Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming [*]

Carles Padró[†] Leonor Vázquez[‡] An Yang[†]

[†] School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore
{carlespl, yang0246}@ntu.edu.sg

[‡] ORIONEARTH, Oil Reservoir Integration on Earth, Mexico
leobaki@hotmail.com

August 14, 2012

Abstract

Optimizing the maximum, or average, length of the shares in relation to the length of the secret for every given access structure is a difficult and long-standing open problem in cryptology. Most of the known lower bounds on these parameters have been obtained by implicitly or explicitly using that every secret sharing scheme defines a polymatroid related to the access structure. The best bounds that can be obtained by this combinatorial method can be determined by using linear programming, and this can be effectively done for access structures on a small number of participants.

By applying this linear programming approach, we improve some of the known lower bounds for the access structures on five participants and the graph access structures on six participants for which these parameters were still undetermined. Nevertheless, the lower bounds that are obtained by this combinatorial method are not tight in general. For some access structures, they can be improved by adding to the linear program non-Shannon information inequalities as new constraints. We obtain in this way new separation results for some graph access structures on eight participants and for some ports of non-representable matroids. Finally, we prove that, for two access structures on five participants, the combinatorial lower bound cannot be attained by any linear secret sharing scheme.

Key words. Secret sharing, linear programming, polymatroid, non-Shannon information inequalities.

1 Introduction

Secret sharing, which was independently introduced by Blakley [7] and Shamir [40], deals with methods to distribute a *secret value* among a set of participants, in such a way that only some *qualified subsets* can recover the secret value. In this work we consider only *unconditionally secure perfect secret sharing schemes*, in which the shares of the participants in an unqualified

[*] A previous version of this paper appeared in the Proceedings of LATIN 2010 [38]. Several new results have been added to the current version, as the ones in Sections 6 and 7. Moreover, the overall presentation of the paper has been greatly improved. This work was partially done while the first and second authors were with Universitat Politècnica de Catalunya, Barcelona. Their work was partially supported by the Spanish Ministry of Education and Science under project MTM2009-07694. The work of the first and third authors is supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

set do not provide any information about the secret. The collection of qualified subsets is called the *access structure* of the secret sharing scheme. The reader that is unfamiliar with secret sharing will find more information about the topic in the surveys by Stinson [41] and by Beimel [2]. In addition, some of the concepts appearing in this paper are described in more detail in [31].

The length of the shares, when compared to the length of the secret value, is usually considered as a measure of the efficiency of a secret sharing scheme. Specifically, the *complexity*, or *information ratio*, of a secret sharing scheme is defined as the ratio between the maximum length of the shares and the length of the secret. The *average complexity*, or *average information ratio*, is defined analogously from the average length of the shares. In every secret sharing scheme, the length of every share is at least the length of the secret [30]. A secret sharing scheme is said to be *ideal* if all shares have the same length as the secret. 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. The *optimal average complexity* $\widetilde{\sigma}(\Gamma)$ is defined analogously. Clearly, $1 \leq \widetilde{\sigma}(\Gamma) \leq \sigma(\Gamma)$.

Determining the values of these parameters is one of the main open problems in secret sharing. Even though many partial results have been found, important questions remain unsolved. In particular, the asymptotic behavior of these parameters is unknown and there is a huge gap between the best known upper and lower bounds. Because of the difficulty of finding general results, this problem has been considered for several particular families of access structures in [8, 13, 14, 15, 16, 23, 29, 32] among other works. And a great achievement has been obtained recently by Csirmaz and Tardos [15] by determining the optimal complexity of all access structures defined by trees.

In a *linear secret sharing scheme*, the secret value and the shares are vectors over some finite field, and every share is the value of a given linear map on some random vector. The homomorphic properties of linear secret sharing schemes are very important for some of the main applications of secret sharing as, for instance, secure multiparty computation. On the other hand, linear secret sharing schemes are obtained when applying the best known techniques to construct efficient schemes, as the decomposition method by Stinson [42]. Because of that, it is also interesting to consider the parameters $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, the infimum of the (average) complexities of all *linear* secret sharing schemes for Γ. Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$. In fact, almost all known upper bounds on the optimal complexity are upper bounds on λ, and the same applies to the corresponding parameters for the average optimal complexity. Even though non-linear secret sharing schemes have been proved to be in general more efficient than the linear ones [3, 6], not many examples of access structures with $\sigma(\Gamma) < \lambda(\Gamma)$ are known.

On the other hand, Csirmaz [12] explained how most of the known lower bounds on the optimal complexity have been found by implicitly or explicitly using a combinatorial method based on the connection between the Shannon entropy and polymatroids presented by Fujishige [24]. The best known asymptotic lower bound [12] was obtained by using this method. The parameter $\kappa(\Gamma)$ was introduced in [31] to denote the best lower bound on $\sigma(\Gamma)$ that can be obtained by this method. We introduce here the corresponding parameter $\widetilde{\kappa}(\Gamma)$ for the combinatorial lower bounds on the optimal average complexity.

As far as we know, $\kappa(\Gamma) = \lambda(\Gamma)$ for all access structures whose optimal complexity $\sigma(\Gamma)$ has been determined. This is due of course to the techniques that have been most used until now. Namely, the combinatorial method, which provide lower bounds on κ, and several decomposition methods, which provide almost always linear secret sharing schemes, and hence upper bounds on λ. In particular, these are the methods used by Jackson and Martin [29] to determine the optimal (average) complexities of almost all 180 non-isomorphic access structures on five participants. The same techniques were used by van Dijk [16] to find the the optimal complexities of almost all 112 non-isomorphic graph access structures on six participants. Some improvements in the upper bounds for the unsolved cases were presented in [11, 19].

Determining the values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ for a given access structure Γ is a linear program. Both the number of variables and of constraints grow exponentially in the number of participants. Moreover, Csirmaz [14, Section 1.2] pointed out that the system of constraints is overdetermined. Nevertheless, linear programming can be used to compute $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ for access structures on a small number of participants. This method has been applied on access structures with four minimal qualified subsets [32] and on bipartite access structures [23].

The use of linear programming, whenever it is possible, to compute $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ has two useful advantages. First, it does not only provide a lower bound on the optimal (average) complexity, but the best bound that can be obtained by using that combinatorial method. That is, other techniques are needed if the obtained lower bound is not tight. And second, after solving the linear program, a polymatroid attaining the optimal value of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ is given, which may facilitate the search for optimal secret sharing schemes.

In this paper, we present the results of such a computation on the access structures on five participants and the graph access structures on six participants whose optimal complexities have not been previously determined. Several known lower bounds are improved and, in a few cases, the value of the optimal (average) complexity is determined. After the publication of the previous version of this paper [38], Gharahi and Dehkordi [25] presented lower bounds on the optimal complexities of some graph access structures. Their bounds coincide with the values of $\kappa(\Gamma)$ that we computed by linear programming, but a different proof is given. For one of those access structures, an upper bound is given in [25] that makes it possible to determine $\sigma(\Gamma)$.

The lower bound $\kappa(\Gamma)$ on the optimal complexity is not tight in general. The first found examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$ were the ports of the Vamos matroid [4]. An infinite family of graph access structures with $\kappa(\Gamma) < \lambda(\Gamma)$ was presented by Csirmaz [14]. These results are proved, respectively, by using the non-Shannon information inequality by Zhang and Yeung [43] and the Ingleton inequality [26]. These and other known information inequalities, as for instance the ones in [20, 35, 21, 22], are linear inequalities, and hence they can be added as constraints to the linear program computing $\kappa(\Gamma)$. For some access structures, better lower bounds on $\sigma(\Gamma)$ (or on $\lambda(\Gamma)$ if the Ingleton inequality is used) are obtained in this way. Nevertheless, Beimel and Orlov [5] proved that all known non-Shannon information inequalities cannot improve our knowledge on the asymptotic behavior of the optimal (average) complexity.

We checked that, for the aforementioned access structures on five participants and graph access structures on six participants, no better lower bounds on $\lambda(\Gamma)$ can be obtained by adding the Ingleton inequality to the linear program. Nevertheless, we found in this way three graph access structures on eight participants with $\kappa(\lambda) < \lambda(\Gamma)$. By using in the same way the non-Shannon information inequalities from [20, 43], we present other examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$. As in [4], they are ports of non-representable matroids.

Finally, we analyze in more detail two of the access structures on five participants and we prove, by using other techniques, that there is no linear secret sharing scheme for those access structures with complexity equal to $\kappa(\Gamma)$. For one of them, we prove the same result for the average complexity. In particular, this implies that the techniques used by Jackson and Martin [29] are not sufficient to determine the optimal (average) complexities of all access structures on five participants.

2 Polymatroids and Secret Sharing

We use $\mathcal{P}(Q)$ to denote the power set of a set Q. A *polymatroid* is a pair (Q, f), where Q is a finite set, and f is a map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

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

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

3. f is *submodular*: $f(A \cup B) + f(A \cap B) \le f(A) + f(B)$ for all $A, B \subseteq Q$.

The set Q and the map f are called, respectively, the *ground set* and the *rank function* of the polymatroid. A polymatroid is said to be *integer* if its rank function is integer-valued. A *matroid* M is an integer polymatroid $M = (Q, f)$ such that $f(A) \le |A|$ for every $A \subseteq Q$. The *independent sets* of M are the subsets $A \subseteq Q$ with $f(A) = |A|$.

Let $(V_i)_{i \in Q}$ be a family of subspaces of some vector space E. Then the map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $f(A) = \dim(\sum_{i \in A} V_i)$ for every $A \subseteq Q$. The polymatroids that can be defined in this way from a family of vector subspaces are called *linear.* If $\mathcal{S} = (Q, f)$ is a polymatroid, the polymatroids of the form (Q, cf) for some real number $c > 0$ are called the *multiples* of $\mathcal{S}$. The multiples of a linear polymatroid are called *poly-linear*.

For a finite set Q, consider a family of discrete random variables $(S_i)_{i \in Q}$, where S_i is defined on a set E_i. For every $A \subseteq Q$, we use S_A to denote the random variable $(S_i)_{i \in A}$ on the set $\prod_{i \in A} E_i$, and $H(S_A)$ will denote its Shannon entropy. The map $h\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(A) = H(S_A)$ if $\emptyset \neq A \subseteq Q$ is the rank function of a polymatroid with ground set Q. This connection between Shannon entropy and polymatroids was discovered by Fujishige [24]. Every polymatroid that can be defined in this way from a family of random variables is called *entropic*. The multiples of an entropic matroid are said to be *poly-entropic.*

An *access structure* Γ on a set P of *participants* is a monotone increasing family of subsets of P, which are called the *qualified sets*. Since every superset of a qualified set is qualified, an access structure Γ is determined by the family $\min \Gamma$ of its minimal qualified sets. In a *connected* access structure, every participant is in a minimal qualified set. Only connected access structures are considered in this paper.

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 and, for every $i \in Q$, consider a finite set E_i and a surjective map $\pi_i\colon E \to E_i$. The tuple $\Sigma = (\pi_i)_{i \in Q}$ induce a family $(S_i)_{i \in Q}$ of discrete random variables on the sets $(E_i)_{i \in Q}$. Consider the polymatroid (Q, h) given by $h(A) = H(S_A)$ for every $A \subseteq Q$. In this situation, the tuple $\Sigma = (\pi_i)_{i \in Q}$ is a *secret sharing scheme* with *access structure* Γ on the set of participants P if $h(\{p_0\}) > 0$ and, for every $A \subseteq P$, the following properties are satisfied.

1. $h(A \cup \{p_0\}) = h(A)$ if $A \in \Gamma$.

2. $h(A \cup \{p_0\}) = h(A) + h(\{p_0\})$ 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* $(s_i)_{i \in Q}$, where $s_i = \pi_i(\mathbf{x}) \in E_i$ is the *share* of the participant $i \in P$ and $s_{p_0} = \pi_{p_0}(\mathbf{x}) \in E_{p_0}$ is the *shared secret value.* The polymatroid $\mathcal{S}(\Sigma) = (Q, f)$ defined by $f(A) = h(A)/h(\{p_0\})$ for every $A \subseteq Q$ is called *polymatroid associated to the secret sharing scheme* Σ.

The *complexity* of a secret sharing scheme Σ is defined as $\sigma(\Sigma) = \max_{i \in P} h(\{i\})/h(\{p_0\})$, that is, the maximum length of the shares in relation to the length of the secret. The *average complexity* is defined by $\widetilde{\sigma}(\Sigma) = (1/n) \sum_{i \in P} h(\{i\})/h(\{p_0\})$, where $n = |P|$ is the number of participants. It is not difficult to check that $h(\{i\}) \geq h(\{p_0\})$ for every participant $i \in P$, and hence $\sigma(\Sigma) \geq \widetilde{\sigma}(\Sigma) \geq 1$. Secret sharing schemes with $\sigma(\Sigma) = 1$ are said to be *ideal* and their access structures are called *ideal* as well.

Ito, Saito and Nishizeki [27] proved that there exists a secret sharing scheme for every access structure. 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 for Γ. The *optimal average complexity* $\widetilde{\sigma}(\Gamma)$ is defined analogously.

A secret sharing scheme Σ is said to be *linear* if the sets E and E_i are vector spaces over some finite field $\mathbb{K}$, the maps π_i are $\mathbb{K}$-linear, and the uniform probability distribution is considered on E. For every $i \in Q$, consider the subspace $V_i = (\ker \pi_i)^{\perp}$ of the dual space E^*. Then $h(A) = H(S_A) = \log(|\mathbb{K}|) \dim(\sum_{i \in A} V_i)$, and hence the polymatroid (Q, h) is poly-linear. By reversing this argument, it can be easily proved that every linear polymatroid is poly-entropic.

As a consequence of the general construction in [27], 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. We consider as well the corresponding parameter $\widetilde{\lambda}(\Gamma)$ for the average complexity.

Csirmaz [12] used the aforementioned connection between Shannon entropy and polymatroids to provide a unified description for the methods previously used to find most of the known lower bounds on the optimal complexity. Namely, they can be obtained by using the fact that the access structure of a secret sharing scheme implies certain restrictions on the polymatroid derived from the random variables involved in the scheme. More details about this combinatorial method to obtain lower bounds on the optimal complexity are given in the following.

An element $p_0 \in Q$ is said to be an *atomic point* of the polymatroid $\mathcal{S} = (Q, f)$ if $f(\{p_0\}) = 1$ and, for every $A \subseteq Q$, either $f(A \cup \{p_0\}) = f(A)$ or $f(A \cup \{p_0\}) = f(A) + 1$. For a polymatroid $\mathcal{S} = (Q, f)$ with an atomic point $p_0 \in Q$, we define on the set $P = Q - \{p_0\}$ the access structure

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

which is clearly a monotone increasing family of subsets of P. For an access structure Γ on P, a polymatroid $\mathcal{S}$ with ground set $Q = P \cup \{p_0\}$ is said to be a Γ*-polymatroid* if p_0 is an atomic point of $\mathcal{S}$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$. Obviously, if Σ is a secret sharing scheme with access structure Γ, then the associated polymatroid $\mathcal{S}(\Sigma) = (Q, f)$ is a Γ-polymatroid. If $\mathcal{S}$ is a matroid, then the access structure $\Gamma_{p_0}(\mathcal{S})$ is called the *port of the matroid* $\mathcal{S}$ *at the point* p_0. If Σ is an ideal secret sharing scheme, then its associated polymatroid $\mathcal{S}(\Sigma)$ is a matroid, and hence the access structure of Σ is a matroid port [9].

For a polymatroid $\mathcal{S} = (Q, f)$ and $p_0 \in Q$, we define $\sigma_{p_0}(\mathcal{S}) = \max\{f(\{i\}) \,:\, i \in P\}$ and $\widetilde{\sigma}_{p_0}(\mathcal{S}) = (1/n) \sum_{i \in P} f(\{i\})$, where $P = Q - \{p_0\}$ and $n = |P|$. Clearly, $\sigma(\Sigma) = \sigma_{p_0}(\mathcal{S}(\Sigma))$ and $\widetilde{\sigma}(\Sigma) = \widetilde{\sigma}_{p_0}(\mathcal{S}(\Sigma))$ for every secret sharing scheme Σ. Moreover, from the discussion in this section it is clear that, for every access structure Γ,

$$\sigma(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a poly-entropic } \Gamma\text{-polymatroid}\} \tag{1}$$

and

$$\lambda(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a poly-linear } \Gamma\text{-polymatroid}\}, \tag{2}$$

and the analogous properties apply to $\widetilde{\sigma}(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$. Therefore, the parameter

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}, \tag{3}$$

which was introduced in [31], is a lower bound on the optimal complexity. Moreover, it is the best lower bound that can be obtained by the combinatorial technique that has been used to compute most of the known lower bounds. The parameter $\widetilde{\kappa}(\Gamma)$, which is introduced here for the first time, is defined analogously and it is a lower bound on the optimal average complexity.

For an access structure Γ on a set P, the *dual access structure* Γ^* is defined by $\Gamma^* = \{A \subseteq P : P - A \notin \Gamma\}$. From every linear secret sharing scheme for an access structure Γ, a linear scheme with the same (average) complexity can be obtained for the dual access structure Γ^* [18, 28], and hence $\lambda(\Gamma^*) = \lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma^*) = \widetilde{\lambda}(\Gamma)$. In addition, it was proved in [31] that $\kappa(\Gamma^*) = \kappa(\Gamma)$ and, by using the same arguments, it is not difficult to check that $\widetilde{\kappa}(\Gamma^*) = \widetilde{\kappa}(\Gamma)$. Nevertheless, the behavior of the parameters σ, $\widetilde{\sigma}$ with respect to duality is unknown.

3 Linear Programming Approach

We discuss here how the values $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ can be obtained by solving linear programming problems. Nevertheless, the number of variables and of constraints is exponential in the number of participants, and hence, this only can be done if the set of participants is not too large.

Observe that, by ordering in some way the elements in $\mathcal{P}(Q)$, the rank function of a polymatroid $\mathcal{S} = (Q, f)$ can be seen as a vector $f = (f(A))_{A \subseteq Q} \in \mathbb{R}^k$, where $k = |\mathcal{P}(Q)| = 2^{n+1}$. The polymatroid axioms imply a number of linear constraints on this vector. If, in addition, we assume that $\mathcal{S}$ is a Γ-polymatroid for some access structure Γ on $P = Q - \{p_0\}$, other linear constraints appear. Since $\widetilde{\sigma}_{p_0}(\mathcal{S})$ is also a linear function on the vector f, one can determine $\widetilde{\kappa}(\Gamma)$ by solving the linear programming problem

$$\begin{array}{ll} \text{Minimize} & (1/n) \sum_{i \in P} f(\{i\}) \\ & \\ \text{subject to} & f \text{ is the rank function of a } \Gamma\text{-polymatroid.} \end{array}$$

Observe that $\sigma_{p_0}(\mathcal{S})$ is not linear. Because of that, we introduce a new variable v. Obviously, $\kappa(\Gamma)$ is the solution of the linear program

$$\begin{array}{ll} \text{Minimize} & v \\ & \\ \text{subject to} & f \text{ is the rank function of a } \Gamma\text{-polymatroid and} \\ & v \geq f(\{i\}) \text{ for every } i \in Q. \end{array}$$

The feasible region for the first linear programming problem is

$$\Omega = \Omega(\Gamma) = \{f \in \mathbb{R}^k : f \text{ is the rank function of a } \Gamma\text{-polymatroid}\}.$$

Since there exist Γ-polymatroids for every access structure, $\Omega \neq \emptyset$. For the other linear programming problem, the feasible region is

$$\Omega' = \{(f, v) \in \mathbb{R}^{k+1} : f \in \Omega \text{ and } v \geq f(\{i\}) \text{ for every } i \in Q\},$$

which is obviously nonempty as well. Therefore, both linear programs are feasible and bounded, and hence $\kappa(\Gamma) = \min\{\sigma_{p_0}(\mathcal{S}) : \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}$ and $\kappa(\Gamma)$ is a rational number. The same applies to $\widetilde{\kappa}(\Gamma)$.

The number of constraints to define these feasible regions can be reduced by using the following characterization of polymatroids given by Matúš [34]. Namely, $f : \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if

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

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

3. $f(A \cup \{i\}) + f(A \cup \{j\}) \geq f(A \cup \{i,j\}) + f(A)$ 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 $\mathcal{S} = (Q, f)$ is a Γ-polymatroid if and only if

4. $f(\{p_0\}) = 1$,
5. $f(A \cup \{p_0\}) = f(A)$ if $A \subseteq P$ is a minimal qualified subset of Γ, and
6. $f(B \cup \{p_0\}) = f(B) + 1$ if $B \subseteq P$ is a maximal unqualified subset of Γ.

For every $A \subseteq Q$, we consider the vector $\mathbf{e}_A \in \mathbb{R}^k$ with $\mathbf{e}_A(A) = 1$ and $\mathbf{e}_A(B) = 0$ for every $B \in \mathcal{P}(Q) - \{A\}$. At this point, we can present a set of linear constraints defining the feasible region Ω (vectors are considered as columns).

1. $\mathbf{e}_\emptyset^T f = 0$.
2. $(\mathbf{e}_{Q-\{i\}} - \mathbf{e}_Q)^T f \leq 0$ for every $i \in Q$.
3. $(\mathbf{e}_{A\cup\{i,j\}} + \mathbf{e}_A - \mathbf{e}_{A\cup\{i\}} - \mathbf{e}_{A\cup\{j\}})^T f \leq 0$ for every $i, j \in Q$ with $i \neq j$ and for every $A \subseteq Q - \{i,j\}$.
4. $\mathbf{e}_{\{p_0\}}^T f = 1$.
5. $(\mathbf{e}_{A\cup\{p_0\}} - \mathbf{e}_A)^T f = 0$ for every $A \in \min\Gamma$.
6. $(\mathbf{e}_{B\cup\{p_0\}} - \mathbf{e}_B)^T f = 1$ for every maximal unqualified subset B.

Both the number of variables and the number of constraints grow exponentially on the number n of participants. The number of variables is $k = 2^{n+1}$. If $m = |\min\Gamma|$ and m' is the number of maximal unqualified subsets, then the number N_c of constraints is $N_c = \binom{n+1}{2} \cdot 2^{n-1} + n + 2(m + m') + 5$. In addition, $m, m' \leq \binom{n}{\lfloor n/2 \rfloor}$ by Sperner's Theorem [1].

4 New Bounds

Jackson and Martin [29] determined the optimal (average) complexities of all access structures on five participants except a few ones, for which upper and lower bounds were given. Specifically, there are 180 non-isomorphic access structures with five participants, and they found the optimal complexities of 170 of them and the optimal average complexities of 165 of them. The techniques used in [29] provide lower bounds on $\kappa(\Gamma)$ and upper bounds on $\lambda(\Gamma)$. The value of $\sigma(\Gamma)$ is determined only if these bounds imply that $\kappa(\Gamma) = \lambda(\Gamma)$. The same applies to the corresponding parameters for the optimal average complexity. Because of that, the results that are obtained for an access structure apply as well to its dual. Taking this into account, the unsolved cases in [29] reduce to the 13 ones that are listed in Table 1, which involve access structures on $P = \{1,2,3,4,5\}$ described in the following and their duals. They are enumerated as in [29]. The lower bound on $\widetilde{\sigma}(\Gamma_{73})$ was improved by van Dijk [17]. From now on, we unburden the notation by writing the subsets of P in compact form, that is, 12 instead of $\{1,2\}$.

- $\min\Gamma_{73} = \{12, 13, 24, 35, 145\}$.
- $\min\Gamma_{80} = \{12, 13, 234, 235, 45\}$.
- $\min\Gamma_{82} = \{12, 13, 234, 235, 145, 245\}$.

- $\min \Gamma_{83} = \{12, 13, 234, 235, 145, 245, 345\}$.
- $\min \Gamma_{86} = \{12, 13, 234, 45\}$.
- $\min \Gamma_{88} = \{12, 13, 234, 145, 245\}$.
- $\min \Gamma_{89} = \{12, 13, 234, 145, 245, 345\}$.
- $\min \Gamma_{150} = \{123, 124, 134, 125, 235\}$.
- $\min \Gamma_{152} = \{123, 124, 134, 125, 345\}$.
- $\min \Gamma_{153} = \{123, 124, 134, 125, 2345\}$.

Table 1: Our results for access structures on five participants

Access structure	σ from [29]	$\widetilde{\sigma}$ from [29, 17]	κ with LP	$\widetilde{\kappa}$ with LP	Current $\widetilde{\sigma}$	Number of constraints
$\Gamma_{73} \cong \Gamma^*_{151}$	$[3/2, 5/3]$	$[3/2, 8/5]$	$3/2$	$3/2$	$[3/2, 8/5]$	272
$\Gamma_{80} \cong \Gamma^*_{18}$	$3/2$	$[6/5, 7/5]$		$13/10$	$[13/10, 7/5]$	274
$\Gamma_{82} \cong \Gamma^*_{107}$	$[3/2, 5/3]$	$[6/5, 7/5]$	$3/2$	$13/10$	$[13/10, 7/5]$	274
$\Gamma_{83} \cong \Gamma^*_{136}$	$3/2$	$[6/5, 7/5]$		$13/10$	$[13/10, 7/5]$	280
$\Gamma_{86} \cong \Gamma^*_{123}$	$3/2$	$[6/5, 7/5]$		$13/10$	$[13/10, 7/5]$	268
$\Gamma_{88} \cong \Gamma^*_{88}$	$3/2$	$[6/5, 7/5]$		$7/5$	$7/5$	270
$\Gamma_{89} \cong \Gamma^*_{113}$	$3/2$	$[6/5, 7/5]$		$13/10$	$[13/10, 7/5]$	274
$\Gamma_{150} \cong \Gamma^*_{40}$	$[3/2, 12/7]$	$7/5$	$3/2$		$7/5$	272
$\Gamma_{152} \cong \Gamma^*_{53}$	$[3/2, 5/3]$	$[7/5, 8/5]$	$3/2$	$3/2$	$[3/2, 8/5]$	272
$\Gamma_{153} \cong \Gamma^*_{30}$	$[3/2, 5/3]$	$7/5$	$3/2$		$7/5$	274

By using our linear programming approach, we are able to improve the results in [29] by determining the values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ for all those access structures. The obtained results are given in Table 1. The entries with an interval correspond to a lower and an upper bound. Observe that we improved some of the lower bounds on $\widetilde{\sigma}(\Gamma)$ but we could not improve the lower bounds on $\sigma(\Gamma)$ for any of these access structures. Nevertheless, the exact values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ have been determined. Therefore, we know now that no better lower bounds can be obtained by the combinatorial techniques used in [29]. That is, whether better constructions of secret sharing schemes are obtained for those structures, or better lower bounds have to be searched by considering information inequalities other than the basic Shannon inequalities, as discussed in Section 5. We also included in the table the number of constraints that define the feasible region.

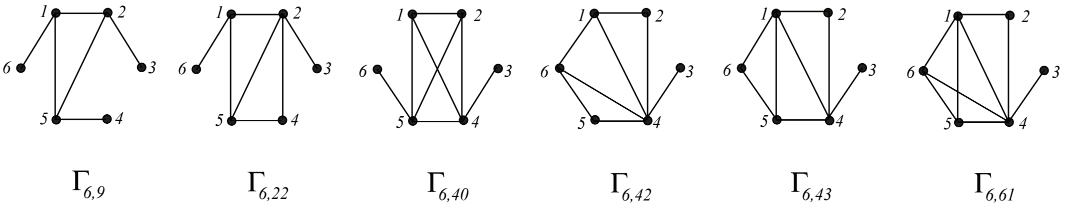

Figure 1: Graph access structures with six vertices.

The optimal complexities of 94 of the 112 non-isomorphic graph access structures on six participants were determined by van Dijk [16], while lower and upper bounds were given for the remaining ones. Some of these upper bounds were improved in [11, 19]. By using linear programming, we have computed the values of $\kappa(\Gamma)$ for the 18 unsolved cases from [16], which improve the lower bounds for six of them, namely the ones in Figure 1. The results are shown in Table 2. We notice that, by mistake, we did not include the results about $\Gamma_{6,22}$ in the previous version of this paper [38]. Except for $\Gamma_{6,61}$, these new lower bounds determine the values of $\sigma(\Gamma)$. After the publication of the previous version of this paper [38], Gharahi and Dehkordi [25] presented lower bounds on the optimal complexities of all access structures in Figure 1 except $\Gamma_{6,9}$. Their bounds coincide with the values of $\kappa(\Gamma)$ that are given in Table 2, but they are proved by using the same techniques as in [16]. Moreover, they present a decomposition construction of a linear secret sharing scheme for $\Gamma_{6,61}$ that makes it possible to determine the optimal complexity of this access structure.

Table 2: Our results for graph access structures on six vertices

Access structure	σ from [16]	σ from [11]	κ with LP	Current σ	Number of constraints
$\Gamma_{6,9}$	$[5/3, 2]$	$[5/3, 7/4]$	$7/4$	$7/4$	703
$\Gamma_{6,22}$	$[5/3, 9/5]$	$[5/3, 7/4]$	$7/4$	$7/4$	705
$\Gamma_{6,40}$	$[5/3, 9/5]$	$[5/3, 7/4]$	$7/4$	$7/4$	707
$\Gamma_{6,42}$	$[5/3, 7/4]$	no improvement	$7/4$	$7/4$	707
$\Gamma_{6,43}$	$[5/3, 7/4]$	no improvement	$7/4$	$7/4$	707
$\Gamma_{6,61}$	$[5/3, 2]$	$[5/3, 16/9]$	$7/4$	$7/4$ ([25])	707

5 Sharpening the Feasible Region

The lower bounds on the optimal (average) complexity given by $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ are not tight in general. This is due to the fact that the sets in (1), (2) and (3) are different.

This is due to the existence of the so-called *non-Shannon information inequalities*. The polymatroid axioms correspond to the basic *Shannon information inequalities* (namely, the mutual information is nonnegative). Zhang and Yeung [43] presented an information inequality that must be satisfied by the rank function of every poly-entropic polymatroid but is independent from the polymatroid axioms. Many other such non-Shannon information inequalities have been found since then [20, 22, 35]. Moreover, Zhang-Yeung inequality was used in [4] to present the first examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$. The bounds in [4] were improved in [36] by using the inequalities from [20]. In addition, there exist several *rank inequalities*, which are satisfied by the rank function of every poly-linear polymatroid. The first one was presented by Ingleton [26], and other such inequalities were given by Dougherty, Freiling and Zeger [21].

Beimel and Orlov [5] proved that all known non-Shannon information inequalities cannot improve our knowledge on the asymptotic behavior of the optimal (average) complexity. Nevertheless, since all these inequalities are linear, they can be added to the linear programs that are discussed in Section 3. In this way, better lower bounds on $\sigma(\Gamma)$, or on $\lambda(\Gamma)$ if rank inequalities are used, can be found for some access structures. Differently to the one in (3), the sets in (1) and (2) cannot be described by a finite number of linear inequalities [21, 35], and hence the values of $\sigma(\Gamma)$ and $\lambda(\Gamma)$ cannot be determined by linear programming.

In this section, we explain how to use the Ingleton inequality to obtain a linear program providing better lower bounds on $\lambda(\Gamma)$. For a polymatroid $\mathcal{S} = (Q, f)$ and $A, B, C, D \subseteq Q$, consider

$$\begin{aligned} I(f; A, B, C, D) &= f(A) + f(B) + f(C \cup D) + f(A \cup B \cup C) + f(A \cup B \cup D) \\ &\quad -f(A \cup B) - f(A \cup C) - f(A \cup D) - f(B \cup C) - f(B \cup D). \end{aligned}$$

Specifically, Ingleton inequality states that, if $\mathcal{S} = (Q, f)$ is a poly-linear polymatroid, then

$$I(f; A, B, C, D) \leq 0 \text{ for every } A, B, C, D \subseteq Q. \tag{4}$$

Moreover, according to the main result of [10], a polymatroid $\mathcal{S} = (Q, f)$ satisfies (4) if and only if

$$I(f; A \cup X, B \cup X, C \cup X, D \cup X) \leq 0$$

for all disjoint sets $A, B, C, D, X \subseteq Q$ with A, B, C, D nonempty. For an access structure Γ, consider the linear program

Minimize v

subject to f is the rank function of a Γ-polymatroid,
$I(f; A \cup X, B \cup X, C \cup X, D \cup X) \leq 0$
for all disjoint sets $A, B, C, D, X \subseteq Q$ with A, B, C, D nonempty, and
$v \geq f(\{i\})$ for every $i \in Q$.

Since there exists a linear secret sharing scheme for Γ, this linear program is feasible and bounded. The solution $\lambda_{IN}(\Gamma)$ is a lower bound on $\lambda(\Gamma)$. Moreover, it is the best lower bound on $\lambda(\Gamma)$ that can be obtained by adding only the Ingleton inequality to the Shannon information inequalities.

By solving this linear program, we obtained that $\lambda_{IN}(\Gamma) = \kappa(\Gamma)$ for the 5 access structures on five participants and the 12 graph access structures on six participants whose optimal complexities are still undetermined. Therefore, the Ingleton inequality does not improve the lower bounds on $\lambda(\Gamma)$ for these access structures. Nevertheless, we explored graph access structures on more than 6 participants and we found three examples, the graphs in Figure 2, with $\lambda_{IN}(\Gamma) > \kappa(\Gamma)$, and hence they are new examples of access structures with $\kappa(\Gamma) < \lambda(\Gamma)$. Specifically, $\lambda_{IN}(\Gamma_1) = 19/10$ and $\lambda_{IN}(\Gamma_2) = \lambda_{IN}(\Gamma_3) = 13/7$, while $\kappa(\Gamma_1) = 11/6$ and $\kappa(\Gamma_2) = \kappa(\Gamma_3) = 9/5$.

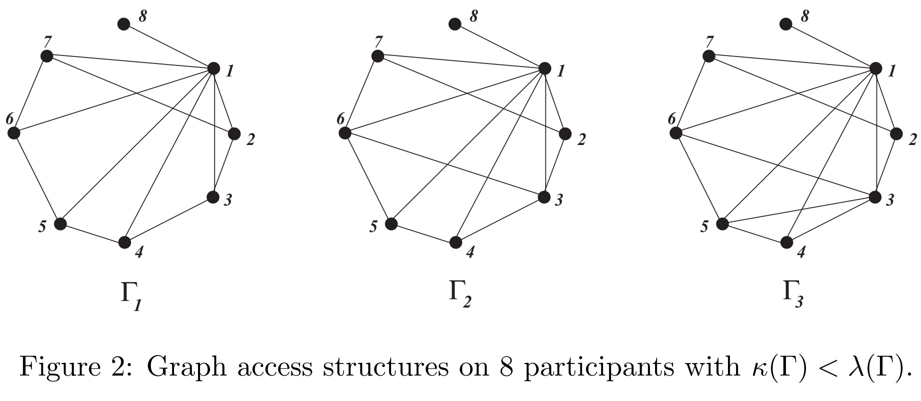

Figure 2: Graph access structures on 8 participants with $\kappa(\Gamma) < \lambda(\Gamma)$.

6 Ports of Non-representable Matroids

In this section, we use linear programming to extend the results in [4, 36, 39] about the ports of the Vámos matroid to the ports of other non-linear matroids. Seymour [39] proved that the Vámos matroid is not poly-entropic, and hence the two non-isomorphic ports $\mathcal{V}_1$ and $\mathcal{V}_6$ of the Vámos matroid do not admit any ideal secret sharing scheme. By using the non-Shannon information inequality by Zhang and Yeung [43], lower bounds on the optimal complexities of those access structures proving that $\sigma(\mathcal{V}_i) > \kappa(\mathcal{V}_i) = 1$ where presented in [4]. This bounds were improved in [36] by using some of the non-Shannon information inequalities given by Dougherty, Freiling and Zeger [20] (DFZ inequalities from now on). In addition, a lower bound on $\lambda(\mathcal{V}_i)$ (the same for both structures, because they are dual of each other) are obtained in [4] from the Ingleton inequality. A construction given in [31] provides an upper bound on $\lambda(\mathcal{V}_i)$. Specifically, the results in [4, 31, 36] are summarized as follows.

- $\kappa(\mathcal{V}_1) = 1 < 19/17 \leq \sigma(\mathcal{V}_1) \leq \lambda(\mathcal{V}_1) \leq 4/3$.
- $\kappa(\mathcal{V}_6) = 1 < 21/19 \leq \sigma(\mathcal{V}_6) \leq \lambda(\mathcal{V}_6) \leq 4/3$.
- $5/4 \leq \lambda(\mathcal{V}_1) = \lambda(\mathcal{V}_6) \leq 4/3$.

These results were obtained without using linear programming. Nevertheless, linear programming was used in [36] to prove that no better lower bounds on $\sigma(\mathcal{V}_i)$ can be obtained by using only the Zhang-Yeung and DFZ inequalities. In the Appendix of [37], we find two matroids, $AG(3,2)'$ and Q_8, that, similarly to the Vámos matroid, are among the smallest non-linear matroids. By using linear programming, we prove similar results for the ports of these matroids.

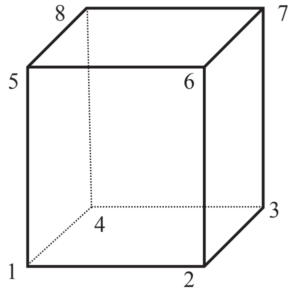

Figure 3: $AG(3,2)'$ and Q_8

Definition 6.1. The matroid $AG(3,2)'$ is defined on the set $V = \{1,\ldots,8\}$. Its independent sets are all the sets with at most 4 elements except the six faces, the six diagonal planes and the twisted plane $\{1,3,6,8\}$ of the cube in Figure 3.

Definition 6.2. The matroid Q_8 is defined on the set $V = \{1,\ldots,8\}$. Its independent sets are all the sets of cardinality at most 4 except the six faces and exactly five of the six diagonal planes of the cube in Figure 3. Assume that the diagonal plane $\{1,3,5,7\}$ is the independent one.

It is not difficult to check that there are only two non-isomorphic ports of the matroid $AG(3,2)'$, namely $\mathcal{AG}_1 = \Gamma_1(AG(3,2)')$ and $\mathcal{AG}_2 = \Gamma_2(AG(3,2)')$. Moreover, $\mathcal{AG}_1^* = \mathcal{AG}_2$. Similarly, the two non-isomorphic ports of the matroid Q_8 are $\mathcal{Q}_1 = \Gamma_1(Q_8)$ and $\mathcal{Q}_2 = \Gamma_2(Q_8)$. As before, $\mathcal{Q}_1^* = \mathcal{Q}_2$. The minimal qualified sets of these access structures are listed in the following.

- $\min \mathcal{AG}_1 = \{234, 256, 458, 357, 278, 467, 368, 2457\}$.
- $\min \mathcal{AG}_2 = \{134, 367, 156, 178, 358, 468, 4578, 4567, 3457, 1457\}$.
- $\min \mathcal{Q}_1 = \{234, 256, 458, 278, 467, 2368, 2457, 3468, 3568, 3678, 2357, 3457, 3567, 3578\}$.
- $\min \mathcal{Q}_2 = \{156, 367, 134, 468, 178, 358, 1357, 4567, 1457, 3567, 1567, 1368\}$.

Zhang-Yeung inequality [43] implies that, for every poly-entropic polymatroid (Q, f) and for every $A, B, C, D \subseteq Q$,

$$\begin{aligned} ZY(f; A, B, C, D) &= f(A) + 2f(B) + 2f(C) + f(A \cup D) + 4f(A \cup B \cup C) + 4f(B \cup C \cup D) \\ &\quad -3f(A \cup B) - 3f(A \cup C) - 3f(B \cup C) - f(B \cup D) - f(C \cup D) \leq 0 \end{aligned}$$

If we set $\{A, B, C, D\} = \{18, 36, 27, 45\}$ for $AG(3, 2)'$ and $\{A, B, C, D\} = \{15, 26, 37, 48\}$ for Q_8, then $ZY(f; A, B, C, D) > 0$. Therefore, the matroids $AG(3, 2)'$ and Q_8 are not poly-entropic, and hence their ports do not admit any ideal secret sharing scheme. By adding to the corresponding linear program the Zhang-Yeung inequality, or the DFZ inequalities, or the Ingleton inequality, with the previous choices of the sets A, B, C, D, we obtain the lower bounds in Table 3. In particular, these are new examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$.

Table 3: Result for $AG(3, 2)'$ and Q_8

Access structure	Lower bound of σ by ZY	Lower bound of σ by DFZ	Lower bound of λ by Ingleton
$\mathcal{AG}_1$	10/9	19/17	5/4
$\mathcal{AG}_2$	9/8	9/8	5/4
$\mathcal{Q}_1$	9/8	9/8	5/4
$\mathcal{Q}_2$	10/9	19/17	5/4

7 An Impossibility Result

Since no better bounds on $\lambda(\Gamma)$ can be obtained for the access structures in Tables 1 and 2 by using Ingleton inequality, one could expect that there exist for those access structures linear secret sharing schemes with complexity equal to the lower bound $\kappa(\Gamma)$. We prove in this section that, at least for two of those access structures, this is not the case.

If Γ is an access structure with $\kappa(\Gamma) = \widetilde{\kappa}(\Gamma)$ and $\mathcal{S} = (Q, f)$ is a Γ-polymatroid with $\sigma_{p_0}(\mathcal{S}) = \kappa(\Gamma)$, then $h(\{i\}) = \kappa(\Gamma)$ for every $i \in P$. This simplifies the search for linear schemes with complexity equal to $\kappa(\Gamma)$. We find in Table 1 two access structures with that property. Namely $\kappa(\Gamma) = \widetilde{\kappa}(\Gamma) = 3/2$ if $\Gamma = \Gamma_{73}$ or $\Gamma = \Gamma_{152}$. We prove in the following that the complexity of every linear secret sharing scheme for one of these structures is larger than $3/2$. Moreover, for Γ_{73}, the same applies to the average complexity. Here we consider $\Gamma_{53} = \Gamma_{152}^*$ instead of Γ_{152}. The minimal qualified sets of Γ_{73} and Γ_{53}, which are represented in Figure 4, are

- $\min \Gamma_{73} = \{12, 13, 24, 35, 145\}$, and
- $\min \Gamma_{53} = \{12, 13, 24, 34, 35, 145\} = \min \Gamma_{73} \cup \{34\}$.

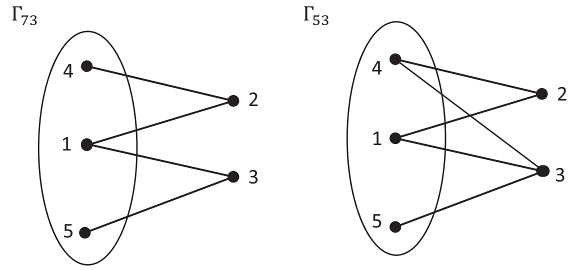

Figure 4: Access Structures Γ_{73} and Γ_{53}

The remaining of this section is devoted to prove the following impossibility result. The proof is quite long and it is divided into several partial results.

Proposition 7.1. *There does not exist any linear secret sharing scheme Σ with access structure Γ_{53} or Γ_{73} with complexity $\sigma(\Sigma) = 3/2$. There does not exist any linear secret sharing scheme Σ with access structure Γ_{73} with average complexity $\widetilde{\sigma}(\Sigma) = 3/2$.*

When using linear programming to compute the value of $\kappa(\Gamma)$ for $\Gamma = \Gamma_{53}$ or $\Gamma = \Gamma_{73}$, we always obtain as an optimal solution the polymatroid $\mathcal{S}_1$ and, respectively, $\mathcal{S}_2$ that are described in Definition 7.2. We prove in Lemma 7.4 that these polymatroids are not poly-linear.

Definition 7.2. The polymatroids $\mathcal{S}_1$ and $\mathcal{S}_2$ are defined as the only Γ_{53}-polymatroid and, respectively, the only Γ_{73}-polymatroid satisfying the following properties.

1. $f(i) = 3/2$ for every $i \in P$.
2. $f(A) = 5/2$ for every unqualified set $A \subseteq P$ with $|A| = 2$.
3. $f(A) = 3$ for every qualified set $A \subseteq P$ with $|A| = 2$.
4. $f(A) = 7/2$ for every $A \subseteq P$ with $|A| \geq 3$.

Lemma 7.3. *Let V_1, V_2, V_3 be subspaces of a vector space E. Then,*

$$\max\left\{0, s - \sum s_i + \sum r_i\right\} \leq \dim(V_1 \cap V_2 \cap V_3) \leq \min\{t_1, t_2, t_3\},$$

where $s = \dim(V_1 + V_2 + V_3)$, $s_i = \dim(V_j + V_k)$, $r_i = \dim V_i$, and $t_i = \dim(V_j \cap V_k)$ for every $\{i, j, k\} = \{1, 2, 3\}$.

Proof. Put $t = \dim(V_1 \cap V_2 \cap V_3)$. Since $(V_1 \cap V_3) + (V_2 \cap V_3) \subseteq (V_1 + V_2) \cap V_3$, we have that

$$\dim((V_1 + V_2) \cap V_3) - \dim((V_1 \cap V_3) + (V_2 \cap V_3)) = \sum s_i - \sum r_i - s + t \geq 0.$$

Obviously, $t \leq t_i$. □

Lemma 7.4. *The polymatroids $\mathcal{S}_1$ and $\mathcal{S}_2$ are not poly-linear.*

Proof. Take $Q = \{0, 1, 2, 3, 4, 5\}$ with $p_0 = 0$. Let $\mathcal{S} = (Q, f)$ be one of these polymatroids and suppose that it is poly-linear. Then there must exist a positive integer c and subspaces $(V_i)_{i \in Q}$ of a vector space E such that $\dim \sum_{i \in A} V_i = 2c\, f(A)$ for every $A \subseteq Q$.

Clearly, $\dim(V_1 \cap V_4) = \dim(V_1 \cap V_5) = \dim(V_4 \cap V_5) = c$, and hence $\dim(V_1 \cap V_4 \cap V_5) = c$ by Lemma 7.3. Therefore $V_1 \cap V_4 = V_1 \cap V_5 = V_4 \cap V_5 = U_0$.

Since $\dim[(V_2+V_3)\cap V_5] = \dim(V_2+V_3)+\dim V_5 - \dim(V_2+V_3+V_5) = 5c+3c-7c = c$ and $\dim(V_2\cap V_5) = c$, we have that $U_0\cap(V_2+V_3)\subseteq V_5\cap(V_2+V_3) = V_5\cap V_2$. Therefore, $U_0\cap(V_2+V_3)=\{0\}$ because $V_1\cap V_2=\{0\}$.

The subspace V_0 corresponding to the dealer is contained in V_A for every $A\in\Gamma$. Therefore,

$$V_0\subseteq(V_1+V_2)\cap(V_1+V_3)\cap(V_2+V_4)\cap(V_3+V_5)=W$$

We prove in the following that $3c\le\dim W\le 4c$. Indeed, on one hand,

$$\begin{aligned}
\dim W &= \dim\{[(V_1+V_2)\cap(V_2+V_4)]\cap[(V_1+V_3)\cap(V_3+V_5)]\}\\
&= \dim[(V_1+V_2)\cap(V_2+V_4)]+\dim[(V_1+V_3)\cap(V_3+V_5)]\\
&\quad -\dim\{[(V_1+V_2)\cap(V_2+V_4)]+[(V_1+V_3)\cap(V_3+V_5)]\}\\
&\le 5c+5c-\dim[V_2+(V_1\cap V_4)]+[V_3+(V_1\cap V_5)]\\
&= 5c+5c-\dim(V_2+V_3+U_0)\\
&= 5c+5c-6c\\
&= 4c. \qquad (5)
\end{aligned}$$

On the other hand, $\dim\{[(V_1+V_2)\cap(V_2+V_4)]+[(V_1+V_3)\cap(V_3+V_5)]\}\le 7c$, and hence $\dim W\ge 5c+5c-7c=3c$.

The next step is to prove that $\dim[W\cap(V_2+V_5)]=2c$.

$$\begin{aligned}
\dim[W\cap(V_2+V_5)] &= \dim W+\dim(V_2+V_5)-\dim(W+V_2+V_5)\\
&\le \dim W+\dim(V_2+V_5)-\dim(V_0+V_2+V_5)\\
&\le 4c+5c-7c\\
&= 2c. \qquad (6)
\end{aligned}$$

The other inequality is obtained by

$$\begin{aligned}
\dim[W\cap(V_2+V_5)] &= \dim\{(V_1+V_2)\cap(V_1+V_3)\cap(V_2+V_4)\cap(V_3+V_5)\cap(V_2+V_5)\}\\
&= \dim\{[(V_1+V_2)\cap(V_2+V_5)\cap(V_2+V_4)]\cap[(V_1+V_3)\cap(V_3+V_5)]\}\\
&\ge \dim[(V_2+U_0)\cap(V_3+U_0)]\\
&= \dim(V_2+U_0)+\dim(V_3+U_0)-\dim(V_2+V_3+U_0)\\
&= 4c+4c-6c\\
&= 2c \qquad (7)
\end{aligned}$$

In particular, all inequalities in (6) must be equalities, which implies that $\dim W=4c$. Moreover, the inequality in (5) must be also an equality, and hence

$$\begin{aligned}
[(V_1+V_2)\cap(V_2+V_4)]+[(V_1+V_3)\cap(V_3+V_5)] &= [V_2+(V_1\cap V_4)]+[V_3+(V_1\cap V_5)]\\
&= V_2+V_3+U_0.
\end{aligned}$$

Therefore, $(V_1+V_3)\cap(V_3+V_5)\subseteq V_2+V_3+U_0$ and $(V_1+V_3)\cap(V_3+V_5)\subseteq V_2+V_3+U_0$.

$$\begin{aligned}
\dim(W\cap V_2) &= \dim[(V_1+V_3)\cap(V_3+V_5)\cap V_2]\\
&= \dim[(V_1+V_3)\cap(V_3+V_5)]+\dim V_2\\
&\quad -\dim\{[(V_1+V_3)\cap(V_3+V_5)]+V_2\}\\
&\ge \dim[(V_1+V_3)\cap(V_3+V_5)]+\dim V_2-\dim(V_2+V_3+U_0)\\
&= 5c+3c-6c\\
&= 2c
\end{aligned}$$

Analogously, $\dim(W \cap V_3) \geq 2c$. Therefore,

$$\begin{aligned}
\dim[W \cap (V_2 + V_3)] &\geq \dim[(W \cap V_2) + (W \cap V_3)] \\
&= \dim(W \cap V_2) + \dim(W \cap V_3) - \dim(W \cap V_2 \cap V_3) \\
&\geq 2c + 2c - c \\
&= 3c \qquad (8)
\end{aligned}$$

Finally, since $V_0 \subseteq W$,

$$\begin{aligned}
\dim[V_0 \cap (V_2 + V_3)] &= \dim[V_0 \cap W \cap (V_2 + V_3)] \\
&\geq \dim(V_0) + \dim[W \cap (V_2 + V_3)] - \dim(W) \\
&\geq 2c + 3c - 4c \\
&= c,
\end{aligned}$$

a contradiction with the fact that $\{2, 3\}$ is not qualified. □

We prove in Lemma 7.7 that the polymatroids $\mathcal{S}_1$ and $\mathcal{S}_2$ are the only optimal solutions of the linear programs computing $\kappa(\Gamma_{53})$ and $\kappa(\Gamma_{73})$, respectively. We need two technical results. The first one is due to Csirmaz [12], while the second one is proved by using the independent sequence technique [8].

Lemma 7.5. *Let Γ be an access structure. The following properties are satisfied by every Γ-polymatroid $\mathcal{S} = (Q, f)$.*

1. *If $B \in \Gamma$, and $A \subseteq B$ and $A \notin \Gamma$, then $f(A) \leq f(B) - 1$.*
2. *If $A, B \in \Gamma$ but $A \cap B \notin \Gamma$, then $f(A \cup B) + f(A \cap B) \leq f(A) + f(B) - 1$.*

Lemma 7.6. *Let Γ be an access structure and $\mathcal{S} = (Q, f)$ a Γ-polymatroid. If $a, b, c, d \in P$ are such that $ab, bc, acd \in \Gamma$ and $b, ac, ad \notin \Gamma$, then $f(bc) \geq 3$.*

Lemma 7.7. *If $\Gamma = \Gamma_{53}$ or $\Gamma = \Gamma_{73}$, there exists a unique Γ-polymatroid $\mathcal{S}$ with $\sigma_{p_0}(\mathcal{S}) = 3/2$.*

Proof. Let $\mathcal{S} = (Q, f)$ be such a polymatroid. Obviously, $f(i) = 3/2$ for every $i \in P$ since $\kappa(\Gamma) = \widetilde{\kappa}(\Gamma) = 3/2$. If $ij \in \Gamma$, then $f(ij) = 3$ by Lemma 7.6 and $f(ij) \leq f(i) + f(j)$. Clearly, every 3-subset of P is qualified. Take three different participants $i, j, k \in P$ such that $ij, jk \notin \Gamma$. By Lemma 7.5,

$$f(ij) + 1 \leq f(ijk) \leq f(ij) + f(jk) - f(j),$$

which implies that $f(ij) \geq 5/2$. Symmetrically, $f(jk) \geq 5/2$, and hence $f(ijk) \geq 7/2$. Obviously, this implies that $f(ij) \geq 5/2$ for every pair $ij \notin \Gamma$. In addition, since every 3-subset contains at least one unqualified 2-subset, $f(A) \geq 7/2$ for every $A \subseteq P$ with $|A| = 3$. Consider now three different participants $i, j, k \in P$ such that $ij, jk \in \Gamma$. Applying Lemma 7.5 again,

$$f(ijk) \leq f(ij) + f(jk) - f(j) - 1 = 7/2,$$

and hence $f(ik) = 5/2$. This implies that $f(ij) = 5/2$ for every pair $ij \notin \Gamma$ except for 45 for Γ_{73}. Therefore,

$$f(145) \leq f(14) + f(15) - f(1) = 7/2,$$

and hence $f(45) \leq f(145) - 1 = 5/2$. Analogously, $f(A) = 7/2$ for every $A \subseteq P$ with $|A| = 3$, and $f(A) = 5/2$ for every $A \subseteq P$ with $|A| = 2$ and $A \notin \Gamma$. Let A be a 4-subset of P, and let $B \subseteq A$ be an unqualified 2-subset. Then $A = B \cup ij$ and

$$f(A) \leq f(B \cup i) + f(B \cup j) - f(B) - 1 = 7/2,$$

and hence $f(A) = 7/2$. One can prove in the same way that $f(P) = 7/2$. All these facts determine a unique Γ-polymatroid $\mathcal{S}$. □

Lemmas 7.4 and 7.7 suffice to prove the first statement in Proposition 7.1. In order to prove the impossibility result about the average complexity, we need to analyze in more detail the properties of the Γ_{73}-polymatroids that are optimal solutions for the linear program determining $\widetilde{\kappa}(\Gamma_{73})$.

Let τ be the permutation on Q that interchanges 2 with 3 and 4 with 5 and leaves 1 and p_0 fixed. Clearly, τ induces an automorphism of the access structure Γ_{73}. Therefore, if $\mathcal{S} = (Q, f)$ is a Γ_{73}-polymatroid, then $\tau\mathcal{S} = (Q, f\tau)$ is also a Γ_{73}-polymatroid. Moreover, if $\mathcal{S}$ is poly-linear over some finite field $\mathbb{K}$, the same applies to $\tau\mathcal{S}$. Consider the polymatroid $\mathcal{S}' = (Q, f')$ with $f' = (f + f\tau)/2$. Clearly, $\mathcal{S}'$ is a Γ_{73}-polymatroid. Moreover, $\tau\mathcal{S}' = \mathcal{S}'$ because τ^2 is the identity map. Finally, if there exists a linear secret sharing scheme Σ for Γ_{73} that is associated to the polymatroid $\mathcal{S}$, then there exists a linear secret sharing scheme Σ' for Γ_{73} that is associated to the polymatroid $\mathcal{S}'$, and both schemes have the same average complexity. By taking this into account, Lemma 7.8 concludes the proof of Proposition 7.1.

Lemma 7.8. *There exists a unique* Γ_{73}*-polymatroid* $\mathcal{S} = (Q, f)$ *such that* $\tau\mathcal{S} = \mathcal{S}$ *and* $\widetilde{\sigma}_{p_0}(\mathcal{S}) = 3/2$*.*

Proof. By Lemma 7.6, $f(ij) \geq 3$ if $ij \in \Gamma$. Then,

- $f(1) + f(3) = f(1) + f(2) \geq 3$, and
- $f(2) + f(4) = f(3) + f(5) \geq 3$.

We have used here that $\tau\mathcal{S} = \mathcal{S}$. Combining these inequalities with $\sum_{i=1}^{5} f(i) = 15/2$, we obtain $f(4) = f(5) \leq 3/2$, and $f(2) = f(3) \geq 3/2$, and $f(1) \leq 3/2$.

By Lemma 7.5,

$$f(23) + 1 \leq f(234) \leq f(23) + f(34) - f(3), \tag{9}$$

and hence $f(34) \geq 5/2$. Similarly, $f(23) \geq 5/2$ and $f(234) \geq 7/2$. In addition, by using again that τ is an automorphism of the polymatroid, $f(235) = f(234) \geq 7/2$ and $f(25) = f(34) \geq 5/2$. Moreover, $f(345) = f(245) \geq f(25) + 1 \geq 7/2$, and similarly $f(134) = f(125) \geq 7/2$ and $f(123) \geq 7/2$.

We claim $f(124) = f(135) \leq 7/2$ and $f(145) \leq 7/2$. Indeed,

$$\begin{aligned} f(124) &\leq f(12) + f(24) - f(2) - 1 \\ &\leq f(1) + f(2) + f(4) - 1 \\ &= 1/2 \times 15/2 + f(1)/2 - 1 \\ &\leq 7/2. \end{aligned} \tag{10}$$

And

$$\begin{aligned} f(145) &\leq f(14) + f(15) - f(1) \\ &= 2f(14) - f(1) \\ &\leq 2[f(124) - 1] - f(1) \\ &\leq 2[f(12) + f(24) - f(2) - 2] - f(1) \\ &= 2[f(12) - f(2) - f(1)] + 2f(24) + f(1) - 4 \\ &\leq 2f(24) + f(1) - 4 \\ &\leq 2f(2) + 2f(4) + f(1) - 4 \\ &= 15/2 - 4 = 7/2. \end{aligned}$$

The next step is to prove that $f(124) - f(14) = f(135) - f(15) = 1$. Observe that $f(124) - f(14) = 1 + \epsilon$ for some $\epsilon \geq 0$, and hence $f(14) = f(15) \leq 5/2 - \epsilon$. Since $1 + f(14) + f(1245) \leq f(124) + f(145)$, we have that

$$7/2 \leq f(1245) \leq \epsilon + f(145) \leq f(14) + f(15) - f(1) \leq 5 - \epsilon - f(1), \tag{11}$$

and hence $f(1) \leq 3/2 - \epsilon$. Now, inequality (10) implies that $f(124) \leq 7/2 - 1/2\epsilon$, and hence $f(15) = f(14) \leq 5/2 - 3/2\epsilon$. By using this last inequality in (11), we have that $f(1) \leq 3/2 - 2\epsilon$. By repeating this argument, $f(1) \leq 3/2 - n\epsilon$ for every positive integer n, which implies that $\epsilon = 0$.

Therefore, $f(145) \geq f(1245)$ by (11), and hence $f(145) = f(1245) = f(1345) = 7/2$. Moreover, $f(245) = f(345) = 7/2$ and $f(134) = f(125) = 7/2$, which implies that $f(25) = f(34) = 5/2$. We can now use (9) to obtain $f(2) = f(3) = 3/2$, and hence $f(i) = 3/2$ for all $i \in P$. By far, we conclude the proof of Proposition 7.1. □

8 Conclusion and Open Problems

In this paper, we present several results on the optimization of the (average) complexity of secret sharing schemes that have been obtained by using linear programming. Other results by using the same technique have been given in [23, 32]. Differently to these other works, some of our results are obtained by using non-Shannon information inequalites (as the one by Zhang and Yeung [43]) and the Ingleton inequalities. Nevertheless, since the number of variables and constraints in the involved linear programs is exponential in the number of participants, the power of the techniques applied in this paper seems to be rather limited.

The most obvious open problem that can be posed here is to finish the projects initiated by Jackson and Martin [29] and by van Dijk [16] for access structures on five participants and graph access structures on six participants, respectively. As we saw in Section 5, the Ingleton inequality does not provide any improvement on the bounds. In addition, the impossibility result in Section 7 indicates that this is not an easy task.

In regard to that impossibility result, we notice that it does not imply that $\kappa(\Gamma) < \lambda(\Gamma)$ for the involved access structures. Indeed, there could exist infinite linear secret sharing schemes whose complexities are arbitrarily close to 3/2. Maybe other rank inequalities different from the Ingleton one can prove that stronger separation result.

Another interesting line of future work is to apply the techniques in Section 6 to other matroids that are not poly-entropic, as the non-Desargues matroids and other examples presented in [33].

References

[1] I. Anderson, Combinatorics of Finite Sets, Oxford University Press, 1987.

[2] A. Beimel, Secret-Sharing Schemes: A Survey, IWCC'2011. Lect. Notes Comput. Sc. 6639 (2011) 11–46.

[3] A. Beimel, Y. Ishai, On the power of nonlinear secret sharing schemes, SIAM J. Discrete Math. 19 (2005) 258–280.

[4] A. Beimel, N. Livne, C. Padró, Matroids can be far from ideal secret sharing, Proc. of TCC'2008, Lect. Notes Comput. Sc. 4948 (2008) 194–212.

[5] A. Beimel, I. Orlov, Secret Sharing and Non-Shannon Information Inequalities, Proc. of TCC'2009, Lect. Notes Comput. Sc. 5444 (2009) 539–557.

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

[7] G.R. Blakley, Safeguarding cryptographic keys, AFIPS Conf. P. 48 (1979) 313–317.

[8] 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.

[9] E.F. Brickell, D.M. Davenport, On the Classification of Ideal Secret Sharing Schemes, J. Cryptology, (1991) 123–134.

[10] T.H. Chan, L. Guillé, A. Grant, The minimal set of Ingleton inequalities, IEEE Trans. Inform. Theory Vol. 57 Iss. 4 (2011) 1849–1864.

[11] B.L. Chen, H.M. Sun, Weighted Decomposition Construction for Perfect Secret Sharing Schemes, Comput. Math. Appl. Vol. 43 Iss. 6–7 (2002) 877–887.

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

[13] L. Csirmaz, Secret sharing on the d-dimensional cube, Cryptology ePrint Archive, Report 2005/177 (2005) `http://eprint.iacr.org`.

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

[15] L. Csirmaz, G. Tardos, Secret sharing on trees: problem solved, Preprint (2009), Available at `http://eprint.iacr.org/2009/071`.

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

[17] M. van Dijk, More information theoretical inequalities to be used in secret sharing? Inform. Process. Lett. 63 (1997) 41–44.

[18] M. van Dijk, W.A. Jackson, K.M. Martin, A note on duality in linear secret sharing schemes, Bull. Inst. Combin. Appl. 19 (1997) 93–101.

[19] M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls, Improved constructions of secret sharing schemes by applying-(λ, ω)-decompositions, Inform. Process. Lett. Vol. 99 Iss. 4 (2006) 154–157.

[20] R. Dougherty, C. Freiling, K. Zeger, Six new non-Shannon information in-equalities, ISIT'2006, (2006) 233-236.

[21] R. Dougherty, C. Freiling, K. Zeger, Linear rank inequalities on five or more variables, Available at `arXiv.org`, arXiv:0910.0284v3 (2009).

[22] R. Dougherty, C. Freiling, K. Zeger, Non-Shannon Information Inequalities in Four Random Variables, Available at `arXiv.org`, arXiv:1104.3602v1 (2011).

[23] O. Farràs, J.R. Metcalf-Burton, C. Padró, L. Vázquez, On the optimization of bipartite secret sharing schemes, Des. Codes Cryptogr. 63 (2012) 255–271.

[24] S. Fujishige, Polymatroidal Dependence Structure of a Set of Random Variables, Inform. and Control. 39 (1978) 55–72.

[25] M. Gharahi, M.H. Dehkordi, The complexity of the graph access structures on six participants, Des. Codes Cryptogr, Online First (2011).

[26] A.W. Ingleton, Representation of matroids, in: D.J.A Welsh (Ed.), Combinatorial Mathematics and its Applications, Academic Press, London, 1971, pp. 149–167.

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

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

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

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

[31] J. Martí-Farré, C. Padró, On Secret Sharing Schemes, Matroids and Polymatroids, J. Math. Cryptol. 4 (2010) 95–120.

[32] J. Martí-Farré, C. Padró, L. Vázquez, Optimal Complexity of Secret Sharing Schemes with Four Minimal Qualified Subsets, Des. Codes Cryptogr. 61 (2011) 167–186.

[33] F. Matúš, Matroid representations by partitions, Discrete Math. 203 (1999) 169–194.

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

[35] F. Matúš, Infinitely many information inequalities, IEEE International Symposium on Information Theory (2007) 41–44.

[36] J.R. Metcalf-Burton, Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid, Discrete Math. vol. 311, Iss. 8-9 (2011) 651C662.

[37] J.G. Oxley, Matroid Theory, Second ed., Oxford University Press, New York, 2011.

[38] C. Padró, L. Vázquez, Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming, LATIN 2010: Theoretical Informatics. Lecture Notes in Comput. Sci. 6034 (2010) 344-355.

[39] P.D. Seymour, On secret-sharing matroids, J. Combin. Theory Ser. B, 56 (1992) 69–73.

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

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

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

[43] Z. Zhang, R.W. Yeung, On characterization of entropy function via information inequalities, IEEE Trans. Inform. Theory 44 (1998) 1440–1452.