BACHELOR'S THESIS

Degree in Mathematics

Title: Secret Sharing Schemes: Optimizing the Information Ratio

Author: Félix Hernández Ansuátegui

Advisor: Carles Padró

Department: Applied Mathematics

Academic year: 2016-2017

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Secret Sharing Schemes: Optimizing the information ratio

Felix Hernandez Ansuategui,
Mathematics Student in Facultat de Matemàtiques i Estadística

June 24, 2017

Abstract

Several authors in the scope of Secret Sharing have tried to obtain and improve bounds for both the information ratio and average information ratio of access structures. Following that topic, this work deals with the optimization of these two parameters when considering secret sharing schemes for access structures on 5 and 6 participants. First, access structures with 5 participants will be considered, and then it will follow a study on the ones on 6 participants that are based on graphs. The main goal of the paper is to check existing lower bounds (and improve some of them) by using linear programs with the sage solver. The technique used is based on the combinatorial method presented by Crismaz [11], which has been used as well in other articles in order to find better bounds for these parameters. Shannon information inequalities have been used to translate the polymatroid axioms into linear constraints that were included in the programs in order to find the desired bounds. Some upper bounds have been found for these parameters as well, using a decomposition method that was presented previously by Stinson [33].

Contents

Chapter 1

Introduction

Secret Sharing refers to methods used to distribute a secret value among a group of participants. It is one of the widely studied topics in cryptography nowadays. It is a fundamental tool for some of the latest and more complex applications of cryptography. For example, it can be applied when using distributed signatures. A *signature* is a hash value (value computed mathematically from plain text that has always the same length) calculated from a message that is encrypted with a secret key S. Asymmetric cryptography, a set of techniques in cryptography that are based on the existence of two different keys, is used when encrypting S. The two keys are the private key (one or few holders) and the public key (distributed among several users). If one message (or hash value, when signing a message) is encrypted with the private key it has to be decrypted with the public one, and vice versa. So when one talks about distributed signatures, the objective is that several co-certifiers sign a message without imposing any signing order over them. The signers can share the secret key as a secret value and then secret sharing can be adopted. The signers will not know the key separately, but if they join together the share of each of them, they will be able to retrieve the key and encrypt the message as it was needed. This is only one example, but there are a lot more useful applications of secret sharing nowadays: Byzantine agreement [1], threshold cryptography[3], access control [4], attribute-based encryption [5]...

Its main application, however, is the so-called *Secure Multi-party Computation* [6, 7] which has been the big motivation for the development and study of secret sharing. Nowadays, it is regular for individuals and companies to encounter situations in which private data is a very valuable resource. So, imagine one needs to do some computation with this valuable data but does not trust everyone involved in the operation. In a secure multi-party computation, secret sharing can be used in order to protect everyone's data: each party can spread the data in different fragments so that all together they hold full information, yet no individual party has all the information. A very interesting fact that makes this problem even more important is that there are many situations in which a large amount of added value can be obtained when combining confidential information from several sources and computing some result that holds interest for all parties. This happens for example in benchmarking, data mining,... So it can be seen that there is a real need for secret sharing, a need that is bigger every day. This was the main motivation for this work, as the need for these techniques make secret sharing an up to date and very important topic.

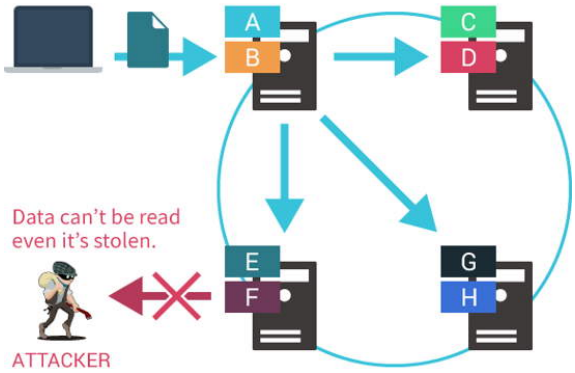

Figure 1.1: Secret Sharing Scheme example 1.

Following the topic of secret sharing, there are some important concepts related to it which the reader should become familiar with in order to understand this work. A secret sharing scheme is a method that allows some secret information, called the *secret* to be protected in a communication between a set P of different participants. This is achieved by assigning to each participant a small *share*, a piece of related information, in such way that only some subsets of them can recover the secret value by joining their shares. The subsets of participants that are able to recover the secret are called the qualified subsets, whereas the ones that cannot recompose it are called unqualified subsets. The qualified subsets of a secret sharing scheme compose the *access structure* of such scheme. The first examples of mathematically based secret sharing schemes were given by Blakley [9] and Shamir [31]. They presented a very useful type of secret sharing schemes called *threshold schemes*. Their most distinguishable characteristic is that the qualified subsets of the access structure include all sets of more than t players, for some threshold value t. Threshold secret sharing schemes have also found numerous applications in cryptography. In most of these applications, one tries to use the "best" known scheme for the access structure at hand. There is a small explanation of Blakley and Shamir solutions for the Secret Sharing problem in [2], which goes deeper into threshold secret sharing schemes as well.

Secret sharing schemes can be defined from several geometrical figures, such as matroids, polymatroids or graphs. Matroids and polymatroids are the most common ones, and they are defined as a pair of a set and a function that meet some particular requirements (this will be explained later).

One of the ways of measuring the efficiency of a secret sharing scheme is the so-called *(average) information ratio*. These parameters can be calculated for every secret sharing scheme that can be used for an access structure (there are many secret sharing schemes that have the same access structure). They are defined as the (average) ratio between the maximum length of the shares of every participant and the length of the secret. The optimal information ratio of an access structure Γ is defined as the infimum of the information ratios of all secret sharing schemes for Γ. The optimal average information ratio is defined analogously. They are usually represented as $\sigma(\Gamma)$ and by $\widetilde{\sigma}(\Gamma)$. The computation of these parameters is one of the most important open problems in secret sharing nowadays. Although it is true that some partial results have been found, there are still some important questions that remain unsolved. Due to the difficulty of finding general results,

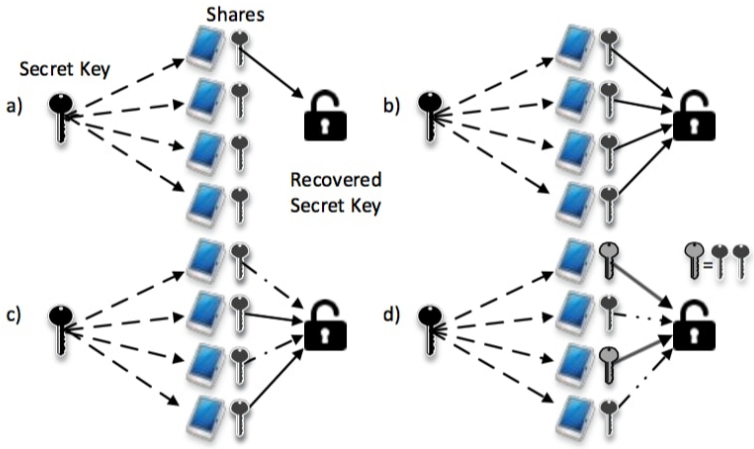

Figure 1.2: Secret Sharing Scheme example 2.

this problem has been considered for many different families of access structures in [8, 12, 13, 14, 15, 19, 24, 25] among other works. One of the greatest achievements has been made by Csirmaz and Tardos [14] who determined the optimal information ratio for all access structures that are defined by trees. As it is an up to date issue that has no defined solution, the objective of this paper is to provide better lower bounds regarding the optimization of this parameters, despite that it will be commented how upper bounds can be found and some examples will be given. This optimization results in shorter shares for every participant within a secret sharing scheme, which is why their value is used to measure the efficiency of the scheme.

Linear secret sharing scheme are an interesting type of secret sharing scheme due to their homomorphic properties, which are important for some of the applications of secret sharing (such as secure multi-party computation). In a linear secret sharing scheme, the secret value and the shares are vectors over some finite field, and the shares of the participants are values of a given linear map over some random vector. Linear secret sharing schemes are obtained by applying some of the best-known techniques to construct efficient schemes, such as the decomposition method by Stinson [33]. When studying linear schemes, it is interesting to define new parameters $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, which correspond to the infimum of the (average) information ratios of all linear secret sharing schemes for Γ. Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$. Actually, almost all known upper bounds on the optimal information ratio are upper bounds on $\lambda(\Gamma)$, and the same applies to the corresponding parameters for the average optimal information ratio. Even though non-linear secret sharing schemes have been proved to have lower information ratios in general, there are not many known examples of access structures with $\sigma(\Gamma) < \lambda(\Gamma)$.

On the other hand, Csirmaz [11] explained that most of the lower bounds for the optimal information ratio have been found by using a combinatorial method based on the connection between the Shannon entropy and polymatroids, which was presented by Fujishige in [20]. The best known asymptotic lower bound was obtained in [11] by using this method. The parameter $\kappa(\Gamma)$ was introduced in [25] (and will be used in this paper as well) to denote the best lower bound on $\sigma(\Gamma)$ that can be obtained by using this technique. In fact, so far it has been checked that $\kappa(\Gamma) = \lambda(\Gamma)$ for all access structures whose optimal complexity has been determined. This is a consequence of the techniques used until now. The combinatorial method

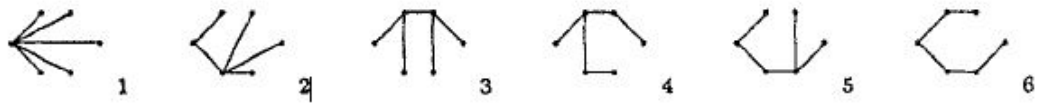

Figure 1.3: Example of some access structures on 6 participants defined by graphs.

has been used in several works to provide lower bounds on κ, which result in lower bounds in σ. It was used for example in [24] and in [29]. However, the decomposition methods usually result in linear secret sharing schemes and hence, bounds (upper bounds) in λ.

This method can be formalized as a linear program, which is the strategy that has been followed for this work. Together, polymatroids and access structures define the feasible region for the linear programs used when computing the lower bounds on the information ratio (all of this will be further explained later on). This is the scheme followed in order to get the results presented here: First, polymatroids axioms have been translated into linear constraints using their connection with Shannon entropy. Then these constraints have been used, together with the conditions of access structure, to define the feasible region of the linear programs. Finally, these programs have been executed using the Sage solver and the bounds have been computed. In the interest of simplification, only *perfect* or *unconditionally secure* secret sharing schemes are going to be considered. A secret sharing scheme is said to be *perfect* if the members in unqualified subsets cannot get any information of the secret. This kind of secret sharing schemes are easier to study as every subset that is not qualified is forbidden. Besides, this work has focused on access structures with only 5 and 6 participants, and especially on upgrading the lower bounds for the information ratio for those access structures.

Jackson and Martin [24] used both the combinatorial method and the decomposition method explained before in order to find lower and upper bounds for all access structures on 5 participants. They were able to determine the exact value of the information ratio for almost all of this access structures. In particular, the exact value of the information ratio was obtained for the ones that had the lower bound equal to the upper bound. They did all the calculations manually but, for the purposes of this work, new linear programs are used when calculating the lower bounds. This programs were first used in [29] and it was possible to improve some of the bounds given by Jackson and Martin. Using this approach, all the lower bounds presented in [24] were checked by translating the polymatroid axioms into linear constraints. That is, using only the *Shannon information inequalities*. However, as it was discovered later some of the bounds Jackson and Martin found can be improved by effectively adding new information or rank inequalities. Therefore, for some of the access structures which optimal information ratio had not been found yet, constraints using *non-Shannon information inequalities* were defined. Including these new constraints in the linear programs, it was possible to improve some of the bounds presented in [24], as it was done by Carles Padró, Leonor Vàzquez and An Yang in [29]. Basically, the strategy followed for the proof of the Ingleton's inequality (although the inequality itself was not used because it did not work properly with the programs) was implemented.

This work is divided into three parts. The first one will provide an introduction

to secret sharing, including all the concepts presented in this chapter and their mathematical definition. The linear programs that have been used to check the lower bounds given by Jackson and Martin as well as the lower bounds given by Van Dijk [15] for graph-based access structures, will also be explained in this part. Then, it will follow an explanation of the new constraints used to improve some of the results presented by Jackson and Martin. Finally the last part of the work will analyze how, with the help of the Shannon information inequalities, the bounds given by Van Dijk will be checked. They are bounds for the information ratio on access structures defined by graphs with 6 participants. These particular access structures have the characteristic that their minimal qualified subsets are always compounded by two participants. Apart from this checking, new bounds for the optimal average information ratio will be given as well, again using Shannon information inequalities. One example of a graph defined access structure can be found in Figure 1.3.

In order to understand the idea of secret sharing, there are some previous concepts the reader should become familiar with. For that purpose, a brief introduction on matroids and polymatroids will be given, followed by an explanation of secret sharing schemes and access structures along with some important properties. Also, the linear programs used will be further explored in this preliminary section.

Chapter 2

Secret Sharing, Matroids and Polymatroids

2.1 Matroids and Polymatroids

For the whole section, Q will be a finite set and $\mathcal{P}(Q)$ will be its power set, that is, the set of all subsets in Q.

Definition 2.1.1. *A polymatroid is a pair $S = (Q, f)$ where f is a map satisfying:*

1. $f(\emptyset) = 0$
2. f is monotone increasing: $A \subseteq B \subseteq Q \Rightarrow f(A) \leq f(B)$, for every $A, B \subseteq Q$
3. f is submodular:$f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$ for every $A, B \subseteq Q$

Q is called the *ground set* and f the *rank function* of S. Moreover, if f is integer valued, then S is said to be an *integer polymatroid*.

Definition 2.1.2. *A matroid M is an integer polymatroid (Q, r) which rank function r satisfies the following condition: $r(A) \leq |A|$, for all $A \subseteq Q$. The independent sets of M are he ones with $r(A) = |A|$ while the dependent sets are the ones with $r(A) < |A|$.*

Some polymatroids can be obtained from others by applying special operations. If $c \in \mathbb{R}, c \geq 0$, this implies that $cS = (Q, cf)$ is a polymatroid called *multiple* of S.

Definition 2.1.3. *Let $\mathcal{Z} = (Q, f)$ be an integer polymatroid, E be a vector space over some finite field $\mathbb{K}$ and $(V_i)_{i \in Q}$ a tuple of subspaces E. Then, if:*

$$f : \mathcal{P}(Q) \longrightarrow \mathbb{Z},$$
$$f(X) = \dim \left(\sum_{i \in X} V_i \right), X \in Q$$

$\mathcal{Z}$ is said to be a $\mathbb{K}$-linear polymatroid and $(V_i)_{i \in Q}$ is called a $\mathbb{K}$-linear representation of $\mathcal{Z}$. A $\mathbb{K}$-poly-linear polymatroid is a multiple of a a $\mathbb{K}$-linear polymatroid.

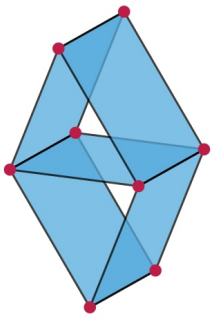

Figure 2.1: Vamos Matroid.

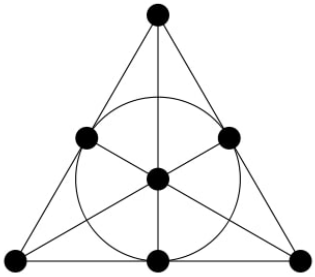

Figure 2.2: Fano's Matroid.

Two interesting examples of matroids are the Vamos matroid and the Fano matroid, which are represented in figure 2.1 and in figure 2.2. These pictures give an idea of both Vamos and Fano's matroid. They both define a secret sharing scheme and an access structure. The dependent and independent subsets can be seen as unauthorized and authorized subsets. For the Vamos matroid, all 3-sets (sets with 3 elements) are independent (which implies that all 2-sets are also independent), whereas all the subsets with 5 elements are dependent. For the case of subsets with 4 elements they are dependent if the four elements are coplanar in figure 2.1 and independent if they are not. One can easily see the dependent subsets of the Vamos matroid as they are the ones that are composed of the vertices conforming the colored faces of the figure. One interesting property of this matroid is that the two top vertices and the two bottom vertices are not coplanar, while the four middle ones are (one can see it as the plane generated by the middle vertices is colored, while the one generated by the top and bottom ones is not). Indeed, that is the reason why the Vamos matroid is not representable over any field.

With respect to Fano's matroid, it is actually a representation of the projective plane of 2 dimensions. All 2-subsets are independent, whereas the 3-subsets are dependent if the vertices composing them are aligned and independent if they are not. For instance, every side of the triangle in figure 2.2 is dependent, while the vertices over the small circle are not. It is representable over every field with characteristic 2.

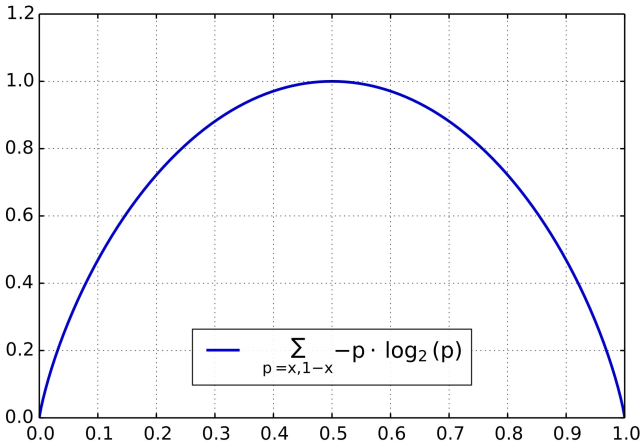

Figure 2.3: Shannon entropy visual example of a binary random variable.

2.2 Shannon Entropy and Entropic Polymatroids

Definition 2.2.1. *Let X be a discrete random variable on the finite set E. The Shannon entropy of X is*

$$H(X) = -\sum_{x \in E} p(x) \log p(x),$$

where $p(x) \log(p(x)) = 0$ if $p(x) = 0$.

The binary logarithm is taken. The Shannon entropy measures the average amount of bits necessary to represent the information given by all the possible events of the variable X. The least probable events result in a bigger logarithm (in absolute value) which means that they provide more information. However, they are less probable so they occur less times that the more probable ones. In figure 2.3, one can find a visual interpretation of the Shannon entropy of a binary random variable. This image depicts the value of the entropy for a random variable with only 2 events, one with $p(x_1) = x$, and the other with $p(x_2) = 1 - x$. One can see that the bigger entropy is obtained when $p(x_1) = p(x_2) = \frac{1}{2}$, which correspond to the uniform distribution. On the other hand, one can see that $H(X) = 0$ when the probability of one of the events is 1 and the probability of the other is 0. The idea of Shannon entropy is to know which event will be the upcoming one, so if on has one event with a high probability and one with a low one, it will be easier to determine which event will be coming up next than when we have the same probability for all the events.

Proposition 2.2.2. *One interesting property about the Shannon entropy is*

$$0 \leq H(X) \leq \log |E|$$

$H(X) = 0$ when there is one event x_0 of the random variable X with probability $p(x_0) = 1$. On the other side, $H(X) = 1$ if X follows a uniform distribution, which means that $p(x_i) = p(x_j) = 1/|E|$, for every $x_i, x_j \in E$

If one considers now X and Y two random variables on the sets E and F, respectively, then the entropy of the random variable (X, Y) on the set $E \times F$ is

$$H(XY) = -\sum_{(x,y) \in ExF} p(x, y) \log(p(x, y))$$

Besides, for every $y \in F$, one can consider the random variable $X|Y = y$ on the set E, which entropy is

$$H(X|Y = y) = -\sum_{x \in E} p(x|y) \log\left(p(x|y)\right)$$

Definition 2.2.3. *Let X be and Y be random variables on the sets E and F. The conditional entropy of X with respect to Y is:*

$$H(X|Y) = -\sum_{y \in F} p(y) \left(\sum_{x \in E} p(x|y) \log(p(x|y)) \right)$$

There are also some interesting properties related with the conditional Shannon entropy that will be useful later on to understand some of the upcoming concepts.

Proposition 2.2.4. *For a Discrete random variable X on a set E, the following properties hold*

1. $0 \leq H(X|Y) \leq H(X)$. *Here, $H(X|Y) = 0$ if and only if for every $y \in F$, there exists an $x \in E$ such that $p(x|y) = 1$, whereas $H(X|Y) = H(X)$ if and only if the random variables X and Y are independent.*

2. $H(XY) = H(Y) + H(X|Y) = H(X) + H(Y|X)$

There are two other functions that help to understand the relation between Shannon entropy and polymatroids, which are the *Mutual information* and the *Conditional Mutual information*. These two concepts will be defined here, although they are explained later in chapter 4.

Definition 2.2.5. *Let X and Y in the sets E, F be two (discrete) random variables and (X, Y) in the set $E \times F$ another random variable which is distributed according to the probability function $p(x, y)$. Then the mutual information of X and Y is*

$$\begin{aligned} I(X;Y) &= \sum_{(x,y) \in E \times F} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(XY) \end{aligned}$$

Definition 2.2.6. *The conditional mutual information of two random variables X, Y given the value of a third Z is defined as:*

$$I(XY|Z) = H(XZ) + H(YZ) - H(XYZ) - H(Z) = H(X|Z) - H(X|YZ)$$

Proposition 2.2.7.

$$I(XY|Z) \geq 0$$

where X, Y, Z are random variables.

These are the most important properties related to Shannon entropy and they explain the connection between such entropy and polymatroids. Consider now a random vector $(S_i)_{i\in Q}$, $S_i \in E_i$, where E_i is the support of the random variable S_i. For every $A \subseteq Q$, the variable S_A denotes 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. It was Fujishige [27, 28] who found the relation between such entropy and polymatroids, as stated in the following theorem.

Theorem 2.2.8. *Let $(S_i)_{i\in Q}$ be a family of random variables. Consider the mapping $h : P(Q) \longrightarrow \mathbb{R}$, defined by $h(\emptyset) = 0$ and $h(A) = H(S_A)$, for all $A \subseteq Q, A \neq \emptyset$. Then h is the rank function of a polymatroid with ground set Q.*

As a consequence of this last theorem, one can now use a family of discrete random variables to represent a polymatroid. This will define a new type of polymatroids.

Definition 2.2.9. *A polymatroid $S = (Q, f)$ is said to be entropic if there exists $(S_i)_{i\in Q}$ a family of discrete random variables such that $h(A) = H(S_A)$, for every $A \subseteq Q$.*

Theorem 2.2.10. *Let $\mathbb{K}$ be a finite field and $S = (Q, f)$ a $\mathbb{K}$-linear polymatroid. If one takes $c = \log|\mathbb{K}|$, then $S_2 = (Q, cf)$ is an entropic polymatroid, which means that, in particular, every poly-linear polymatroid is entropic.*

Before proving this last theorem, it is necessary to define a special type of families of discrete random variables, the ones defined by linear maps

Definition 2.2.11. *Consider a finite field $\mathbb{K}$, a family $(E_i)_{i\in Q}$ of $\mathbb{K}$-vector spaces and an injective $\mathbb{K}$-linear map:*

$$\pi : E \longrightarrow \prod_{i\in Q} E_i$$

such that the induced linear maps $\pi_i : E \longrightarrow E_i$ are surjective. By taking the uniform probability distribution on E, these linear maps define a random variable $S_i \in E_i$, for every $i \in Q$. A random vector $(S_i)_{i\in Q}$ that can be defined like this is said to be $\mathbb{K}$-linear.

Proof. Consider a $\mathbb{K}$-linear random vector $(S_i)_{i\in Q}$. If, for every $A \subseteq Q$ one considers the linear map $\pi_A : E \longrightarrow \prod_{i\in A} E_i$, defined by $\pi_A(x) = \pi_i(x)_{i\in A}$, then it is clear that:

$$H(S_A) = \operatorname{rank}\pi_A \log(|\mathbb{K}|) = (\dim E - \dim\ker(\pi_A))\log(|\mathbb{K}|)$$

Now, for every $i \in Q$ consider $W_i = \ker\pi_i$ and its orthogonal subspace $V_i = W_i^{\perp} \subseteq E^*$. The collection $(V_i)_{i\in Q}$ of subspaces define a $\mathbb{K}$-linear integer polymatroid $\mathcal{Z} = (Q, f)$ with:

$$f(A) = \dim\sum_{i\in A} V_i = \dim E - \dim\left(\sum_{i\in A} V_i\right)^{\perp} = \dim E - \dim\cap_{i\in A} W_i.$$

Finally, as $\ker\pi_A = \cap_{i\in A}\ker\pi_i$:

$$f(A) = \dim E - \dim\ker\pi_A = \frac{H(S_A)}{\log(|\mathbb{K}|)}$$

Because of the last equality, one has that $h(A) = \log(|\mathbb{K}|)f(A) = cf(A) = H(S_A)$ for every $A \in Q$, and hence the polymatroid $S = (Q, cf)$ is poly-entropic. □

The previous results and definitions provide a small introduction to matroids and polymatroids, which could be considered as the containers for the elements included in a secret sharing scheme. However, in order to understand the process involved in secret sharing, one needs to know some other concepts as well.

2.3 Secret Sharing Schemes and Access Structures

Definition 2.3.1. *An access structure* Γ *is a monotone increasing set of subsets of* P*, the set of participants. It is determined by the minimal family of subsets* $\min\Gamma$ *that are qualified*

$$\Gamma = \min\{B \in Q : H(S_0|S_B) = 0\}$$

Definition 2.3.2. *If* $\Gamma = (A)$*,* $A \in \mathcal{P}(Q)$*, is an access structure, the dual access structure of* Γ *is* $\Gamma^* = (A^c)$ *defined on the same set* Q *as*

$$\Gamma^* = \{B \in P : P \setminus B = \overline{B} \notin \Gamma\}$$

Definition 2.3.3. *A perfect secret sharing scheme is a family of random variables* $(S_i)_{i \in Q}$ *with support sets* $(E_i)_{i \in Q}$ *such that:*

1. $A \in \Gamma$ *(A is a qualified subset) if* $H(S_0|S_A) = 0$*.*
2. $B \notin \Gamma$ *(B is an unqualified subset) if* $H(S_0|S_B) = H(S_0)$*.*

for every $A, B \subseteq Q$*, ground set.* S_0 *corresponds to the random variable that is related to the dealer,* p_0

One could understand a *secret sharing scheme* as a method for distributing a secret value among a set of participants P in a way that only some subsets of participants, the *qualified subsets*, are able to recover the secret value by combining their shares (piece of information each of them receives). A secret sharing scheme is called *perfect* if the non-qualified subsets of participants cannot have any more information about the secret that could have an outsider to the secret sharing scheme (and thus, they are not only unqualified but also *forbidden*). Non-perfect secret sharing schemes are also studied by some authors, but they will be not treated in this work for simplification purposes. All the concepts presented in this chapter are defined only for perfect secret sharing schemes.

Definition 2.3.4. *An access structure is connected if every participant* $x \in P$ *is in a minimal qualified set. If* Γ *is connected, then* Γ^* *is connected.*

Definition 2.3.5. *The information ratio and average information ratio of a secret sharing scheme* $\Sigma = (S_i)_{i \in Q}$ *are represented as* $\sigma(\Sigma)$ *and* $\widetilde{\sigma}(\Sigma)$*, and they are defined as the (average) maximum relation of length of the shares related to the length of the secret*

$$\sigma(\Sigma) = \frac{\max\{H(S_i) : i \in Q\}}{H(S_0)}$$

$$\widetilde{\sigma}(\Sigma) = \frac{1}{n}\sum_{i \in Q} H(S_i)$$

Definition 2.3.6. *Let P be a finite set of participants, $p_0 \notin P$ a special element called the dealer, $Q = P \cup \{p_0\}$ and. Given a map $h : \mathcal{P}(Q) \longrightarrow \mathbb{R}$, a secret sharing scheme Σ on P is a collection of discrete random variables $(S_i)_{i \in Q}$ such that $h(p_0) > 0$, where $h : P(Q) \longrightarrow \mathbb{R}$, $h(\emptyset) = 0$ and $h(A) = H(S_A)$, for every $A \neq \emptyset, A \subseteq Q$.*

Consider $S = (Q, f)$ a polymatroid, and $p_0 \in Q$ one distinguished element of Q with $f(p_0) > 0$. Then $\Gamma_{p_0}(S)$ is an access structure defined by:

- $A = \{B \subseteq Q : f(p_0|B) = 0\}$

Besides, if M is a matroid, then $\Gamma_{p_0}(M)$ is said to be a a *matroid port* or, more specifically, *the port of the matroid M at the point p_0*. To end this sections, two important parameters will be introduced. These two parameters are used as a measure of efficiency for a secret sharing scheme, and their optimization is the main motivation of this work.

2.4 Linear Secret Sharing Schemes

Definition 2.4.1. *For a finite field $\mathbb{K}$, a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ is a $\mathbb{K}$-linear (or simply linear) secret sharing scheme if $(S_i)_{i \in Q}$ is a $\mathbb{K}$-linear family of random variables or random vector. The support of the random vector $(S_i)_{i \in Q}$ are vector subspaces $(E_i)_{i \in Q}$*

In this case, the random variable S_{p_0} corresponds with the secret value of the scheme. The information, secret value included, is distributed among all the different the participants according to the random variables $(S_i)_{i \in Q}$. The random variable S_i regulates the information acquired by the participant p_i, and S_{p_0} regulates how the secret value is distributed throughout the participants. Linear secret sharing schemes can be represented by matrices. Brickell [22] presented a method for constructing perfect secret sharing schemes for some access structures that were based on linear codes.

Definition 2.4.2. *Using these concepts, the information ratio of a linear secret sharing scheme can be defined as*

$$\lambda(\Sigma) = \frac{\max \dim E_i}{\dim E_0}$$

Definition 2.4.3. *A $\mathbb{K}$-linear secret sharing scheme in which $E_i = \mathbb{K}$, for every $i \in Q$ is called a $\mathbb{K}$-vector space secret sharing scheme*

For every collection $(\pi_i)_{i \in Q}$ of non-zero linear forms on a $\mathbb{K}$-vector space E and for every choice of a distinguished participant $p_0 \in Q$ (which will be the dealer), a $\mathbb{K}$-vector space secret sharing scheme is generated on $P = Q - \{p_0\}$. Such schemes are always perfect. Besides, a set $A \subseteq P$ is qualified if and only if the linear form $\pi_{p_0} \in E^*$ (which is the linear form associated to the dealer) is a linear combination of the linear forms $(\pi_i)_{i \in A}$.

Let Σ be a $\mathbb{K}$-vector space secret sharing scheme and $S = (Q, h)$ its associated polymatroid. Given a basis of the vector space E consider the matrix G such that

$\pi(x) = xG$ for every $x \in E$. This means that every column of $G = (G_0|G_1|\cdots|G_n)$, where G_i is a $k \times k_i$ matrix, corresponds to the linear form π_i. The columns of G_i are linear forms in E (that is, vectors in E^*) and correspond to the vector subspace V_i, for every $i \in Q$. G_i has as many columns as the dimension of the subspace V_i. If one considers the matrix representation of a secret sharing scheme, C is a vector subspace of the vector space $E = (E_0 \times E_1 \times \cdots \times E_n)$. Every codeword $(s_0 \times s_1 \times \cdots \times s_n) \in C \subseteq (E_0 \times E_1 \times \cdots \times E_n)$ corresponds to a share vector of the secret sharing scheme (it describes a different distribution of the shares of the participants). The entry of the codeword given by the dealer, p_0, corresponds to the secret value, and the other entries correspond to the shares that have to be distributed among the rest of participants (s_i corresponds to the share of the participant i). All the linear combinations of words conform the vector subspace C. In a perfect secret sharing scheme, if a subset of participants is authorized, then the columns corresponding to the subspaces of the participants included in the subset generate the columns that correspond to the subspace of the secret value (G_0).

G can be see as the generator matrix of a linear code $C \subseteq K^Q$ that has length $|Q| = n+1$. The code defines a $\mathbb{K}$-linear matroid $M = (\widehat{Q}, r)$ whose ground set $\widehat{Q}$ is in one to one correspondence with the columns of G. For that reason $\widehat{Q} = \cup_{i \in Q} \widehat{Q}_i$, where $|\widehat{Q}_i| = k_i$. The integer polymatroid $\mathcal{Z} = (Q, f)$ that is defined by the subspaces $(V_i)_{i \in Q}$ can be determined from the matroid M because $f(A) = r(\cup_{i \in A} \widehat{Q}_i)$ for every $A \subseteq Q$.

On the other hand, when taking into account the dual code $C^\perp$ of C, it has generator matrix $H = (H_0|H_1|\cdots|H_n)$ which is the transpose matrix of a parity check matrix of C. It defines a secret sharing scheme Σ^* on the same set of participants as Σ, which is called the *dual linear secret sharing scheme* of Σ. Besides, the code $C^\perp$ is a $\mathbb{K}$-linear representation of the dual matroid $M^* = (\widehat{Q}, r^*)$ of M. The access structure of Σ^* is $\Gamma_{p_0}(\mathcal{Z}^*)$, where $\mathcal{Z}^* = (Q, f^*)$ is the polymatroid defined by:

$$f^*(A) = r^*\left(\bigcup_{i \in A} \widehat{Q}_i\right) = \left|\bigcup_{i \in A} \widehat{Q}_i\right| - r(\widehat{Q}) + r\left(\bigcup_{i \in Q-A} \widehat{Q}_i\right) = \sum_{i \in A} k_i - k + f(Q - A)$$

for every $A \subseteq Q$. The formula for r^* is given by the following proposition:

Proposition 2.4.4. *If $M = (Q, r)$ matroid and r^* rank function of $M^* = (Q, r^*)$, then $r^*(A) = |A| - r(Q) + r(Q - A)$, for every $A \subseteq Q$*

To illustrate the previous concepts of linear codes and secret sharing schemes defined by matrices, here is an example (which was taken from Carles Padró lecture notes): Take $Q = \{0, 1, 2, 3, 4\}$ and $p_0 = 0$. Consider a finite field $\mathbb{K}$, the $\mathbb{K}$-vector space $E = \mathbb{K}^6$ and $(E_i)_{i \in Q}$ with $E_0 = E_1 = E_4 = \mathbb{K}^2$ and $E_2 = E_3 = \mathbb{K}^3$. Then Σ is a linear secret sharing scheme on P defined by the linear map $\pi : E \longrightarrow \prod_{i \in Q} E_i$ given by the matrix:

$$G = \left(\begin{array}{cc|cc|ccc|ccc|cc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

Now,if one considers for $i \in Q = \{0, 1, 2, 3, 4\}$ vector subspaces $V_i \subseteq E^*$ represented by the columns of G. A subset will be qualified if $V_0 \subseteq (V_i)_{i \in A}$. It is simple to check that $V_0 \subseteq V_i + V_j$ if $\{i, j\}$ is one of the following subsets: $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $A_3 = \{3, 4\}$ and that $V_0 \cap (V_i + V_j) = \{0\}$ if $\{i, j\}$ is any other 2 subset of $\{1, 2, 3, 4\}$. This means that the secret sharing scheme defined from the linear mappings π_i is perfect and the minimal qualified subsets in its access structure are A_1, A_2, A_3. The information ratio, as one can see from the dimensions of the subspaces $(V_i)_{i \in A}$, is $3/2$. It can be seen that the longest shares have length 3 (3 columns are needed to represent the vector subspaces V_2 and V_3) while the secret has length 2 (the vector subspace V_0 has dimension 2), which means that $\sigma(\Gamma) = 3/2$ because of the definition of $\sigma(\Gamma)$.

Chapter 3

Parameters to be optimized

3.1 State of the Art

One of the most widely used ways of measuring the efficiency of a secret sharing scheme is the computation of two important parameters that were introduced in the previous chapter: the information ratio and average information ratio of the scheme. For a particular access structure, they are defined as the infimum ratio between the maximum (or average) length of the shares and the length of the secret from all the different secret sharing schemes for that particular access structure. The maximum, for the information ratio, and the average, for the average information ratio. This parameters are represented as $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$, respectively.

Definition 3.1.1. *The information ratio $\sigma(\Gamma)$ and average information ratio $\widetilde{\sigma}(\Gamma)$ of an access structure Γ are defined as*

- $\sigma(\Gamma) = \inf\{\sigma(\Sigma)$*: Σ is a secret sharing scheme for* $\Gamma\}$
- $\sigma(\Gamma) = \inf\{\widetilde{\sigma}(\Sigma)$*: Σ is a secret sharing scheme for* $\Gamma\}$

Remember that $\sigma(\Sigma)$ and $\widetilde{\Sigma}(\Gamma)$ are defined as:

$$\sigma(\Sigma) = \frac{\max\{H(S_i) : i \in Q\}}{H(S_0)}$$

$$\widetilde{\sigma}(\Sigma) = \frac{1}{n}\sum_{i \in Q} H(S_i)$$

Analogously, the parameters $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ are used to represent the (average) information ratio when taking into account only linear secret sharing schemes and access structures.

Definition 3.1.2. *The information ratio $\lambda(\Gamma)$ and average information ratio $\widetilde{\lambda}(\Gamma)$ of an access structure Γ are defined as*

- $\lambda(\Gamma) = \inf\{\lambda(\Sigma)$*: Σ is a linear secret sharing scheme for* $\Gamma\}$
- $\lambda(\Gamma) = \inf\{\widetilde{\lambda}(\Sigma)$*: Σ is a linear secret sharing scheme for* $\Gamma\}$

The following definition is motivated by the connection between secret sharing schemes and polymatroids.

Definition 3.1.3. *Given $S = (Q, f)$ a polymatroid and $p_0 \in Q$*

$$\sigma_{p_0}(S) = \frac{\max\{f(i) : i \in Q - \{p_0\}\}}{f(\{p_0\})} \quad \widetilde{\sigma}_{p_0}(S) = \frac{1}{|Q| - 1} \sum_{i \in Q - \{p_0\}} \frac{f(\{i\})}{f(\{p_0\})}$$

This provides a different characterization of the optimal information ratio

- $\sigma(\Gamma) = \inf\{\sigma_{p_0}(S)\colon\ S \text{ is a entropic polymatroid with } \Gamma = \Gamma_{p_0}(S)\}$
- $\widetilde{\sigma}(\Gamma) = \inf\{\widetilde{\sigma}_{p_0}(S)\colon\ S \text{ is a entropic polymatroid with } \Gamma = \Gamma_{p_0}(S)\}$

And then again when considering only linear secret sharing schemes one obtains poly-linear polymatroids, so the corresponding parameters are

- $\lambda(\Gamma) = \inf\{\sigma_{p_0}(S)\colon\ S \text{ is a poly-linear polymatroid with } \Gamma = \Gamma_{p_0}(S)\}$
- $\widetilde{\lambda}(\Gamma) = \inf\{\widetilde{\sigma}_{p_0}(S)\colon\ S \text{ is a poly-linear polymatroid with } \Gamma = \Gamma_{p_0}(S)\}$.

Also, a new parameter can be used in order to obtain lower bounds for $\sigma(\Sigma)$

- $\kappa(\Gamma) = \inf\{\sigma_{p_0}(S)\colon\ S \text{ is a polymatroid with } \Gamma = \Gamma_{p_0}(S)\}$
- $\widetilde{\kappa}(\Gamma) = \inf\{\widetilde{\sigma}_{p_0}(S)\colon\ S \text{ is a polymatroid with } \Gamma = \Gamma_{p_0}(S)\}$

These are the parameters for which upper and lower bounds are trying to be found in this work. By giving the correct upper and lower bounds, one can find the optimal value of the parameters, which will provide a measure of the efficiency of the schemes. The optimal value is only completely determined when it is checked that the better lower bound and upper bound that have been calculated for a secret sharing scheme are equal. Then, one can conclude that the optimal value of the parameter has been found.

It could be useful to know the relation between these parameters and their corresponding ones in the dual access structure. If Σ is a linear secret sharing scheme for Γ, one can obtain another linear secret sharing scheme with the same (average) information for the dual access structure Γ^*, which means that $\lambda(\Gamma^*) = \lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma^*) = \widetilde{\lambda}(\Gamma)$. It was proved in [25] that $\kappa(\Gamma^*) = \kappa(\Gamma)$ as well, and by using the same arguments, one can find out that $\widetilde{\kappa}(\Gamma^*) = \widetilde{\kappa}(\Gamma)$. Nevertheless, the behavior of $\sigma, \widetilde{\sigma}$ with respect to duality is yet unknown.

Taking a closer look to the definition of the aforementioned parameters, one can find some relations between them:

1. $1 \leq \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$
2. $1 \leq \widetilde{\kappa}(\Gamma) \leq \widetilde{\sigma}(\Gamma) \leq \widetilde{\lambda}(\Gamma)$

For every perfect access structure Γ. This technique has some limitations, though. The value of $\kappa(\Gamma)$ is bounded by Theorem 3.1.5. Before stating the theorem, a small proposition is needed in order to prove it

Proposition 3.1.4. *Let Γ be an access structure on a set P and $S' = (P, f)$ a polymatroid with ground set P. S' can be extended to a polymatroid $S = (Q, f)$ with $f(p_0) = 1$ such that $S \setminus \{p_0\} = S'$ and $\Gamma = \Gamma_{p_0}(S)$ if and only if the following conditions are satisfied*

1. *If* $A \subseteq B \subseteq P$ *are such that* $A \notin \Gamma$ *and* $B \in \Gamma$, *then* $f(A) \leq f(B) - 1$.

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

Even though it has been proved that there exists a secret sharing scheme for every access structure [37], the problem when studying general families of access structures is that length of the shares grow exponentially with the number of participants. The main opinion among the researchers in this field is that this problem is unavoidable. The best known asymptotical lower bounds were given by Csirmaz [11], who presented a family of access structures on an arbitrary number of participants n that had shares of length $\Omega(n/\log n)\times$length of the secret. Several other papers have worked in the search for lower bounds using the same technique [8, 17, 11, 24].

However, a negative result was proved in [11]. Csirmaz proved that the bounds obtained with this method using the conditions of access structure and the Shannon entropy constraints are, at most, linear in the number of participants.

Theorem 3.1.5. *If* Γ *is an access structure on a set of* n *participants, then* $\kappa(\Gamma) \leq n$

Proof. For a set P with $|P| = n$, consider the polymatroid $S' = (P, f)$ defined by $f(X) = n + (n-1) + \cdots (n-(k-1))$ if $|X| = k$, for every $X \subseteq P$. This polymatroid satisfies the conditions in Proposition 3.1.4 for every access structure Γ and hence, there exists a polymatroid with $\sigma(\Gamma) = n$ for every Γ. □

That is why, as it is explained in the next chapter, several non-Shannon information inequalities are included in this work in order to find better bounds. The first non-Shannon information inequalities were presented by Zhang and Yeung [36].

The linear programs used in this combinatorial method can also be improved by using rank inequalities, which apply to the joint entropies of collections of random variables defined from linear maps. The first rank inequality that cannot be derived from Shannon information inequalities was found by Ingleton [21]. The use of such rank inequalities improved the known lower bounds on the information ratio of linear secret sharing schemes for some particular families of access structures [13, 29]. It is important to remark that some difficulties arise when using non-Shannon information inequalities. On the one hand, only a few methods to derive rank and information inequalities are known and the general opinion is that many of them remain unknown. On the other hand, no spanning sets for the information or rank inequalities on a given number of variables are known. Even for four participants, there are a lot of independent information inequalities.

The negative result discovered by Csirmaz was generalized by Beimel and Orlov [30] who presented another negative result about the power of non-Shannon information inequalities to provide better lower bounds on the information ratio. Basically, they proved that the lower bounds that can be obtained by considering all the information inequalities in four or more variables that are known up to date are at most linear on the number of participants.

Another negative result was presented in [38] by Sebastià Martń, Carles Padró and An Yang who proved that by using information inequalities with a constant number of variables only polynomial lower bounds are obtained.

Nevertheless, the polymatroid technique (finding lower bounds on $\kappa(\Gamma)$, due to the construction and definition of the linear programs used to find such bounds) has been very helpful when studying some families of access structures. It is especially

useful for access structures with a small number of participants, as the ones considered in this work (5 and 6 participants only). This is the reason why the method has been used in several other works to compute lower bounds on the information ratio [23, 15]. Despite the fact that the same technique is used here, the main difference between those articles and this work is that here the linear programs are not solved manually. Instead, some programs are created in Python and those programs are used to compute the value of the bounds. Obviously this consideration increases the precision when calculating the bounds as the human factor is removed from the equation. These programs have been used both to check the results given so far and to find some new ones by including some non-Shannon information inequalities.

The **upper bounds** are obtained by finding a secret sharing scheme with the desired σ or λ (which means that the information ratio can be smaller, but not higher, as it is by definition, the *infimum* of the information ratios among all the secret sharing schemes that have Γ as access structure). This secret sharing scheme is usually found by using the decomposition method presented by Stinson [33], which results in linear secret sharing schemes (bounds for λ).

3.2 Improving the linear programming approach to the optimization of the information ratio

As it has been mentioned at the end of the last section, lower bounds given for $\sigma(\Gamma)$ are in fact lower bounds in $\kappa(\Gamma)$. Bounds on both $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ can be obtained by solving a linear programming problem. The fact that $\kappa(\Gamma) \leq \sigma(\Gamma)$ means that lower bounds on $\kappa(\Gamma)$ are also lower bounds for $\sigma(\Gamma)$. Let $S = (Q, f)$ be a polymatroid and $P = Q - \{p_0\}$ be its set of participants, with $|P| = n$. By reordering the elements of P, one can see the rank function f as a vector $f = (f(A))_{A \subseteq Q} \in \mathbb{R}^k$, where $k = |\mathcal{P}(Q)| = 2^{|Q|} = 2^{n+1}$. Imposing that S has to be a Γ-polymatroid ($\Gamma = \Gamma_{p_0}(S)$) some linear constraints are obtained for f. Besides, $\widetilde{\sigma}_{p_0}(S)$ is linear over the vector f, which means that $\widetilde{\kappa}(\Gamma)$ can be determined by solving:

Minimize $(\frac{1}{n}) \sum_{i \in P} f(\{i\})$

subject to f rank function of a Γ-polymatroid. This can be translated into:

1. $f(\{p_0\}) = 1$
2. $S = (Q, f)$ polymatroid
3. $\Gamma = \Gamma_{p_0}(S)$

On the other hand, $\sigma_{p_0}(S)$ is not linear on the vector f, which means that an auxiliary linear vector is needed in order to compute a linear problem to obtain the value of $\kappa(\Gamma)$:

Minimize v

subject to f rank function of a Γ-polymatroid

$v \geq f(\{i\})$, for all $i \in Q$

The main issue with these linear problems is that both the number of variables and the number of constraints are exponential on the number of participants. They can only be efficiently computed for access structures with a small number of participants. The feasible regions Ω and Ω' from the first and second problem are:

1. $\Omega = \Omega(\Gamma) = \{f \in \mathbb{R}^k : f \text{ is the rank function of a } \Gamma\text{-polymatroid}\}$
2. $\Omega' = \Omega'(\Gamma) = \{(f, v) \in \mathbb{R}^{k+1} : f \in \Omega \text{ and } v \geq f(\{i\}) \text{ for every } i \in Q\}$

As there is a Γ-polymatroid for every access structure, both regions are feasible and bounded, which means that $\kappa(\Gamma) = \min\{\sigma_{p_0}(\mathrm{S})\text{: } S \text{ is a } \Gamma\text{-polmatroid}\}$ and that $\kappa(\Gamma)$ is a rational number. The same applies for $\widetilde{\kappa}(\Gamma)$.

The main issue with these linear programs is the great amount of variables and constraints needed in order to solve them, so it may be a good idea to reduce the number of constraints. It can be achieved by using different techniques, such as:

1. Matúš [27] gave a characterization of polymatroids that helps to make the problem simpler by reducing the number of constraints that define these feasible regions:

$f : \mathcal{P}(Q) \longrightarrow \mathbb{R}$ is the rank function of a polymatroid wih ground set Q if and only if:

(a) $f(\emptyset) = 0$

(b) $f(Q - \{i\}) \leq f(Q)$, for every $i \in Q$

(c) $f(A \cup \{i\}) + f(A \cup \{j\}) \geq f(A \cup \{i, j\}) + f(A)$, for every $i, j \in Q, i \neq j$ and for all $A \subseteq Q - \{i, j\}$

2. $S = (Q, f)$ is a $\Gamma-$polymatroid if and only if:

(a) $f(\{p_0\}) = 1$

(b) $f(A \cup \{p_0\}) = f(A)$ for every $A \subseteq P$ is a minimal qualified subset of Γ.

(c) $f(B \cup \{p_0\}) = f(B) + 1$, for every $B \subseteq P$ maximal unqualified subset of Γ.

The second part will be used in this work in order to reduce the number of constraints of the linear programs. These conditions can be resumed by considering, for every $A \subseteq Q$, vectors $e_A \in \mathbb{R}^k$ with $e_A(A) = 1$ and $e_A(B) = 0$, for all $B \in \mathcal{P}(Q) - \{A\}$. The feasible reagion Ω can then be defined by the following set of linear constraints:

- $e_\emptyset^t f = 0$
- $(e_{Q-\{i\}} - e_Q)^t f \leq 0$, for every $i \in Q$
- $(e_{A\cup\{i,j\}} + e_A - e_{A\cup\{i\}} - e_{A\cup\{j\}})^t f \leq 0$, for every $\{i, j\} \in Q$ and $A \subseteq Q - \{i, j\}$
- $e_{\{p_0\}}^t f = 1$
- $(e_{A\cup\{p_0\}} - e_A)^t f = 0$, for every $A \in \min(\Gamma)$
- $(e_{B\cup\{p_0\}} - e_B)^t f = 1$, for every B maximal unqualified subset of Γ

Chapter 4

New approach for calculating the bounds

The optimal (average) information ratio, $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$, were first calculated by Jackson and Martin [24] for almost all access structures on 5 participants. The techniques they used provided lower bounds on $\kappa(\Gamma)$ and upper bounds on $\lambda(\Gamma)$. The value of $\sigma(\Gamma)$ is exactly determined if and only if these bounds imply that $\kappa(\Gamma) = \lambda(\Gamma)$, and the same occurs with $\widetilde{\sigma}(\Gamma), \widetilde{\kappa}(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$. Because of that, the results obtained for an access structure apply as well to its dual access structure, which reduces the number of cases to be studied.

In this paper, the lower bounds calculated in [24] have been checked with the help of some linear programs programmed in Python. Actually, they are solved using Sage solver, but the API of Sage in Python is used to simplify the implementation and comprehension of the programs. Using the Shannon information inequalities and the conditions of access structure, a mixed integer linear program was solved using GLP (Sage is included in this package). GLP is the linear programming kit provided by GNU (Linux) to solve linear problems. It uses simplex method in order to solve the problem. Further information on the simplex method can be found in [39, 40]. In order to use Sage, one needs a virtual machine, such as Virtual Box, and also an already mounted Sage operating system. It can be easily found how to download both of them on the Internet. Two programs have been created to initialize the constraints of the problem. The first one is used to calculate bounds on $\sigma(\lambda)$ by creating an auxiliary variable such that the objective function is to solve min(v) where $f(p_i) \leq v$, for every $i \in Q$. The second one calculates the value of $\widetilde{\sigma}(\lambda)$ using a similar strategy, but now the constraint in v is changed to $\sum_{i \in Q} f(p_i) \leq v$. In the end, the value obtained from the solution of the program has to be divided by the number of participants in order to to get the correct bound for $\widetilde{\sigma}(\lambda)$.

Some of the bounds obtained in [24] were improved by Carles Padró, Leonor Vàzquez and An Yang in [29] by using the same approach that has been used in this work. Actually, they were able to improve some bounds on $\widetilde{\sigma}(\lambda)$ but not on $\sigma(\lambda)$. Nevertheless, they found the exact value of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\lambda)$ which means that no better lower bounds can be obtained by the combinatorial techniques that have been used so far. These bounds can only be updated by either considering additional information or rank inequalities other than the basic Shannon inequalities (such as Ingleton's inequality, for the lower bounds) or by obtaining better constructions of secret sharing schemes for those access structures (upper bounds).

4.1 Non-Shannon Information Inequalities

The lower bounds obtained so far for $\kappa(\Gamma)$ and for $\widetilde{\kappa}(\Gamma)$ are not tight in general. This is due to the existence of the so called *Non-Shannon information inequalities*. The polymatroids axioms correspond to the Shannon information inequalities. These axioms together with the conditions of being an access structure conform the restrictions that have been used up to now. However, many other information inequalities have been found lately. First, a reminder on mutual information and conditional mutual information of two random variables will be given.

Definition 4.1.1. *The mutual information of two random variables X and Y supported on the sets E and F, respectively, is*

$$\begin{aligned} I(X;Y) &= \sum_{(x,y)\in E\times F} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(XY) \end{aligned}$$

Definition 4.1.2. *The conditional mutual information of two random variables X, Y given the value of a third Z is defined as:*

$$I(XY|Z) = H(XZ) + H(YZ) - H(XYZ) - H(Z) = H(X|Z) - H(X|YZ)$$

All the inequalities that can be derived from the expression:

$$\sum_{i\in Q} \alpha_i I(A_iB_i|C_i)$$

are the *Shannon information inequalities*. The inequalities regarding 3 or less random variables are all Shannon type. On the other hand, any non-trivial inequality that cannot be obtained as a linear combination of the expression for the conditional mutual information are said to be non-Shannon type information inequalities. For example, Randall Dougherty, Christopher Freiling and Kenneth Zeger [18] improved some of the lower bounds given by Jackson and Martin in [24] by effectively adding some non-Shannon inequalities.

One example of the inequalities they included (which is a Non-Shannon information inequality) is:

$$\begin{aligned} I(A,B) \leq & I(A;R|D) + I(D;R|B;C) + I(B;C|A;R) + I(B;C|D) \\ & + I(A;C|B;R) + I(A;B|C;R) + I(A;B|C) \end{aligned}$$

By using these Non-Shannon type information inequalities one can improve the lower bounds on $\kappa(\Gamma)$ and therefore better lower bounds on $\sigma(\Gamma)$ are achieved. In particular, the idea behind Ingleton's inequality has been used in this work as an additional constraint to the linear programs that could provide better lower bounds on $\lambda(\Gamma)$. The following notation has to be introduced in order to understand the next concepts: $f(X|Y) = f(X \cup Y) - f(Y)$.

Lemma 4.1.3. *If f is the rank function a Γ-polymatroid, then:*

$$f(\{b\}|\{c,d\}) - f(\{b\}|\{a,c\}) + f(\{d\}|\{a\}) \geq 0, \tag{4.1}$$

for every $a, b, c, d \in Q$ ground set.

Proof. Let $S = (Q, f)$ be a polymatroid with rank function f and ground set Q. Then, if f is the rank function of a polymatroid it is submodular by definition, which means that:

1. $f(A) \geq 0$, for every $A \subseteq Q$
2. $f(X|Y) \geq f(X|Y \cup Z)$, for every $X, Y, Z \subseteq Q$

and hence

$$\begin{aligned} &f(\{b\}|\{c,d\}) - f(\{b\}|\{a,c\}) + f(\{d\}|\{a\}) \\ &\quad \geq f(\{b\}|\{a,c,d\}) - f(\{b\}|\{a,c\}) + f(\{d\}|\{a,c\}) \\ &\quad = f(\{b,d\}|\{a,c\}) - f(\{b\}|\{a,c\}) \geq 0 \end{aligned}$$

□

Lemma 4.1.4. *If f is the rank function of a polymatroid, then:*

$$\begin{aligned} f(\{e\}) \geq &f(\{a\}|\{c\}) - f(\{a\}|\{b,c\}) + f(\{a\}|\{d\}) - f(\{a\}|\{b,d\}) + \\ &+ f(\{c\}) - f(\{c\}|\{d\}) + 2f(\{e\}|\{a\}) + 2f(\{e\}|\{a,b\}) \end{aligned} \tag{4.2}$$

for every five elements $a, b, c, d, e \in Q$.

Proof. By applying lemma 4.1.3 to the previous formula, one can see that:

1. $f(\{e\}|\{b\}) - f(\{a\}|\{b,c\}) \geq -f(\{a\}|\{c,e\})$
2. $f(\{e\}|\{b\}) - f(\{a\}|\{b,d\}) \geq -f(\{a\}|\{d,e\})$

Due to those two inequalities, the second term of the inequality, which will be referenced as α_1, obeys:

$$\begin{aligned} \alpha_1 \geq &f(\{a\}|\{c\}) - f(\{a\}|\{c,e\}) + f(\{a\}|\{d\}) - f(\{a\}|\{d,e\}) + \\ &+ f(\{c\}) - f(\{c\}|\{d\}) + 2f(\{e\}|\{a\}) = \alpha_2 \end{aligned}$$

By reordering the elements a, b, c, d, e in the inequality and using the lemma 4.1.3 twice again on α_2, one obtains:

$$\begin{aligned} \alpha_2 = &f(\{e\}|\{c\}) - f(\{e\}|\{a,c\}) + f(\{e\}|\{d\}) - f(\{e\}|\{a,d\}) + \\ &+ f(\{c\}) - f(\{c\}|\{d\}) + 2f(\{a\}|\{e\}) \end{aligned}$$

$$\alpha_2 \geq f(\{e\}|\{c\}) + f(\{e\}|\{d\}) + f(\{c\}) - f(\{c\}|\{d\}) = \alpha_3$$

Finally, applying lemma 4.1.3 one last time one gets:

$$\begin{aligned} \alpha_3 &= f(\{e\}|\{c\}) + f(\{c\}) - f(\{c\}|\{e\}) \\ &= f(\{e\} \cup \{c\}) - f(\{c\}) + f(\{c\}) - f(\{e\} \cup \{c\}) + f(\{e\}) \\ &= f(\{e\}) \end{aligned}$$

and the proof is concluded. □

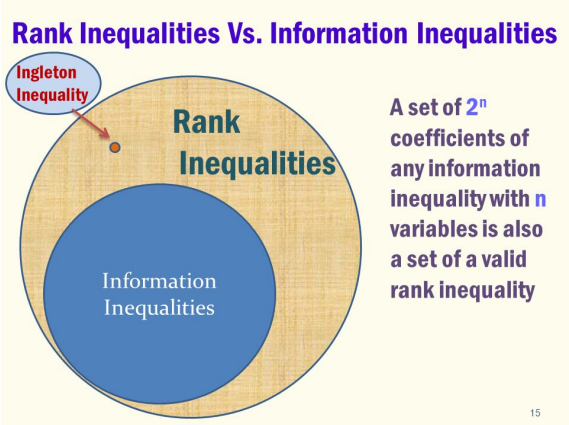

Figure 4.1: Relation between Shannon and non-Shannon information inequalities.

Definition 4.1.5. *Consider $S = (Q, f)$ a polymatroid and $A, B, C, D \subseteq Q$. Then,*

$$I(f; A, B, C, D) = f(A) + f(B) + f(C \cup D) + f(A \cup B \cup C) + f(A \cup B \cup D) - \\ - f(A \cup B) - f(A \cup C) - f(A \cup D) - f(B \cup C) - f(B \cup D) \tag{4.3}$$

Ingleton's inequality states that if $S = (Q, f)$ poly-linear polymatroid, then $I(f; A, B, C, D) \leq 0$, for every $A, B, C, D \subseteq Q$.

Moreover, according to [10], $S = (Q, f)$ poly-linear polymatroid if and only if $I(f; A \cup X, B \cup X, C \cup X, D \cup X) \leq 0$, for every $A, B, C, D \subseteq Q$ disjoint and non-empty sets. In Figure 4.1, one can see a visual example of the relation between Shannon inequalities and Ingleton's inequality.

Proof. The proof will be done for elements in the ground set and can be generalized to subsets of the ground set. It can be assumed that that S is $\mathbb{K}$-linear for some field K. Take $(V_i)_{1 \leq i \leq 4}$ a $\mathbb{K}$-linear representation of S and $V_5 = V_1 \cap V_2$. Consider now $\widehat{S} = (\widehat{Q}, f)$ with $\widehat{Q} = Q \cup \{x_5\}$ represented by $(V_i)_{1 \leq i \leq 5}$. Then:

$$f(\{x_5\}|\{x_1\}) = f(\{x_5\}|\{x_2\}) = 0$$
$$f(\{x_5\}) = f(\{x_1\}) - f(\{x_1\}|\{x_2\}$$

By applying lemma 4.1.4, one gets:

$$f(\{x_1\}) - f(\{x_1\}|\{x_2\}) - f(\{x_1\}|\{x_3\}) + f(\{x_1\}|\{x_2, x_3\}) - f(\{x_1\}|\{x_4\}) + \\ + f(\{x_1\}|\{x_2, x_4\}) - f(\{x_3\}) + f(\{x_3\}|\{x_4\} \leq 0$$

Expanding the previous expression, one has:

$$\begin{aligned} &f(\{x_1\}) - (f(\{x_1, x_2\}) - f(\{x_2\})) - (f(\{x_1, x_3\}) - f(\{x_3\})) + \\ &+ (f(\{x_1, x_2, x_3\}) - f(\{x_2, x_3\})) - (f(\{x_1, x_4\}) - f(\{x_4\})) + \\ &+ (f(\{x_1, x_2, x_4\}) - f(\{x_2, x_4\})) - f(\{x_3\}) + (f(\{x_3, x_4\}) - f(\{x_4\})) \\ &= f(\{x_1\}) + f(\{x_2\}) + f(\{x_1, x_2, x_3\}) + f(\{x_1, x_2, x_4\}) + f(\{x_3, x_4\}) - \\ &- f(\{x_1, x_2\}) - f(\{x_1, x_3\}) - f(\{x_2, x_3\}) - f(\{x_1, x_1\}) - f(\{x_2, x_4\}) \end{aligned}$$

which is the expression for the Ingleton's inequality for every 4 elements of the ground set Q. Using the same strategy with subsets instead of elements in the ground set, the proof is concluded. □

Ingleton's inequality was the first attempt of adding new restrictions in this work. For an access structure Γ one can consider the following linear program:

Minimize v

subject to f rank function of a Γ-polymatroid.

$I(f; A \cup X, B \cup X, C \cup X, D \cup X) \leq 0$, for every $A, B, C, D \subseteq Q$ disjoint and non-empty sets.

$v \geq f(\{i\}) \forall i \in Q$

As there exists a Secret sharing scheme for every Γ access structure [37], the linear program is feasible and bounded. Because it defines linear secret sharing schemes, the solution is a lower bound on $\lambda(\Gamma)$. In fact, it is the best lower bound on $\lambda(\Gamma)$ that can be obtained by adding only the Ingleton inequality to the Shannon information inequalities.

However, this information inequality did not work properly with the rest of the restrictions used in the linear programs created for the purpose of this paper, so a similar strategy was used instead. As it has been shown in the proof of the inequality, a new variable can be defined in order to represent the intersection of two different subsets, say $V_1 \cap V_2$. So, whenever it was needed to include any bound regarding the intersection of vector subspaces (when using non-Shannon information inequalities), a new variable is defined which will be equal to the intersection of such subsets. As Ingleton inequality, this approach can only be applied to linear secret sharing schemes, so in this case, by using this technique one is obtaining lower bounds on $\lambda(\Gamma)$.

Let $M = (Q, h)$ be a linear matroid and Σ a linear secret sharing scheme. The following mapping can be considered:

$$\begin{aligned} Participants: \quad & i \longrightarrow V_i \subseteq V \\ & j \longrightarrow V_j \subseteq V, \qquad V \subseteq \mathbb{F}^r \end{aligned}$$

One may want to include a new constraints based on non-Shannon information inequalities, such as:

$$h(i) + h(j) \geq h(i, j),$$

which is the same thing as to say:

$$\dim(V_i) + \dim(V_j) \geq \dim(V_i + V_j).$$

And it is known that the last inequality is satisfied by every two vector subspaces due to Grassmann equality:

$$\dim(V_i) + \dim(V_j) = \dim(V_i + V_j) + \dim(V_i \cap V_j),$$

But intersections cannot be easily imposed in our linear programs. The solution to this problem was, in this case, to declare an auxiliary variable called V_6 such that $V_6 = V_1 \cap V_2$. Using this new auxiliary participant new bounds in $\lambda(\Gamma)$ were found. The conditions above are translated accordingly to the definition of the new variable.

$$h(1) + h(2) = h(1,2) + h(6)$$

$$\left.\begin{array}{l} h(1) = h(1,6) \\ h(2) = h(2,6) \end{array}\right\} \equiv \begin{cases} \dim(V_1) = \dim(V_1 + V_6) = \dim(V_1 + V_1 \cap V_2) \\ \dim(V_1) = \dim(V_1 + V_6) = \dim(V_1 + V_1 \cap V_2) \end{cases}$$

This has to be done for every subset intersection one wants to include in the restrictions of the problem. Every new intersection means a new auxiliary participant. Remember that the number of constraints and the number of variables are exponential on the number of participants, so these operations increase quite a lot the computational cost of the program.

This technique was used in [29] by Carles Padró, Leonor Vàzquez and An Yang to improve some of the bounds given by Jackson and Martin in [23]. In particular, they could improve the bounds on the following access structures: Γ_{73}, Γ_{80}, Γ_{82}, Γ_{83}, Γ_{86}, Γ_{88}, Γ_{89}, Γ_{150}, Γ_{152}, and Γ_{153}. For these access structures, it has been possible to find better bounds for some of the ones in Table 4.1, but only for $\sigma(\Gamma)$ and not for $\widetilde{\sigma}(\Gamma)$. For the rest of the access structures, no better lower bounds have been obtained. However, it has been found some secret sharing scheme on Γ that has the lower bound as information ratio for each of the remaining access structures, which means that upper and lower bound are the same and the optimum value for $\sigma(\Gamma)$ has been found. In conclusion the optimal information ratio of Γ_{80}, Γ_{82}, Γ_{83}, Γ_{86}, Γ_{88}, Γ_{89} has been found. Some other results have been found for $\widetilde{\sigma}(\Gamma)$. For access structures Γ_{73}, Γ_{152} and Γ_{153} the optimal information ratio has been found. It has been checked that: $\widetilde{\sigma}(\Gamma_{73}) = \widetilde{\sigma}(\Gamma_{153}) = 3/2$ and $\widetilde{\sigma}(\Gamma_{152}) = 7/5$.

Furthermore, for the still open access structures, the technique explained before has been used. This approach results in linear secret sharing schemes and hence, lower bounds on $\lambda(\Gamma)$. In Table 4.2, one can find the updated results (lower bounds) that have been found by using this technique, that is, by including additional variables in the programs in order to consider subset intersections.

Table 4.1: Updated bounds on $\sigma(\Gamma)$ of open access structures with 5 participants

Access structure	σ from [23]	σ from [29]	$\widetilde{\sigma}$ from [29]	updated LB for σ
$\Gamma_{73} \cong \Gamma^*_{151}$	$[3/2, 5/3]$	$3/2$	$[3/2, 8/5]$	$14/9$
$\Gamma_{150} \cong \Gamma^*_{40}$	$[3/2, 12/7]$	$3/2$	$7/5$	No improvement
$\Gamma_{152} \cong \Gamma^*_{53}$	$[3/2, 5/3]$	$3/2$	$[3/2, 8/5]$	$14/9$
$\Gamma_{153} \cong \Gamma^*_{30}$	$[3/2, 5/3]$	$3/2$	$[7/5, 8/5]$	No improvement

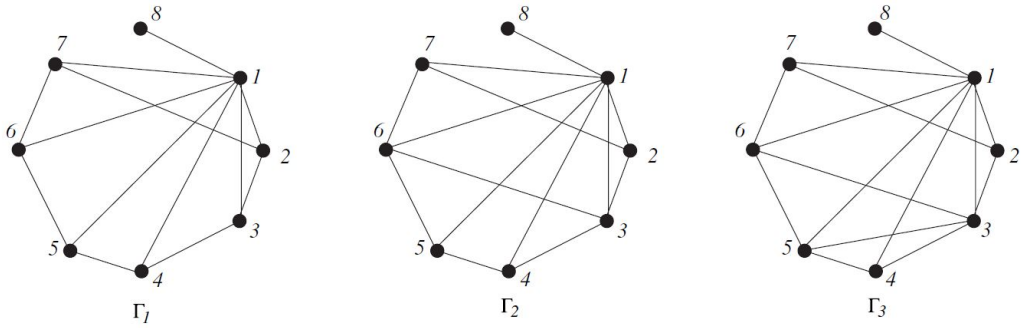

Figure 4.2: Graph access structures on 8 participants with $\kappa(\Gamma) < \lambda(\Gamma)$.

Table 4.2: Updated bounds on $\lambda(\Gamma)$ of open access structures with 5 participants

Access structure	σ from [23]	σ from [29]	$\widetilde{\sigma}$ from [29]	LB λ with LP	LB $\widetilde{\lambda}$ with LP
$\Gamma_{73} \cong \Gamma^*_{151}$	$[3/2, 5/3]$	$3/2$	$[3/2, 8/5]$	$5/3$	$23/15$
$\Gamma_{150} \cong \Gamma^*_{40}$	$[3/2, 12/7]$	$3/2$	$7/5$	$5/3$	No improvement
$\Gamma_{152} \cong \Gamma^*_{53}$	$[3/2, 5/3]$	$3/2$	$[3/2, 8/5]$	$5/3$	No improvement
$\Gamma_{153} \cong \Gamma^*_{30}$	$[3/2, 5/3]$	$3/2$	$[7/5, 8/5]$	$5/3$	No improvement

All of the explained before can make one think that the bounds for $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$ given by the bounds obtained for $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ are tight. But, in general, they are not. In fact, some access structures have been found with $\kappa(\Gamma) < \sigma(\Gamma)$ or with $\kappa(\Gamma) < \lambda(\Gamma)$. The bounds for these particular access structures can be improved by effectively adding some rank or information inequalities that cannot be derived from Shannon information inequalities. For example in [29], the three graph based access structures on 8 participants in Fig 4.2 were studied. By adding the Ingleton inequality (using the technique of the subset intersection explained before) to the aforementioned linear programs, bounds on $\lambda(\Gamma)$ were found. Carles Padró, Leonor Vázquez and An Yang found out that the bound for $\lambda(\Gamma) > \kappa(\Gamma)$, which means that $\kappa(\Gamma) < \lambda(\Gamma)$ for those three access structures. In particular, they obtained $\lambda(\Gamma_1) \geq 19/10$ and $\lambda(\Gamma_2), \lambda(\Gamma_3) \geq 13/7$, while $\kappa(\Gamma_1) = 11/6$ and $\kappa(\Gamma_2) = \kappa(\Gamma_3) = 9/5$.

Chapter 5

Access structures based on graphs

Finally, as it was presented in the Introduction chapter, access structures on 6 participants based on graphs are going to be considered. The aim of this chapter is to check the lower bounds given by Van Dijk [15] for 112 graph-based access structures by using the same linear programs explained so far. In fact, he calculated lower bounds for the optimal information ratio, and not or the average optimal information ratio. So, bounds on $\widetilde{\sigma}(\Gamma)$ are going to be calculated as well.

The same approach is followed when calculating these bounds on graph-based access structures as the one that has been explained in the chapter before. Basically, Shannon information inequalities will be used in order to check the existing bounds and calculate the new ones. In the following table, one can find the results obtained for both $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$ for all the graph based access structures presented by Van Dijk [15].

Table 5.1: Lower bounds obtained with LP for $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$

Nr.	σ from [15]	σ LP	$\widetilde{\sigma}$ LP	**Nr**	σ from [15]	σ LP	$\widetilde{\sigma}$ LP
1	1	1	1	**57**	3/2	3/2	3/2
2	3/2	3/2	7/6	**58**	3/2	3/2	4/3
3	3/2	3/2	7/6	**59****	3/2	3/2	3/2
4	5/3	5/3	4/3	**60**	3/2	3/2	3/2
5	3/2	3/2	7/6	**61**	5/3	7/4*	3/2
6	3/2	3/2	4/3	**62****	3/2	3/2	4/3
7	3/2	3/2	7/6	**63**	3/2	3/2	7/6
8	3/2	3/2	5/4	**64**	3/2	3/2	7/6
9	5/3	7/4*	11/8	**65**	3/2	3/2	4/3
10	5/3	5/3	4/3	**66**	1	1	1
11	3/2	3/2	7/6	**67**	3/2	3/2	4/3
12	3/2	3/2	4/3	**68**	3/2	3/2	3/2
13	5/3	5/3	4/3	**69**	3/2	3/2	7/6
14	5/3	5/3	4/3	**70****	3/2	3/2	4/3
15	3/2	3/2	7/6	**71****	3/2	3/2	4/3
16	3/2	3/2	4/3	**72**	3/2	3/2	4/3
17	3/2	3/2	7/6	**73**	3/2	3/2	4/3
18	5/3	5/3	3/2	**74**	3/2	3/2	4/3
19	3/2	3/2	3/2	**75****	3/2	3/2	3/2

Table 5.1: Lower bounds obtained with LP for $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$

Nr.	σ from [15]	σ LP	$\widetilde{\sigma}$ LP	**Nr**	σ from [15]	σ LP	$\widetilde{\sigma}$ LP
20	3/2	3/2	7/6	**76**	3/2	3/2	3/2
21	3/2	3/2	4/3	**77****	3/2	3/2	3/2
22	5/3	7/4*	4/3	**78**	3/2	3/2	3/2
23	3/2	3/2	7/6	**79**	3/2	3/2	3/2
24	5/3	5/3	4/3	**80**	1	1	1
25	5/3	5/3	4/3	**81**	3/2	3/2	7/6
26	5/3	5/3	4/3	**82**	3/2	3/2	7/6
27	3/2	3/2	7/6	**83**	3/2	3/2	4/3
28	3/2	3/2	7/6	**84****	3/2	3/2	17/12
29	5/3	5/3	4/3	**85**	3/2	3/2	4/3
30	3/2	3/2	7/6	**86**	3/2	3/2	4/3
31	5/3	5/3	3/2	**87**	3/2	3/2	4/3
32	3/2	3/2	7/6	**88**	3/2	3/2	4/3
33	3/2	3/2	4/3	**89**	3/2	3/2	4/3
34	3/2	3/2	7/6	**90**	3/2	3/2	3/2
35	3/2	3/2	4/3	**91****	3/2	3/2	3/2
36	3/2	3/2	4/3	**92**	3/2	3/2	4/3
37**	3/2	3/2	3/2	**93****	3/2	3/2	3/2
38	3/2	3/2	3/2	**94**	3/2	3/2	4/3
39	3/2	3/2	7/6	**95**	3/2	3/2	7/6
40	5/3	7/4*	4/3	**96**	3/2	3/2	4/3
41	3/2	3/2	7/6	**97**	3/2	3/2	4/3
42	5/3	7/4*	3/2	**98**	3/2	3/2	4/3
43	5/3	7/4*	3/2	**99**	3/2	3/2	4/3
44	3/2	3/2	7/6	**100**	1	1	1
45	3/2	3/2	7/6	**101**	3/2	3/2	3/2
46**	3/2	3/2	4/3	**102**	3/2	3/2	3/2
47	3/2	3/2	4/3	**103**	3/2	3/2	3/2
48	5/3	5/3	3/2	**104**	3/2	3/2	4/3
49	3/2	3/2	4/3	**105**	1	1	1
50	3/2	3/2	7/6	**106**	3/2	3/2	3/2
51	3/2	3/2	4/3	**107**	3/2	3/2	4/3
52	1	1	1	**108**	1	1	1
53	3/2	3/2	3/2	**109**	3/2	3/2	4/3
54	3/2	3/2	4/3	**110**	1	1	1
55**	3/2	3/2	4/3	**111**	1	1	1
56	3/2	3/2	7/6	**112**	1	1	1

The bounds that have been updated with respect to the ones given by Van Dijk [15] are marked with a *. These bounds were actually found in [29] and, as the same linear programs have been used, one can see that the same bounds have been updated with the same values. Open access structures are highlighted with **. Those are the access structures for which new bounds are being looked for. In fact, from those access structures three have been closed: It has been determined

that $\sigma(\Gamma_{37}) = \sigma(\Gamma_{46}) = \sigma(\Gamma_{62}) = 3/2$. This means that the value of the optimal information ratio is achieved and these access structures are closed. The bounds for the rest of the open access structures are trying to be updated by using some non-Shannon information inequalities. Remember that the technique explained before is being used, and hence only bounds on $\lambda(\Gamma)$ will be achieved. Some results have been found lately and can be found in Table 5.2. However, the access structures on that table are still open and the same technique will be applied with newer constraints in the search for better bounds. Probably, the information ratio of all of these access structure on a small number of participants will be effectively calculated in a near future.

Table 5.2: Lower bounds obtained with LP for $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$

Nr.	σ from [15]	λ LP	**Nr**	σ from [15]	λ LP
55	3/2	8/5	**77**	3/2	8/5
59	3/2	8/5	**84**	3/2	8/5
70	3/2	8/5	**91**	3/2	8/5
71	3/2	8/5	**93**	3/2	8/5
75	3/2	8/5			

Bibliography

[1] Rabin, M.O. Randomized Byzantine generals. *Proc. of the 24th IEEE Symp. on Foundations of Computer Science.* (1983) 403—409

[2] Nadi Bozkurt, İ. Function and Secret Sharing Scheme extensions for Blakley and Asmuth-Bloom Secret Sharing Schemes (2009) https://pdfs.semanticscholar.org/0869/4a5cc13bd72e3d12a1ae55599925ecbfda98.pdf

[3] Desmedt, Y.G., Frankel, Y. Shared generation of authenticators and signatures. *Feigenbaum, J. (ed.) CRYPTO 1991 LNCS* **576** Springer, Heidelberg (1992) 457—469.

[4] Naor, M., Wool, A. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems* **9(1)** (1998) 909—922

[5] Goyal, V., Pandey, O., Sahai, A., Waters, B. Attribute-based encryption for fine grained access control of encrypted data. *Proc. of the 13th ACM Conference on Computer and Communications Security* (2006) 89—98

[6] Chaum, D., Crépeau, C., Damgard, I. Multiparty unconditionally secure protocols. *Proc. of the 20th ACM Symp. on the Theory of Computing* (1988) 11-–19

[7] Cramer, R., Damgard, I.B., Maurer, U.M. General secure multi-party computation from any linear secret-sharing scheme. *Preneel, B. (ed.) EUROCRYPT 2000. LNCS* **1807** Springer, Heidelberg (2000) 316-–334.

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

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

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

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

[13] Csirmaz, L. An impossibility result on graph secret sharing. *Designs, Codes and Cryptography* **53** (2009) 195–209.

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

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

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

[17] Capocelli, R.M., De Santis, A. Gargano, L., Vaccaro, U. On the Size of Shares for Secret Sharing Schemes *J. Cryptology 6* (1993) 157–167

[18] Dougherty, R., Freiling, C., Zeger, K. Six new non-Shannon information inequalities. In *ISIT 2006.* (2006) 233–236.

[19] Farràs, O., Metcalf-Burton, J.R., Padró, C. and Vázquez, L. On the optimization of bipartite secret sharing schemes. *In Proceedings of the 4th international conference on Information theoretic security (ICITS'09)*, (2009) 93–109.

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

[21] Ingleton, A. W. Conditions for representability and transversability of matroids. In *Proc. Fr. Br. Conf 1970.* (1971) 27–62.

[22] Brickell, E.F. Some ideal secret sharing schemes. Journal of Combinatorial Mathematics and Combinatorial Computing **9** (1989) 105—113.

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

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

[25] Martí-Farré, J., Padró, C. On Secret Sharing Schemes, Matroids and Polymatroids. *Journal of Mathematical Cryptography* **4** (2010) 95–120.

[26] Matúš, F. Piecewise linear conditional information inequality. On *IEEE Trans. Inform. Theory.* **44**(2006) 236–238.

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

[28] Matúš, F. Infinitely many information inequalities. *IEEE International Symposium on Information Theory 2007*, pp. 41–44, 2007.

[29] Padró, C., Vàzquez, L., Yang, A. Finding lower bounds on the complexity of secret sharing schemes by linear programming *Discrete Applied Mathematics* **161** (2016)

[30] Beimel, A., Orlov, I. Secret Sharing and Non-Shannon Information Inequalities *IEEE Trans. Inform. Theory* **57** (2011) 5634–5649

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

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

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

[34] Van Dijk, M. On the information rate of perfect secret sharing schemes *Designs, Codes and Cryptography* **6** (1995) 143—169.

[35] Yeung, R. *A First Course in Information Theory*. Kluwer Academic/Plenum Publishers (2002).

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

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

[38] Martín, S., Padró, C., Yang, A. Secret Sharing, Rank Inequalities, and Information inequalites *IEEE Trans. Inform. Theory* **62**, 599–603 (2016) http://eprint.iacr.org/2013/082

[39] Michael Trick's Operations Research Page *Carnegie Mellon University* http://mat.gsia.cmu.edu/classes/QUANT/NOTES/chap7.pdf

[40] Jones, J. *Richland Community College* https://people.richland.edu/james/ictcm/2006/simplex.html