Gamma))$ be its reduced form. Then $\sigma(\Gamma) = \sigma(\Gamma')$ and the same applies to the parameters κ and λ.*

Proof. A direct consequence of Propositions 3.2 and 3.4. □

Therefore, in order to determine the values of the parameters κ, σ, and λ for the access structures with k minimal qualified subsets, it is enough to consider the access structures of the form $\Gamma_k(P)$ with $P \subseteq \mathcal{U}_k$. That is, we have to consider only access structures on at most $2^k - 2$ participants. For a set $P \subseteq \mathcal{U}_k$, we notate $\sigma(P) = \sigma(\Gamma_k(P))$. We have then a mapping $\sigma\colon \mathcal{P}(\mathcal{U}_k) \to \mathbb{R}$. The same notation is used for the parameters κ and λ.

Proposition 3.7. *The mapping $\sigma\colon \mathcal{P}(\mathcal{U}_k) \to \mathbb{R}$ is monotone increasing, and the same applies to the mappings defined by the parameters κ and λ.*

Proof. If $P_1 \subseteq P_2 \subseteq \mathcal{U}_k$, then $\Gamma_k(P_1)$ is a minor of $\Gamma_k(P_2)$. Specifically, $\Gamma_k(P_1) = \Gamma_k(P_2)/Z$, where $Z = P_2 - P_1$. Therefore, $\sigma(P_1) \le \sigma(P_2)$. □

Finally, observe that every permutation τ on the set of indices $\{0,1,\dots,k-1\}$ induces a permutation (that we also denote by τ) on $\mathcal{U}_k$. Clearly, the access structures $\Gamma_k(P)$ and $\Gamma_k(\tau P)$ are isomorphic for every $P \subseteq \mathcal{U}_k$. For instance, if $k = 4$, the permutation $\tau = 3210$ transforms $P_1 = \{3,7,8,\mathsf{D},\mathsf{E}\} \subseteq \mathcal{U}_4$ into $P_2 = \{1,7,\mathsf{B},\mathsf{C},\mathsf{E}\} \subseteq \mathcal{U}_4$, and hence $\Gamma_4(P_1) \cong \Gamma_4(P_2)$.

4 Access Structures with at Most Four Minimal Qualified Subsets

Our objective is to find out as much as possible about the values of the optimal complexities of the access structures with at most four minimal qualified subsets. To this end, we are interested also on the values of the parameters κ and λ for those access structures. As we saw in Section 3, it is enough to determine the values of these parameters for the reduced access structures of the form $\Gamma_4(P)$ with $P \subseteq \mathcal{U}_4$, that is, to determine $\kappa(P)$, $\sigma(P)$, and $\lambda(P)$ for $P \subseteq \mathcal{U}_4$.

4.1 Known Results

The ideal access structures with at most four minimal qualified subsets were characterized in [28]. In particular, as a consequence of the results in [28], an access structure $\Gamma_4(P)$ is ideal that if and only if $\lambda(P) = \kappa(P) = 1$ and, in addition, $\kappa(P) \geq 3/2$ if $\Gamma_4(P)$ is not ideal. The results in [28] are described in more detail in the following by using the representation for such access structures that has been introduced in Section 3. This makes it possible to present the results in [28] in a more compact way.

Every access structure with at most two minimal qualified subsets, admits an ideal $\mathbb{K}$-linear secret sharing scheme for every finite field $\mathbb{K}$. The next proposition is a characterization of the ideal access structures with three minimal qualified subsets.

Proposition 4.1 ([28]). *Consider $P_1 = \{3, 5, 6\} \subseteq \mathcal{U}_3$ and $P_2 = \{1, 2, 3, 4\} \subseteq \mathcal{U}_3$. Then $\Gamma_3(P_1)$ and $\Gamma_3(P_2)$ admit ideal $\mathbb{K}$-linear secret sharing schemes for every finite field with $|\mathbb{K}| \geq 3$. In addition, an access structure with three minimal qualified subsets is ideal if and only if its reduced form is isomorphic to an access structure of the form $\Gamma_3(P)$ with $P \subseteq P_i$ for some $i = 1, 2$.*

The optimal complexities of all access structure with three minimal qualified subsets were determined in [28]. Actually, such an access structure Γ is either ideal with $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 1$ or it satisfies $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 3/2$.

Proposition 4.2 ([28]). *Let Γ be a non-ideal access structure with three minimal qualified subsets. Then $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 3/2$. Moreover, for every finite field $\mathbb{K}$, there exists a $\mathbb{K}$-linear secret sharing scheme Σ for Γ with set of secrets $E_0 = \mathbb{K}^2$ such that, if h is the rank function of the polymatroid $\mathcal{S}(\Sigma)$ defined by Σ, then $h(\{p\}) = 1$ if the participant p has weight $w(p) = 1$ or $w(p) = 3$, while $h(\{p\}) = 3/2$ whenever $w(p) = 2$.*

We present in the following the characterization of the ideal access structures with four minimal qualified subsets.

Proposition 4.3 ([28]). *Consider the following subsets $P_i \subseteq \mathcal{U}_4$: $P_1 = \{1, 2, 3, 4, 8, \mathsf{C}\}$, $P_2 = \{1, 6, \mathsf{A}, \mathsf{C}, \mathsf{E}\}$, $P_3 = \{1, 2, 3, 4, 7, 8\}$, $P_4 = \{3, 5, 6, 9, \mathsf{A}, \mathsf{C}\}$, and $P_5 = \{7, \mathsf{B}, \mathsf{D}, \mathsf{E}\}$. Then $\Gamma_4(P_i)$ admits an ideal $\mathbb{K}$-linear secret sharing scheme for every $i = 1, 2, 3, 4$ and for every finite field with $|\mathbb{K}| \geq 4$. Moreover, an access structure with at most four minimal qualified subsets is ideal if and only if its reduced form is isomorphic to an access structure of the form $\Gamma_4(P)$ with $P \subseteq P_i$ for some $i = 1, 2, 3, 4$.*

The next proposition contains the only result about the optimal complexity of the non-ideal access structures with four minimal qualified subsets that can be derived from the results in [28]. The main objective of this work is to find better bounds on $\sigma(\Gamma)$ for the access structures in that family.

Proposition 4.4 ([28]). *Let Γ be a non-ideal access structure with four minimal qualified subsets. Then $3/2 \leq \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma) \leq 2$.*

4.2 Upper Bounds on the Optimal Complexity

By using the decomposition method by Stinson [38] that is described in Section 2.3, we present in this section some upper bounds on $\lambda(\Gamma)$, and hence on $\sigma(\Gamma)$, for access structures Γ with four minimal qualified subsets.

Unless otherwise is stated, we consider from now on only subsets $P \subseteq \mathcal{U}_4$ such that $\Gamma_4(P)$ has exactly four minimal qualified subsets, that is, $\min \Gamma_4(P) = \{B_0, B_1, B_2, B_3\}$, where $B_i = P \cap \mathcal{U}_4^i$. The substructures $\Lambda_{i,j}(P)$ and $\Phi_i(P)$ of $\Gamma_4(P)$ are defined by $\min \Lambda_{i,j}(P) = \{B_i, B_j\}$ and $\min \Phi_i(P) = \min \Gamma_4(P) - \{B_i\}$.

Our first result is an improvement of the general upper bound given in [28] (Proposition 4.4).

Proposition 4.5. $\sigma(\mathcal{U}_4) \leq \lambda(\mathcal{U}_4) \leq 11/6$.

Proof. The four substructures $\Phi_i = \Phi_i(\mathcal{U}_4)$ form a 3-decomposition of $\Gamma = \Gamma_4(\mathcal{U}_4)$ because every $B_j \in \min \Gamma$ is in the three substructures Φ_i with $i \neq j$. By Proposition 4.2, there exists a linear secret sharing scheme Σ_i for the structure Φ_i such that, if $\mathcal{S}_i = (Q, h_i)$ is the polymatroid associated to Σ_i, then

- $h_i(\{p\}) = 0$ if p has weight 0 in Φ_i, that is, if p is redundant for Φ_i,
- $h_i(\{p\}) = 1$ if the weight of p in Φ_i is 1 or 3, and
- $h_i(\{p\}) = 3/2$ if p has weight 2 in Φ.

Then, by using the results described in Section 2.3, there exists a linear secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = \max_{p \in \mathcal{U}_4} \left(\sum_{i=0}^{3} h_i(\{p\}) \right) / 3$. Consider the participant $0001_2 = 1$. Clearly, $h_0(\{1\}) = 0$ while $h_i(\{1\}) = 1$ if $i = 1, 2, 3$. Therefore, $\sum_{i=0}^{3} h_i(\{1\}) = 3$. By symmetry, $\sum_{i=0}^{3} h_i(\{p\}) = 3$ for every participant p with weight 1 in Γ. For a participant with weight 2 like for instance the participant $0011_2 = 3$, we have $h_0(\{3\}) = h_1(\{3\}) = 1$ and $h_2(\{3\}) = h_3(\{3\}) = 3/2$. Hence, $\sum_{i=0}^{3} h_i(\{3\}) = 5$. Finally $h_3(\{7\}) = 1$ while $h_i(\{7\}) = 3/2$ if $i = 0, 1, 2$, and hence $\sum_{i=0}^{3} h_i(\{7\}) = 11/2$. Therefore, $\sigma(\Sigma) = \max_{p \in \mathcal{U}_4} \left(\sum_{i=0}^{3} h_i(\{p\}) \right) / 3 = 11/6$. □

The next two propositions provide upper bounds on $\lambda(P)$ depending on the number of substructures $\Phi_i(P)$ that are ideal.

Proposition 4.6. *If $P \subseteq \mathcal{U}_4$ is such that at least one of the substructures $\Phi_i(P)$ is ideal, then $\sigma(P) \leq \lambda(P) \leq 5/3$.*

Proof. Assume that $\Phi_0 = \Phi_0(P)$ is an ideal access structure. Then $(\Phi_0, \Phi_0, \Lambda_{0,1}, \Lambda_{0,2}, \Lambda_{0,3})$ is a 3-decomposition of $\Gamma = \Gamma_4(P)$ formed by access structures that admit ideal linear secret sharing schemes over every large enough finite field. Then a linear secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = 5/3$ is obtained from this decomposition. □

Proposition 4.7. *If $P \subseteq \mathcal{U}_4$ is such that at least two of the substructures $\Phi_i(P)$ are ideal, then $\sigma(P) \leq \lambda(P) \leq 3/2$.*

Proof. Assume that the substructures Φ_0 and Φ_1 of $\Gamma = \Gamma_4(P)$ are ideal. Then $(\Phi_0, \Phi_1, \Lambda_{0,1})$ is a 2-decomposition of Γ consisting of three vector space access structures. From this decomposition, a secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = 3/2$ can be constructed. □

The upper bound in the following proposition depends on the configuration of the participants with weights 2 and 3 in the structure. Of course, the bound applies as well to the structures that satisfy the condition after permuting the indices of the minimal qualified subsets.

Proposition 4.8. *If $P \cap \{\mathsf{5}, \mathsf{7}, \mathsf{A}, \mathsf{B}, \mathsf{D}, \mathsf{E}\} = \emptyset$, then $\sigma(P) \leq \lambda(P) \leq 3/2$.*

Proof. Observe that $(\Lambda_{0,1}, \Lambda_{1,2}, \Lambda_{2,3}, \Lambda_{0,3})$ is a 2-decomposition of $\Gamma = \Gamma_4(P)$. We assert that every $p \in P$ is redundant in at least one of the substructures in the decomposition. Clearly this is the case for the participants with weight 1 in Γ. The participants $1100_2 = \mathsf{C}$, $1001_2 = \mathsf{9}$, $0011_2 = \mathsf{3}$, and $0110_2 = \mathsf{6}$ are redundant, respectively, in the structures $\Lambda_{0,1}$, $\Lambda_{1,2}$, $\Lambda_{2,3}$, and $\Lambda_{0,3}$. This proves our assertion. Therefore, the given decomposition provides a secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = 3/2$. □

Finally, the last two propositions in this section present upper bounds on $\lambda(P)$ depending on the number of participants with weight 3.

Proposition 4.9. *If $|P \cap \{\mathsf{7}, \mathsf{B}, \mathsf{D}, \mathsf{E}\}| \leq 1$, then $\sigma(P) \leq \lambda(P) \leq 5/3$.*

Proof. By symmetry, we can suppose that $P \cap \{\mathsf{B}, \mathsf{D}, \mathsf{E}\} = \emptyset$. Consider the 3-decomposition of $\Gamma = \Gamma_4(P)$ given by $(\Gamma_1, \dots, \Gamma_5) = (\Phi_3, \Phi_3, \Lambda_{0,3}, \Lambda_{1,3}, \Lambda_{2,3})$. For $i = 1, \dots, 5$, there exists a linear secret sharing Σ_i for Γ_i such that Σ_i is ideal if $i = 3, 4, 5$ and $\sigma(\Sigma_i) = 3/2$ if $i = 1, 2$. In addition, if $\mathcal{S}_i = (Q, h_i)$ is the polymatroid associated to Σ_i, then the following properties are satisfied.

- If p has weight 1 in Γ, then $\sum_{i=1}^{5} h_i(\{p\}) \leq 5$.
- If p has weight 2 in Γ and $p \in B_3$, then $h_1(\{p\}) = h_2(\{p\}) = 1$ because p has weight 1 in Φ_3, and hence $\sum_{i=1}^{5} h_i(\{p\}) = 5$.
- If p has weight 2 in Γ and $p \notin B_3$, then $h_1(\{p\}) = h_2(\{p\}) = 3/2$ and $h_i(\{p\}) = 0$ for some $i = 3, 4, 5$. Then $\sum_{i=1}^{5} h_i(\{p\}) = 2(3/2) + 2 = 5$.
- If $p = 0111_2 = \mathsf{7}$, then p has weight 3 in Φ_3, and hence $h_1(\{p\}) = h_2(\{p\}) = 1$. This implies that $\sum_{i=1}^{5} h_i(\{p\}) = 5$.

Therefore, there exists a linear secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = 5/3$. □

Proposition 4.10. *If $|P \cap \{\mathsf{7}, \mathsf{B}, \mathsf{D}, \mathsf{E}\}| = 2$, then $\sigma(P) \leq \lambda(P) \leq 7/4$.*

Proof. Assume that $P \cap \{\mathsf{7}, \mathsf{E}\} = \emptyset$ and consider the 2-decomposition $(\Phi_1, \Phi_2, \Lambda_{1,2})$ of $\Gamma = \Gamma_4(P)$ and the corresponding linear secret sharing schemes Σ_i for $i = 1, 2, 3$. If p has weight 3 in Γ, then $p = 1011_2 = \mathsf{B}$ or $p = 1101_2 = \mathsf{D}$. Observe that $h_1(\{\mathsf{B}\}) = 3/2$ and $h_2(\{\mathsf{B}\}) = 1$, while $h_1(\{\mathsf{D}\}) = 1$ and $h_2(\{\mathsf{D}\}) = 3/2$. Therefore, $\sum_{i=1}^{3} h_i(\{p\}) = 3/2 + 1 + 1 = 7/2$ if $w(p) = 3$. If $p = 1001_2 = \mathsf{9}$, then $h_1(\{p\}) = h_2(\{p\}) = 3/2$ and $h_3(\{p\}) = 0$. If $p = 0110_2 = \mathsf{6}$, then $h_i(\{p\}) = 1$ for every $i = 1, 2, 3$. If p is any other participant with weight 2, then p has weight 1 in Φ_1 or in Φ_2, and hence $\sum_{i=1}^{3} h_i(\{p\}) = 3/2 + 1 + 1 = 7/2$. Finally, $h_i(\{p\}) \leq 1$ for every $i = 1, 2, 3$ if p has weight 1 in Γ. □

4.3 Lower Bounds on the Optimal Complexity

For every given access structure Γ, the value $\kappa(\Gamma)$ is the solution to a linear programming problem. Nevertheless, the number of variables and constraints is exponential on the number of participants, and hence it is only possible to determine $\kappa(\Gamma)$ by using linear programming if the number of participants is not too large. Actually, we have been able to determine in this way the value of $\kappa(\Gamma)$ for every access structure Γ with four minimal qualified sets on at most nine participants. In this section, we discuss this linear programming approach.

By ordering in some way the elements in $\mathcal{P}(Q)$, the rank function of a polymatroid $\mathcal{S} = (Q, h)$ can be seen as a vector $h = (h(A))_{A \subseteq Q} \in \mathbb{R}^m$, where $m = 2^{|Q|}$. The axioms of polymatroids impose a number of linear constraints on the vector h. If, in addition, we assume that $\mathcal{S}$ is a Γ-polymatroid for some access structure on $P = Q - \{p_0\}$, then other linear constraints on h appear. We obtain in this way the feasible region $\Omega(\Gamma) \subseteq \mathbb{R}^{m+1}$ of our linear programming problem. Namely, a vector $(h, \kappa) \in \mathbb{R}^{m+1}$ is in $\Omega(\Gamma)$ if and only if h is the rank function of a Γ-polymatroid and $h(\{i\}) \leq \kappa$ for every $i \in P$. Since every access structure Γ admits a Γ-polymatroid, $\Omega(\Gamma) \neq \emptyset$. Obviously $\kappa(\Gamma)$ is the solution to the problem:

$$\begin{array}{ll} \text{Minimize} & \kappa \\ \text{subject to} & (h, \kappa) \in \Omega(\Gamma). \end{array}$$

The number of constraints to define the feasible region can be reduced by using the following characterization of polymatroids given by Matúš [31]. Namely, $h : \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid $\mathcal{S} = (Q, h)$ if and only if

1. $h(\emptyset) = 0$,

2. $h(Q - \{i\}) \leq h(Q)$ for every $i \in Q$, and

3. $h(A \cup \{i\}) + h(A \cup \{j\}) \geq h(A \cup \{i, j\}) + h(A)$ for every $i, j \in Q$ with $i \neq j$ and for every $A \subseteq Q - \{i, j\}$.

Moreover, we can further reduce the number of constraints by taking into account that a polymatroid $\mathcal{S} = (Q, h)$ is a Γ-polymatroid if and only if

1. $h(\{p_0\}) = 1$,

2. $h(A \cup \{p_0\}) = h(A)$ if $A \subseteq P$ is a minimal qualified subset of Γ, and

3. $h(B \cup \{p_0\}) = h(B) + 1$ if $B \subseteq P$ is a maximal unqualified subset of Γ.

5 Determining the Optimal Complexity of the Access Structures with Four Minimal Qualified Subsets

In this section we present our results about the values of the considered parameters for access structures with exactly four minimal qualified subsets. As we explained in Section 4.1, these values are known for access structures with less that four minimal qualified subsets. Specifically, we present in this section all the information that we have been able to determine about the values of $\kappa(P)$, $\sigma(P)$, and $\lambda(P)$ for the subsets $P \subseteq \mathcal{U}_4$ such that the access structure $\Gamma_4(P)$ has exactly four minimal qualified subsets. In order to simplify the notation, we represent the subsets of $\mathcal{U}_4$ by the increasingly ordered sequence of their elements. For instance, we write $\mathsf{136ABE}$ for the subset $\{\mathsf{1}, \mathsf{3}, \mathsf{6}, \mathsf{A}, \mathsf{B}, \mathsf{E}\}$.

A computer program has been used to explore all non-isomorphic access structures $\Gamma_4(P)$ with $P \subseteq \mathcal{U}_4$ that have four minimal qualified subsets. First, the sequences representing subsets of $\mathcal{U}_4$ that define access structures with less than four minimal qualified subsets are discarded. Next, the remaining sequences are ordered, first by their length then lexicographically. Finally, a single representant of every isomorphism class is selected in the following way: at every step, the first non-selected subset is picked and all other subsets that can be obtained from it by permuting the indices of the minimal qualified subsets are removed from the list. In this way, we obtain an ordered list of all non-isomorphic reduced access structures with four minimal subsets. In addition, for every isomorphism class, we have selected the lexicographically smallest representant. By following this procedure, a list of subsets $P \subseteq \mathcal{U}_4$ defining all non-isomorphic reduced access structures with four minimal qualified subsets is obtained, and we find out that there are 606 such access structures.

By using the linear programming approach presented in Section 4.3, we have been able to determine the values of $\kappa(P)$ for all such subsets with $|P| \leq 9$. We observe that, for every one of these subsets, $\kappa(P) \in \{1, 3/2, 5/3, 7/4\}$. By using these values in combination with Propositions 3.7, 4.3, and 4.4, the upper bounds in Section 4.2, and the results by Stinson [36] and Jackson and Martin [26] about access structures on four and five participants, we can determine the value of $\sigma(P)$ for a number of subsets $P \subseteq \mathcal{U}_4$ in the aforementioned list, and lower and upper bounds on this parameter for the other subsets. All these values and bounds are presented in nine tables. The subsets for which we determined the exact value of $\sigma(P)$ are listed in the first three tables. Namely, the subsets defining ideal access structures are listed in Table 1. The subsets in Table 2 are such that $\kappa(P) = \sigma(P) = \lambda(P) = 3/2$, while the ones in Table 3 satisfy $\kappa(P) = \sigma(P) = \lambda(P) = 5/3$. We were not able to determine the exact value of $\sigma(P)$ for the subsets in the remaining five tables, and only lower and upper bounds are given. In all these tables, the value of $\kappa(P)$ attains the lower bound whenever $|P| \leq 9$. In addition, one of the anonymous referees computed the exact values of $\kappa(P)$ for some subsets with $|P| = 10, 11$. For these subsets, which are marked in the tables with an asterisk (*), the value of $\kappa(P)$ coincides as well with the lower bound. In particular, this implies that the value of $\kappa(P)$ has been determined for all subsets appearing in Tables 4, 5 and 6.

In the following, we describe in more detail how the bounds in those tables have been obtained. Table 1 is derived from the characterization of the ideal access structures with at most four minimal subsets from [28], which is presented here in Proposition 4.3. The optimal complexities of all access structures on four participants and of most of the ones on five participants were determined, respectively, by Stinson [36] and by Jackson and Martin [26]. In particular, the optimal complexities of all reduced access structures with four minimal qualified subsets that are defined from sets with $|P| \leq 5$ can be found in those works. For all such subsets, $\kappa(P) = \sigma(P) = \lambda(P)$. For some subsets with $6 \leq |P| \leq 9$, the value of $\kappa(P)$ that has been obtained by using linear programming matches one of the upper bounds on $\lambda(P)$ given in Section 4.2. Clearly, $\kappa(P) = \sigma(P) = \lambda(P)$ and the value of $\sigma(P)$ is determined for those subsets. In addition, in some cases in which the value of $\kappa(P)$ was not found by using linear programming, the lower bound on $\kappa(P)$ coincides with the upper bound on $\lambda(P)$, and hence the exact value of $\sigma(P)$ is obtained. These sets appear in Table 3. Consider, for instance, the set $P = \mathsf{123456789A}$. By Proposition 3.7, we know that $\kappa(P) \geq 5/3$ because it contains the set $P' = \mathsf{1234579A}$, which has $\kappa(P') = 5/3$. On the other hand, $\lambda(P) \leq 5/3$ by Proposition 4.9. Of course, similar methods have been applied to find the lower and upper bounds for the subsets appearing in Tables 4 to 9. For example, take $P = \mathsf{123456789B}$. By Proposition 4.10, $\lambda(P) \leq 7/4$. The permutation $\tau = 2013$ on the indices of the minimal qualified subsets transforms $P' = \mathsf{13249E}$ into $\tau P' = \mathsf{24568B} \subseteq P$, and hence $\kappa(P) \geq \kappa(\tau P') = \kappa(P') = 5/3$ by Proposition 3.7.

6 Open Problems

The problem of determining the optimal complexity of *all* access structures with four minimal qualified subsets remains unsolved. The main question at this point is whether it is possible to find all values of $\sigma(P)$ with $P \subseteq \mathcal{U}_4$ by using the tools in this paper or new techniques are needed. This question can be rephrased actually in terms of the parameters that have been studied in this paper. If $\kappa(P) = \sigma(P) = \lambda(P)$ for every $P \subseteq \mathcal{U}_4$, then the techniques deployed

$\lvert P\rvert = 4$	$\lvert P\rvert = 5$	$\lvert P\rvert = 6$
1248	12348	123478
16AC	12478	12348C
35AC	16ACE	3569AC
7BDE	3569A	

Table 1: $\kappa(P) = \sigma(P) = \lambda(P) = 1$

$\lvert P\rvert = 4$	$\lvert P\rvert = 5$	$\lvert P\rvert = 6$	$\lvert P\rvert = 7$	$\lvert P\rvert = 8$
16AD	1249A	123458	1234568	12345678
359E	1249E	12348D	1234578	123458AC
	1259C	12349A	123458A	123478BC
	125AC	12349C	123458B	
	127BC	1234BC	12345AC	
	135AC	1235AC	123478B	
	136AC	1237BC	123478C	
	167AC	12478B	12347BC	
	167AD	12479E	12348DE	
	16ADE	1249AB	12349AB	
	16BDE	1249AD		
	17BDE	12569A		
	3569E	1259CD		
	3579E	167ACE		
	357AC			
	35ADE			
	35BDE			
	37BDE			

Table 2: $\kappa(P) = \sigma(P) = \lambda(P) = 3/2$

in this paper would be enough to determine all values of $\sigma(P)$. Only that they should be used in a more powerful way, and maybe new methods to construct linear secret sharing schemes, as for instance the one proposed in [18], are required. On the other hand, if there existed subsets $P \subseteq \mathcal{U}_4$ such that $\kappa(P) < \sigma(P)$ or $\sigma(P) < \lambda(P)$, then new techniques would be necessary. In the first case, non-Shannon information inequalities would be needed to find tight lower bounds on $\sigma(P)$. In the second case, constructions of non-linear secret sharing schemes would be required to find tight upper bounds on $\sigma(P)$. Actually there exist in the literature examples of access structures such that $\kappa(\Gamma) < \sigma(\Gamma)$ [1] or $\sigma(\Gamma) < \lambda(\Gamma)$ [3]. Examples of graph-based access structures with $\kappa(\Gamma) < \lambda(\Gamma)$ have been presented in [14].

Acknowlegments

We are deeply grateful to one of the anonymous referees who thoroughly and carefully revised our paper, finding even a mistake in our tables, and helped in great measure to improve the presentation of our results.

$\|P\| = 5, 6$	$\|P\| = 7$	$\|P\| = 8$	$\|P\| = 9, 10, 11$
1259E	123458E	1234568B	12345678B
125BC	123459E	1234569E	12345679A
1359E	12345AD	1234578B	12345679E
136AD	123478D	1234578E	12345689B
136BC	123479A	1234579A	12345689E
	123479C	1234579E	1234569AB
	123479E	123457AC	1234569AD
12349E	12349AD	123457AD	12345789E
12359E	12349BE	1234589E	1234578AC
1235BC	12349CE	123458AD	1234578AD
12479A	12349DE	123458BE	1234579AC
1249BE	123569E	123459AD	123459ABC
12569E	12356BC	123459AE	123459ABE
1256BC	123579C	123459BE	123459ACE
12579C	123579E	12345ABC	123479ABC
12579E	12357AC	12345ACE	1235679AC
1257AC	12357BC	123479AB	123569ACD
1257BC	12359CE	123479AC	
1259CE	12359DE	123479BC	
1259DE	1235ACD	12349ABD	123456789A
125BCD	12479AB	12349ACD	123456789E
125BCE	12479AC	12349CDE	12345679AC
13569E	12479AD	1235679C	12345689AD
1356AD	1249ABD	1235679E	1234569ABC
13579E	125679C	123567BC	
1357AC	125679E	123569AD	
135ACE	12567BC	123569BC	123456789AC
1367AC	12569AD	123569CD	
1367AD	12569BC	123569CE	
1367BC	12569CE	12359CDE	
136ACD	12579CD	12479ABC	
136ADE	1257ACD	125679AC	
136BCD	1259CDE	12569ACD	
136BCE	135679E	12569BCD	
	13567AC	135679AC	
	13567AD	13569ACE	
	13569AD		
	13569AE		
	1356ABC		
	1356ACE		
	136ACDE		

Table 3: $\kappa(P) = \sigma(P) = \lambda(P) = 5/3$

$\|P\| = 6$	$\|P\| = 7$	$\|P\| = 8$	$\|P\| = 9, 10$
12359C	1234589	12345689	123456789
1249AC	123459A	1234569A	12345689A
12569C	12349AC	12345789	1234569AC
125ACD	12349BC	1234578A	
13569A	12349CD	123459AB	
1356AC	123569A	123459AC	12345689AC*
135ABC	123569C	12349ABC	
136ACE	12359CD	1235679A	
167ABC	1249ABC	123569AC	
167ABD	125679A	167ABCDE	
167ADE	12569AC		
167BDE	12569CD		
35679A	135679A		
35679E	13569AC		
3569AD	167ABCD		
356BDE	167ABCE		
357BDE	167ABDE		
	35679AC		
	3567BDE		

Table 4: $3/2 = \kappa(P) \leq \sigma(P) \leq \lambda(P) \leq 5/3$

$\|P\| = 6$	$\|P\| = 7$	$\|P\| = 8$	$\|P\| = 9$
3569BE	135ABCD	125679AB	1235679AB
357ABC	35679AB	135679AB	
357ACE	35679AD	35679ABC	
	3569ADE		

Table 5: $3/2 = \kappa(P) \leq \sigma(P) \leq \lambda(P) \leq 7/4$

$\|P\| = 6$	$\|P\| = 7$	$\|P\| = 8$	$\|P\| = 9, 10$
3579BE	35679BE	35679ABD	35679ABCD
357ADE	3569BDE	35679ADE	35679ABDE
37BCDE	3579BDE	35679BDE	
	357ABCD	357ABCDE	
	357ABDE		35679ABCDE*

Table 6: $3/2 = \kappa(P) \leq \sigma(P) \leq \lambda(P) \leq 11/6$

$\lvert P\rvert = 6, 7$	$\lvert P\rvert = 8$	$\lvert P\rvert = 9$	$\lvert P\rvert = 10, 11, 12$
125ADE	123458BD	1234568BD	123456789B
135ADE	12345ABD	1234569BE	12345679AB*
	12345ADE	12345789B	12345679AD
	123478CD	1234578AB	12345689BD*
1234BCD	123479AD	1234578AE	12345689BE
1235ADE	123479CD	1234579AB	1234569ABD
1235BCD	123479CE	1234579AD	1234569ADE
1235BCE	12349ADE	1234579AE	1234578ABC
1249ADE	12349BCD	123457ABC	1234578ACE*
12569BE	12349BCE	123457ACE	1234579ABC*
12569DE	123569BE	123458ADE	1234579ACE
1256BCD	123569DE	123459ABD	123459ABCD*
12579BC	12356BCD	123459ADE	123459ABCE*
12579CE	123579BC	12345ABCD	1235679ABC*
1257ABC	123579CD	12345ABCE	1235679ACD*
1257ACE	123579CE	123479ACD	123569ACDE*
125ACDE	12357ABC	12349ABCD	
13569BE	12357ACD	12349ACDE	
1356ABD	12357ACE	1235679AD	123456789AB*
1356ADE	1235ACDE	1235679BC	123456789AD
1357ABC	1249ABCD	1235679CD	12345679ABC
1357ACE	125679AD	1235679CE	12345689ADE
135ABCE	125679BC	123569ADE	1234569ABCD
1367ABC	125679CD	123569BCD	
1367ACD	125679CE	123569BCE	
1367ACE	12569ADE	123569CDE	123456789ABC
	12569BCE	125679ABC	
	12569CDE	125679ACD	
	135679AD	12569ACDE	
	135679AE	135679ABC	
	13567ABC	135679ACE	
	13567ACE		
	13569ADE		
	1356ABCD		
	1356ABCE		

Table 7: $5/3 \leq \kappa(P) \leq \sigma(P) \leq \lambda(P) \leq 7/4$

$\lvert P\rvert = 6$	$\lvert P\rvert = 7$	$\lvert P\rvert = 8$	$\lvert P\rvert = 9, 10$
127BCD 137BCE	1237BCD 1257BCD 1367ABD 1367BCD 1367BCE	12357BCD 12579BCD 13567ABD 1357ABCD 1367ABCD 1367ABCE	123579BCD 135679ABD 13567ABCD
			135679ABCD

Table 8: $5/3 \leq \kappa(P) \leq \sigma(P) \leq \lambda(P) \leq 11/6$

$\lvert P\rvert = 6, 7$	$\lvert P\rvert = 8$	$\lvert P\rvert = 9$	$\lvert P\rvert = 10$	$\lvert P\rvert = 11, 12, 13, 14$
124BDE 125BDE 127BDE 135BDE 136BDE 137BDE	12345BDE 123478BD 123478DE 123479BE 123479DE 12347BCD 12347BDE 12349BDE 1234BCDE 12356BDE 123579BE 123579DE 12357ADE 12357BCE 12357BDE 1235BCDE 1237BCDE 12478BDE 12479ABD 12479ADE 12479BDE 1249ABDE 125679BE 125679DE 12567BCD 12567BDE 12569BDE 1256BCDE 12579BCE 12579BDE 12579CDE 1257ABCD 1257ABDE 1257ACDE 1257BCDE 135679BE 13567ADE 13567BDE 13569BDE 1356ABDE 13579BDE 1357ABCE 1357ABDE 135ABCDE 1367ABDE 1367ACDE 1367BCDE	123456BDE 1234578BD 1234578BE 1234579BE 123457ABD 123457ADE 123457BDE 123458BDE 123459BDE 12345ABDE 123478BCD 123478BDE 123479ABD 123479ADE 123479BCD 123479BCE 123479BDE 123479CDE 12347BCDE 12349ABDE 12349BCDE 1235679BE 1235679DE 123567BCD 123567BDE 123569BDE 12356BCDE 123579BCE 123579BDE 123579CDE 12357ABCD 12357ABDE 12357ACDE 12357BCDE 12479ABCD 12479ABDE 1249ABCDE 125679ABD 125679ADE 125679BCD 125679BCE 125679BDE 125679CDE 12567BCDE 12569BCDE 12579BCDE 1257ABCDE 135679ABE 135679ADE 135679BDE 13567ABCE 13567ABDE 1356ABCDE 1357ABCDE 1367ABCDE	12345678BD 12345679BE 1234567BDE 1234568BDE 1234569BDE 12345789BD 12345789BE 1234578ABD 1234578ADE 1234578BDE 1234579ABD 1234579ABE 1234579ADE 1234579BDE 123457ABCD 123457ABCE 123457ABDE 123459ABDE 12345ABCDE 123478BCDE 123479ABCD 123479ABDE 123479ACDE 123479BCDE 12349ABCDE 1235679ABD 1235679ADE 1235679BCD 1235679BCE 1235679BDE 1235679CDE 123567BCDE 123569BCDE 123579BCDE 12357ABCDE 12479ABCDE 125679ABCD 125679ABDE 125679ACDE 125679BCDE 135679ABCE 135679ABDE 13567ABCDE	123456789BD 123456789BE 12345678BDE 12345679ABD 12345679ADE 12345679BDE 12345689BDE 1234569ABDE 12345789BDE 1234578ABCD 1234578ABDE 1234579ABCD 1234579ABCE 1234579ABDE 123457ABCDE 123459ABCDE 123479ABCDE 1235679ABCD 1235679ABDE 1235679ACDE 1235679BCDE 125679ABCDE 135679ABCDE
1234BDE 1235BDE 1237BDE 12478BD 12479BE 1247BDE 1249BDE 1256BDE 12579BE 12579DE 1257ADE 1257BCE 1257BDE 125BCDE 127BCDE 1356BDE 13579BE 1357ADE 1357BDE 135ABDE 1367ADE 1367BDE 136BCDE 137BCDE				123456789ABD 123456789ADE 123456789BDE 12345679ABCD 12345679ABDE 1234569ABCDE 1234578ABCDE 1234579ABCDE 1235679ABCDE
				123456789ABCD 123456789ABDE 12345679ABCDE
				123456789ABCDE

Table 9: $7/4 \leq \kappa(P) \leq \sigma(P) \leq \lambda(P) \leq 11/6$

References

[1] A. Beimel, N. Livne, C. Padró. Matroids Can Be Far From Ideal Secret Sharing. *Fifth Theory of Cryptography Conference, TCC 2008, Lecture Notes in Comput. Sci.* **4948** (2008) 194–212.

[2] A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *SIAM J. Discrete Math.* **22** (2008) 360–397.

[3] A. Beimel, E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.* **34** (2005) 1196–1215.

[4] J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88. Lecture Notes in Comput. Sci.* **403** (1990) 27–35.

[5] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.* **48** (1979) 313–317.

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

[7] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92, Lecture Notes in Comput. Sci.* **740** (1993) 148–167.

[8] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.

[9] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.

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

[11] E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology* **5** (1992) 153–166.

[12] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. Cryptology* **6** (1993) 157–168.

[13] L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.

[14] L. Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptogr.* **53** (2009) 195–209.

[15] L. Csirmaz, P. Ligeti. On an infinite family of graphs with information ratio $2 - 1/k$. *Computing* **85** (2009) 127–136.

[16] L. Csirmaz, G. Tardos. Secret sharing on trees: problem solved. Manuscript (2009). Available at *Cryptology ePrint Archive*, `http://eprint.iacr.org/2009/071`.

[17] M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.* **6** (1995) 143–169.

[18] M. van Dijk. A Linear Construction of Secret Sharing Schemes. *Des. Codes Cryptogr.* **12** (1997) 161–201.

[19] M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls. Improved constructions of secret sharing schemes by applying (λ, ω)-decompositions. *Inf. Process. Lett.* **99** (2006) 154–157.

[20] O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *Advances in Cryptology, Eurocrypt 2007, Lecture Notes in Comput. Sci.* **4515** (2007) 448–465.

[21] O. Farràs, J.R. Metcalf-Burton, C. Padró, L. Vázquez. On the Optimization of Bipartite Secret Sharing Schemes. *Fourth International Conference on Information Theoretic Security ICITS 2009, Lecture Notes in Computer Science* **5973** (2010) 93–109.

[22] O. Farràs, C. Padró. Ideal Hierarchical Secret Sharing Schemes. *Seventh IACR Theory of Cryptography Conference, TCC 2010, Lecture Notes in Computer Science* **5978** (2010) 219–236.

[23] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* **39** (1978) 55–72.

[24] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87* (1987) 99–102.

[25] W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95.

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

[27] E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.

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

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

[30] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *Journal of Mathematical Cryptology*, to appear (2010).

[31] F. Matúš. Adhesivity of polymatroids. *Discrete Math.* **307** (2007) 2464–2477.

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

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

[34] C. Padró, L. Vázquez. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Ninth Latin American Theoretical Informatics Symposium, LATIN 2010, Lecture Notes in Computer Science* **6034** (2010) 344–355.

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

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

[37] D.R. Stinson. New general lower bounds on the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92. Lecture Notes in Comput. Sci.* **740** (1993) 168-182.

[38] D.R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory.* **40** (1994) 118–125.