Secret sharing schemes and polymatroids

Yang, An

2014

Yang, A. (2014). Secret sharing schemes and polymatroids. Doctoral thesis, Nanyang Technological University, Singapore.

https://hdl.handle.net/10356/59108

https://doi.org/10.32657/10356/59108

NANYANG
TECHNOLOGICAL
UNIVERSITY

SECRET SHARING SCHEMES AND POLYMATROIDS

YANG AN
SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

2014

SECRET SHARING SCHEMES AND POLYMATROIDS
YANG AN
2014

Secret Sharing Schemes And Polymatroids

YANG AN

School Of Physical And Mathematical Sciences

A thesis submitted to Nanyang Technological University
in fulfillment of the requirement for the degree of
Doctor of Philosophy in Mathematical Sciences

2014

Acknowledgement

I am deeply grateful to my supervisors Prof Xing Chaoping and Prof Carles Padró for their constant guidance and support during my research. Warm thanks to Prof Xing for his devoted supervision, and for everything I learned from him. Xing brought me to the world of advanced mathematics and let me know how a researcher is working. I learned from him not only methods of solving problems, but also the way of a mathematician thinking. And a million thanks to Prof Padró for his unreserved help and I always enjoyed listening to his brightened and perceptive overview, discussing and exploring with him. His words often enlightened me and excited me. I enjoyed being their student.

I would thank many colleagues, from whom I gained a lot. Especially to to-be-Dr Ma Liming, and thanks for the fact that I could always consult with him, to bother him, and dinner with him.

Thanks to all my co-authors who collaborated with me during this research: Dr Oriol Farràs, Dr Leonor Váquez, Prof Sebastià Martín, Dr Ignacio Cascudo Pueyo and Prof Ronald Cramer. I enjoyed working with them all.

Finally, thanks to my boyfriend Chen Qitian for accompanying aside during my hard time and giving me vital moral support. And also thanks to my parents for all their help and support.

List of Works

Below is the list of works done during my PhD studies in NTU.

1. Oriol Farràs, Carles Padró, Chaoping Xing, An Yang. *Natural Generalizations of Threshold Secret Sharing*. IEEE Transactions on Information Theory (TIT) 60 (2014) 1652–1664.

2. Carles Padró, Leonor Váquez, An Yang. *Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming*. Discrete Applied Mathematics 161 (2013) 1072-1084.

3. Sebastià Martín, Carles Padró, An Yang. *Secret Sharing, Rank Inequalities and Information Inequalities*. Advances in Cryptology - CRYPTO 2013, 277–288.

4. Ignacio Cascudo Pueyo, Ronald Cramer, Chaoping Xing, An Yang. *Asymptotic Bound for Multiplication Complexity in the Extensions of Small Finite Fields*. IEEE Transactions on Information Theory (TIT) 58 (2012) 4930-4935.

Contributions

This thesis mainly contributes to the area of secret sharing and focuses on two main problems in secret sharing: the characterization of the ideal access structures and the optimization of the length of the shares. It covers the results from all the publications except the last one, since my main work during PhD studies focuses on secret sharing. Every chapter includes results from one of our papers according to the order of the above list, but the content is well-organized and written as a whole.

In Chapter 3, we present some novel and useful families of ideal multipartite access structures. They are among the most natural generalization of threshold access structures. We notice that the previous proposals of ideal multipartite secret sharing schemes are associated to families of relatively simple integer polymatroids that are obtained from Boolean polymatroids. By this clue new families of multipartite access structures are discovered. They are ideal, linear and described by a small number of parameters. Moreover, the representation of those access structures over large enough finite fields are guaranteed, as a result, constructing ideal multipartite secret sharing schemes for them are possible. Actually, in the last section of Chapter 3 we abstract a unified framework to construct ideal linear secret sharing schemes based on the result from [41], and from this framework, previous works are highly explicit.

In Chapter 4 information ratios in particular access structures are studied. Namely, we generalize a way by linear programming to determine the lower bounds of information ratio for any access structure with small number of participants. This method gives the best lower bounds by using polymatroids and information inequalities. In the same way, two other examples of non-ideal access structures induced from non-representable matroids are found. Although this method is powerful, lower bounds are not tight, while two examples in the last section of Chapter 4 explain this well.

In Chapter 5 the asymptotic information ratio is studied. This topic is at a standstill after Ito, Saito, Nishizeki [55] and Benaloh, Leichter [13] gave upper bounds, and Csirmaz [30] gave a lower bound. Recently Beimel and Orlov [10] gave a negative result, namely, information inequalities on four and five variables known up to date can only help to improve lower bounds of information ratio for general access structures at most linear on the number of participants. We generalize Beimel and Orlov's result in Chapter 5 to all information inequalities derived from one or two common informations. On the other hand, we prove that all information inequalities on a bounded number of variables only can provide lower bounds that are polynomial on the number of participants. Our two negative results are not constrained to known information inequalities, and provide a better understanding on the limitations of the use of those inequalities in secret sharing.

Contents

Abstract

Secret sharing, which refers to methods of distributing a secret value among a group of participants, is a very important primitive in cryptology. This thesis contains some contribution to this topic. The results that are presented herein deal with two of the main open problems in secret sharing: the characterization of the ideal access structures and the optimization of the length of the shares.

For both open problems, polymatroids are a powerful tool. On one hand, ideal multipartite secret sharing schemes are strongly connected to polymatroids. On the other hand, the entropies of shares of a scheme determine a polymatroid, and because of that, they are fundamental in the search of lower bounds of the length of the shares.

For the first open problem, some new and useful families of ideal multipartite access structures are found by using integer polymatroids. As a result the proofs for the existence of ideal secret sharing schemes for them are simplified in great measure. Regarding the second open problem, we present positive and negative results about the only known technique to find lower bounds: linear programming. The positive result are obtained by strengthening this method. The negative ones show the limitation of this method trying to improve the asymptotic lower bounds.

Chapter 1

Introduction

1.1 Overview

With the wide use of Internet, too many illogical passwords are challenging your memory. Obviously, it is not safe to write all them down. One easy way to store those passwords is to separate them to pieces and save every piece in a different file. In such a way, you are using the idea of secret sharing. *Secret sharing* refers to a method of distributing a secret to shares among a set of *participants* in such a way that only *qualified subsets* of participants can recover the secret. The collection of qualified subsets are called *access structure*. The aim of secret sharing schemes is to keep highly sensitive information confidential and reliable. Reliability comes from the pool of qualified subsets which allows recovery of the secret even if several shares are lost.

Secret sharing is one of the most important primitives in cryptography. The natural use of secret sharing, and the one for which it was invented, is to safely store cryptographic keys. Moreover, a number of much less obvious applications of secret sharing to different kinds of cryptographic protocols have appeared, such as Byzantine agreement [76], secure multiparty computation [14, 26, 34], generalized oblivious transfer [83, 91] and so on. Arguably, secure multiparty computation is the most remarkable application of secret sharing, while secret sharing is an essential building block for secure multiparty computation. A large-scale and practical application of multi-party computation took place in Denmark in January 2008, which is described in [21] as ”Secure Multiparty Computation Goes Live”.

The first proposed secret sharing schemes by Blakley [16] and Shamir [82] in 1979 have *threshold* access structure, that is, the qualified subsets are those having at least a certain number of participants. Both constructions are *unconditionally secure*, that is, their security is independent from the computational power of the adversary. In addition, they are *perfect*, in the sense that unqualified subsets cannot get any information about the secret.

Moreover, both Shamir’s and Blakley’s schemes are efficient, since the complexity of secret distribution and reconstruction algorithms are polynomial on the number of participants. In contrast, for general access structures, efficiency is far to be attained. Ito, Saito and Nishizeki [55] proved that there exists a secret sharing scheme for every access structure, but the schemes are very inefficient because the length of the shares grows exponential on the number of participants. Csirmaz [30] gave a lower bound $\Omega(n/\log n)$ on the length of shares where n is the number of participants. There is a huge gap between the best known lower and upper bounds. Actually, the optimization of secret sharing schemes for general access structures has appeared to be an extremely difficult problem and not much is known about it.

Nevertheless, this does not mean that efficient secret sharing schemes exist only for threshold access structures. Actually, constructions of efficient secret sharing schemes have drawn a lot of attention, especially *ideal* secret sharing schemes, in which the share of every participant has the same length as the secret. Due to the seminal work by Brickell and Davenport [23], ideal secret sharing schemes are strongly connected with *matroids*. One important and outstanding open problem is to characterize *ideal access structures*, the ones admitting ideal secret sharing schemes.

In the study of secret sharing, miscellaneous tools are employed from mathematics, information theory and computer science. We list here several important tools involved in the exploration. Shannon entropy function, a measure of uncertainty in information theory is used to define secret sharing schemes. As a result, information inequalities should be satisfied by secret sharing schemes. Linear programming is generally used to find the optimal solution of lengths of shares. Matroids and polymatroids, well-studied combinatorial objects are widely used.

Many fruitful results in secret sharing schemes have appeared. However, many open problems in this field are far from solved. In this thesis, we discuss the open problems mentioned above mainly employing a powerful tool: *polymatroids*. Polymatroids are a generalization of matroids. Fujishige [45, 46] pointed out that we can get a polymatroid by assigning entropy function to subsets of a finite set of random variables. Csirmaz [30] proved that the entropies of the secret and shares of a secret sharing scheme determine a polymatroid.

Polymatroids have been used to find bounds on the (average) *information ratio* of secret sharing schemes [10, 30, 63, 68], which is the ratio of the maximum (or average) length of the shares to the length of the secret. Martí-Farré and Padró [63] generalized and gave a better understanding of combinatorial methods of finding bounds on information ratio both for secret sharing schemes and linear schemes. Farràs, Martí-Farré and Padró [41] firstly used *integer polymatroids* to characterize *ideal multipartite access structures*, which means that the participants are divided into several parts and the participants in the same part play an equivalent role. They gave a necessary and a (different) sufficient conditions for a multipartite access structure to be ideal, which can be seen as an extension of the result by Brickell and Davenport [23].

This thesis continues to explore the bond between secret sharing schemes and polymatroids. It contributes to the solutions of those open problems on secret sharing schemes and provides some enlightening ideas and directions. A sketch of our contributions will be presented in the end of this chapter.

1.2 Secret Sharing Schemes

In a secret sharing scheme, we have a set of participants P and shares are distributed to all participants in P. Only the subsets of participants in the access structure can use their shares to recover the key. Every access structure is monotone increasing, that is, every superset of a qualified subset is also qualified. Then an access structure is completely determined by the family of its *minimal* *qualified subsets*. In this thesis we only study unconditionally secure perfect secret sharing schemes.

The first proposed family of secret sharing schemes is the (t, n)–*threshold secret sharing* by Shamir [82] and Blakley [16], where t is the threshold and n is the number of participants, $0 < t \leq n$. While the construction by Shamir [82] is based on polynomial interpolation, the one by Blakley [16] uses finite geometries.

A simple example is when $t = n$, and the case is trivial. To construct this scheme, we can give every participant a random share over a finite field and let the secret key be the sum of all the shares. Clearly, this defines a perfect secret sharing scheme in which a set of all n participants P is the only qualified set. And obviously, the length of every share has the same length of the secret, which also gives an example of an ideal secret sharing scheme.

It was noticed by Bloom [17] and by Karnin, Greene and Hellman [59] that Shamir's and Blakley's constructions are *linear*, which implies that both the computation of the shares and the reconstruction of the secret can be performed by using basic linear algebra operations. Linear secret sharing schemes have homomorphic properties that are very interesting for cryptographic applications. Moreover, due to the linearity, the computation of the shares and the reconstruction of the secret in a linear secret sharing scheme are efficient. Linear schemes have been also called geometric schemes [56, 87], or monotone span programs [58].

Secret sharing schemes for non-threshold access structures were first considered in the seminal paper by Shamir [82], where weighted threshold secret sharing schemes were introduced. However, the information ratio of this scheme depends on the maximum weight, which is at least 2. In 1987, Ito, Saito and Nishizeki [55] proved, in a constructive way, that there exists a secret sharing scheme for every access structure. Subsequently, Benaloh and Leichter [13] improve the construction, but in both constructions the length of shares is exponential on the number of participants.

So it is worthwhile to construct efficient secret sharing schemes. The constructions of ideal and linear schemes for non-threshold access structures has attracted a lot of attention.

1.2.1 Ideal secret sharing schemes

The pioneer and remarkable work on characterizing ideal secret sharing schemes is by Brickell [22] and by Brickell, Davenport [23]. They give a tight connection between ideal secret sharing schemes and matroids. Namely, every linear representation of a matroid defines an ideal secret sharing scheme [22] and every ideal secret sharing scheme determines a matroid [23]. Even though Brickell and Davenport did not use the term *matroid port*, their result can be represented as the connection between ideal access structures and matroid port, that is, the access structure of every ideal secret sharing is a matroid port; the ports of representable matroids are ideal access structures. Actually, matroid ports were introduced by Lehman [61] in 1964 to solve the Shannon switching game before the invention of secret sharing schemes. But the introduction of matroid port allows direct research on access structures induced by matroids.

As seen, the necessary condition for a secret sharing scheme to be ideal is not sufficient and the sufficient condition is not necessary. Seymour [81] gave the first example, Vámos matroid which does not admit any ideal secret sharing scheme. Matúš [67] presented an infinite family of such matroids. On the other direction, Simonis and Ashikhmin [86] firstly proved that non-Pappus matroid admits an ideal secret sharing scheme but not representable.

The actual methods of constructing ideal secret sharing schemes were considered. Many studies are dedicated to explore new constructions of particular access structures or some families of ideal access structures. Threshold secret sharing schemes are the first such constructions [16,82]. Subsequently, Kothari [60] posed the open problem of constructing ideal linear secret sharing schemes with hierarchical properties. Simmons [87] introduced the *multilevel* and *compartmented* access structures, and presented geometric constructions of ideal linear secret sharing schemes for some of them. The multilevel and compartmented access structures are *multipartite*, which is a natural generalization of threshold access structure, particularly, allowing numerical expansion of one part and also different relation between parts.

The first multipartite scheme is weighted threshold schemes by Shamir [82], but it is not ideal. Brickell [22] firstly proposed methods to construct ideal hierarchical and compartmented schemes, which can be seen as a generalization of Shamir's threshold schemes [82]. Moreover, Tassa [90] and Tassa and Dyn [92] gave probabilistic algorithms to construct ideal hierarchical and compartmented schemes. Particular cases for hierarchical schemes are studied in [11,49].

Based on results by Brickell [22] and Brickell, Davenport [23], an advanced result was presented by Farràs, Martí-Farré and Padró in [41]. They introduced integer polymatroids to study ideal multipartite secret sharing schemes. Necessary and sufficient conditions for multipartite secret sharing schemes to be ideal are presented, while multipartite matroid port is defined. The power of this new mathematical tool was demonstrated in the same work by using it to characterize the ideal tripartite access structures. Subsequently, the use of integer polymatroids made it possible to characterize the ideal hierarchical access structure [43].

1.3 Efficiency in secret sharing

When constructing secret sharing schemes, several efficiency issues should be taken into account:

1. The computational complexity of the distributing and reconstructing algorithms. The computation time should be polynomial in the number of participants;

2. The size of the secret value. Sometimes, sharing a short secret value is required, but some constructions of secret sharing schemes only work for sufficiently large secret values. In the case of linear secret sharing schemes, the problem is determining over which finite fields a scheme can be constructed.

3. The information ratio. For perfect secret sharing schemes, the smallest possible information ratio is 1, which is attained by the ideal schemes. But most access structures do not admit an ideal scheme, and these cases, we try to minimize the information ratio.

All these considerations matter from the point of practicability of scheme constructions. Among them, information ratio received much attention. Specifically, trying to determine the optimal information ratio of every given access structure or, at least, to find lower and upper bounds on this parameter.

This is a very difficult open problem, and there is a huge gap between the best known lower and upper bounds of general access structures. The length of the shares in the known constructions for general access structures is exponential in the number of participants. The general opinion among the researchers in the area is that this is unavoidable. Specifically, the following conjecture, which was formalized by Beimel [5], is generally believed to be true. It poses one of the main open problems in secret sharing, surely the most difficult and intriguing one.

Conjecture 1.3.1. *There exists an $\epsilon > 0$ such that for every integer n there is an access structure on n participants, for which every secret sharing scheme distributes shares of length $2^{\epsilon n}$, that is, exponential in the number of participants.*

Nevertheless, not many results supporting this conjecture have been proved. No proof for the existence of access structures requiring shares of superpolynomial size has been found. Moreover, the best of the known lower bounds is the one given by Csirmaz [30], who presented a family of access structures on an arbitrary number n of participants that require shares of size $\Omega(n/\log n)$ times the size of the secret. On the negative side, Csirmaz [30] proved that by only using Shannon information inequalities one cannot prove a lower bound of $O(n)$ on the share size. And recently Beimel and Orlov [10] showed that all the information inequalities up to date can only improve the lower bound at linearity.

Due to the difficulty of finding general results, information ratio on particular cases are studied in [19, 31–33, 35, 37, 56]. Given a secret sharing scheme Σ, we denote $\sigma(\Sigma)$ as the information ratio of secret sharing scheme Σ. If an access structure Γ is given, the optimal information ratio of Γ, $\sigma(\Gamma)$ is defined as the infimum of $\sigma(\Sigma)$ for all the secret sharing schemes Σ admitting Γ.

A way to determine σ is to find lower bounds and upper bounds of σ and once they meet, the value of σ is settled. Two more parameters are introduced: κ and λ, while κ is the ratio value when access structure and Shannon basic inequalities are satisfied, and λ is the information ratio of linear secret sharing schemes. Naturally, the value of κ can be seen as the lower bound of σ, and the upper bound of λ as the upper bound of σ. Csirmaz proved that κ is less or equal to the number of participants [30]. By using linear programming in our work [75], the value of κ can be determined, but constrained to the complexity of linear programming, this method for access structures on large number of participants will not work. In [56], most of σ for 5 participants are determined while lower and upper bounds meet.

1.4 Contributions

In this section we summarize our main results of this thesis. Results on ideal secret sharing are presented in Chapter 3, and results on information ratio of secret sharing schemes in Chapter 4 and 5.

In Chapter 3 we present several new and useful families of ideal multipartite access structures, which are natural generalizations of hierarchical and compartmented access structures in previous works. Namely, they admit an ideal linear secret sharing schemes over every large enough finite field, they can be described by a small number of parameters, and they have useful properties for the applications of secret sharing. While no strong connection between all those families was previously known, a remarkable common feature is made apparent by identifying the integer polymatroids that are associated to those ideal multipartite access structures. Namely, they are Boolean polymatroids or basic transformations and combinations of Boolean polymatroids. The use of integer polymatroids, especially Boolean polymatroids and uniform polymatroids, makes it possible to find many new such families and it simplifies in great measure the proofs for the existence of ideal secret sharing schemes for them. Some of the results in this chapter appeared previously in Dr. Farràs' PhD thesis, specifically, the ones in Subsection 3.4.1 about *compartmented access structures with upper and lower bounds*. The other results are contributions of this thesis. Namely, more new families of multipartite access structures are presented in this thesis and moreover, we analyze the efficiency of previous constructions of ideal multipartite secret sharing schemes in a unified framework stated in [41], which gives a uniform scope of efficiency of constructions of ideal multipartite secret sharing schemes.

On the other hand, based on the definition of secret sharing schemes by polymatroids and the representation of information inequalities and rank inequalities by polymatroids, the computation of bounds of information ratio can be quantified.

In Chapter 4 we employ linear programming to give a general way to determine the best lower bounds of information ratio of any given access structure by using combinatorial methods. By applying this linear programming approach, we give some examples of better lower bounds on the optimal information ratio and the optimal average information ratio of several access structures. In particular, Jackson and Martin [57] determined the optimal (average) information ratio of all access structures on five participants except a few ones, for which upper and lower bounds were given. By our method, most of the lower bounds are improved for unsolved cases, and some of optimal average information ratio are settled down. Van Dijk [35] listed all 112 non-isomorphic graph access structures on six vertices and combined several combinatorial methods to determine the information ratio of them. We determine 5 cases among 18 unsolved ones. And by adding the Ingleton inequalities to the previous linear programming approach, we present some access structures for which there is a gap between the optimal information ratio and the combinatorial lower bound of linear secret sharing schemes. Some of the results in this chapter were previously showed in Dr. Vázquez's PhD thesis. In this thesis, further explorations by using that linear programming method have been carried out. For instance, in Section 4.5, lower bounds on information ratio of (linear) secret sharing schemes for the access structures induced by non-representable matroids are presented. However, the lower bounds we can get by linear programming are not tight in all cases or even not able to reach. This is proved by the negative result in Section 4.6, which is also a contribution of this thesis. We give an impossibility result that there do not exist linear secret sharing schemes with the best lower bound of complexity known until now.

In Chapter 5 we deal with Conjecture 1.3.1, that is, we study asymptotic behavior of information ratio. We show the limitation of improving lower bound by non-Shannon inequalities under the method of linear programming. Csirmaz published his result on lower bound $\Omega(n/\log n)$ [30], and he also gave that information inequalities can at most improve this bound to $O(n)$, while only *Shannon basic inequalities* were known at that time. Up to now, infinite non-Shannon inequalities are discovered. It looks that it is a good chance to improve lower bound, however, we prove negative results that those inequalities only help to improve at most linearly on the number of participants. In particular, Beimel and Orlov [10] proved that all information inequalities on four or five variables, together with all information inequalities on more than five variables that are known to date, provide lower bounds on the size of the shares in secret sharing schemes that are at most linear on the number of participants. We present here another negative result about the power of information inequalities in the search for lower bounds in secret sharing. Namely, we prove that all information inequalities on a bounded number of variables only can provide lower bounds that are polynomial on the number of participants. And the proof is quite simple by using a special Boolean and uniform polymatroid. Moreover, we prove that a family of inequalities derived from one or two common informations cannot provide lower bounds that are better than cubic on the number of participants. This family of inequalities at least includes all information inequalities on four and five participants [39]. In addition, our proof does not require computer explorations and more importantly, it provides an explanation to the limitations of non-Shannon information inequalities, and hence we shed some light on the search of better asymptotic lower bounds.

Chapter 2

Preliminaries

In this chapter we will give some background on secret sharing schemes and tools we use through the context.

2.1 Basics on Information Theory

Before giving the definition of secret sharing, we need to introduce some basic concepts of information theory, which will be used to give one definition of secret sharing and also involved in the next discussion frequently. Readers who are not familiar with this subject can refer to [29, 93].

Let S be a discrete random variable on a finite set E and $p(s) = \Pr(S = s)$ be the probability of $S = s, s \in E$.

Definition 2.1.1. *The* Shannon entropy *or shortly* entropy *of S is*

$$H(S) = -\sum_{s \in E} p(s) \log p(s)$$

where the logarithm is binary and we take $p(s)\log p(s) = 0$ *if* $p(s) = 0$*.*

In information theory, the entropy function measures uncertainty of a random variable and it can be proved that $0 \leq H(S) \leq \log|E|$. The upper bound $\log|E|$ is attained if and only if S is uniform on E and the lower bound is attained if and only if S is deterministic.

Let Λ be a finite index set and $(S_i)_{i\in\Lambda}$ be a tuple of random variables. The *joint random variables* $(S_i)_{i\in X}$ is denoted by S_X for any $X \subseteq \Lambda$, which has a joint probability distribution on $\prod_{i\subseteq X} E_i$. For two random variables S_1 and S_2 on $\mathcal{S}_1$ and $\mathcal{S}_2$ respectively, similarly we have the entropy of (S_1, S_2):

$$H(S_1S_2) = -\sum_{(s_1,s_2)\in E_1\times E_2} p(s_1, s_2)\log p(s_1, s_2).$$

Definition 2.1.2 (Shannon's Information Measures). *Let* S_1, S_2 *and* S_3 *be random variables on* E_1, E_2 *and* E_3 *respectively. The* conditional entropy of S_1 given S_3 *is defined as*

$$H(S_1|S_3) = H(S_1S_3) - H(S_3).$$

The mutual information between S_1 and S_2 *is defined as*

$$I(S_1; S_2) = H(S_1) - H(S_1|S_2).$$

And the conditional mutual information between S_1 and S_2 given S_3 *is defined as*

$$I(S_1; S_2|S_3) = H(S_1|S_3) - H(S_1|S_2S_3).$$

Notice that, S_1 and S_2 are symmetric in the formulas above, that is, $I(S_1; S_2) = I(S_2; S_1)$ and $I(S_1; S_2|S_3) = I(S_2; S_1|S_3)$. In addition, the conditional entropy and mutual information are special cases of conditional mutual information , i.e. $I(S_1; S_2|S_3) = H(S_1|S_3)$ if $S_1 = S_2$, and $I(S_1; S_2|S_3) = I(S_1; S_2)$ if S_3 is a degenerate random variable (i.e., S_3 takes a constant value). Thus, the following proposition, the proof of which can be found in [93, Theorem 2.34], tell us all Shannon's information measures are nonnegative.

Proposition 2.1.3. *(Shannon's basic inequality [84]) For the conditional mutual information between S_1 and S_2 given S_3, the following inequality always holds.*

$$I(S_1; S_2|S_3) \geq 0 \tag{2.1.1}$$

2.2 Information Inequalities and Rank Inequalities

Definition 2.2.1. *Let Λ be a finite index set. An* information inequality *is defined as a tuple $\{\alpha_X\}_{X \subseteq \Lambda}$ of real numbers such that the inequality*

$$\sum_{X \subseteq \Lambda} \alpha_X H(S_X) \geq 0$$

holds for every collection of random variables $\{S_i\}_{i \in \Lambda}$.

For example, the inequality 2.1.1, which can be expressed as $H(S_1S_3) + H(S_2S_3) - H(S_3) - H(S_1S_2S_3) \geq 0$, is an information inequality. The inequalities derived from 2.1.1, that is, the non-negative linear combination of Shannon's basic inequalities, are called *Shannon inequalities*, and all the information inequalities that cannot derive from 2.1.1 are called *non-Shannon inequalities*. It is known that all information inequalities involving three or fewer random variables are Shannon inequalities [93]. The first non-Shannon inequality was discovered by Zhang and Yeung [95] in 1998, and it is the following one:

$$\begin{aligned} &3H(S_1S_2)+3H(S_1S_3)+3H(S_2S_3)+H(S_2S_4)+H(S_3S_4)-H(S_1)-2H(S_2) \\ &-2H(S_3)-H(S_1S_4)-4H(S_1S_2S_3)-H(S_2S_3S_4)\geq 0 \end{aligned} \tag{2.2.1}$$

Afterwards, many other non-Shannon inequalities have been found, for example, in [38, 40, 62, 69]. Matúš [69] found an infinite number of independent non-Shannon inequalities over four random variables and [40] expanded the list.

Next we will introduce rank inequalities, which deal with configurations of vector subspaces. The connection with information inequalities is described next.

Let V be a vector space over a field $\mathbb{F}$, and $\{V_i\}_{i\in\Lambda}$ be finite-dimensional subspaces of V, where Λ is a finite index set. The sum of subspaces $\sum_{i\in Y} V_i$ is denoted by V_Y for any $Y\subseteq\Lambda$.

Definition 2.2.2. *Let Λ be a finite index set. A* rank inequality *is defined as a tuple $\{\beta_Y\}_{Y\subseteq\Lambda}$ of real numbers such that the inequality*

$$\sum_{Y\subseteq\Lambda}\beta_Y\dim(V_Y)\geq 0$$

holds for every collection of vector subspaces $\{V_i\}_{i\in\Lambda}$ of a vector space V with finite dimension.

The inequality below is a rank inequality.

$$\dim(V_X) + \dim(V_Y) \geq \dim(V_{X\cup Y}) + \dim(V_{X\cap Y}),\ X, Y \subseteq \Lambda.$$

Dougherty, Freing and Zeger pointed out in [39] that, Rado [77] proved that every representable matroid can be represented over a finite field, and hence any configuration of finite-dimensional vector spaces over any field has a corresponding configuration over some finite field. So $\{\beta_Y\}_{Y\subseteq\Lambda}$ is a rank inequality if this is satisfied for finite fields.

Proposition 2.2.3. *Every information inequality is a rank inequality.*

Proof. Let $\mathbb{F}$ be a finite field and V be a $\mathbb{F}$-vector space with finite dimension. And let V^* be the dual space of V, which is formed by all linear function $\theta\colon V \to \mathbb{F}$. Claim that every subspace of V can be turned into a random variable. Consider a random variable S given by the uniform probability distribution on V^*. Clearly, $H(S) = \dim(V) \cdot \log|\mathbb{F}|$. For any subspace $V_i \subset V, i \in \Lambda$, consider the linear random variable associated to the subspace V_i, is $Y_i = Y|_{V_i}$, the restriction of Y to V_i. The joint random variable $S_Y = (S_i)_{i\in Y} = S|_{(V_i)_{i\in Y}}$ for any $Y \subseteq I$. We have $H(S_Y) = \dim(V_Y) \cdot \log|\mathbb{F}|$, where $V_Y = \sum_{i\in Y} V_i$. So we can rewrite the information inequality 2.2.1 in dimensions up to a factor $\log|\mathbb{F}|$:

$$\sum_{Y\subseteq\Lambda} \alpha_Y \dim(V_Y) \geq 0.$$

This means that all information inequalities are rank inequalities. □

However, the converse is not true. There exist rank inequalities which are not information inequalities, and the first such example is the well-known Ingleton inequality [54]:

$$\begin{aligned}
&\dim(V_1+V_2)+\dim(V_1+V_3)+\dim(V_1+V_4)+\dim(V_2+V_3)\\
&+\dim(V_2+V_4)-\dim(V_1)-\dim(V_2)-\dim(V_3+V_4)\\
&-\dim(V_1+V_2+V_3)-\dim(V_1+V_2+V_4)\geq 0
\end{aligned}$$

As a consequence, every collection of four random variables satisfies

$$\begin{aligned}
&H(S_1S_2)+H(S_1S_3)+H(S_1S_4)+H(S_2S_3)+H(S_2S_4)\\
&-H(S_1)-H(S_2)-H(S_3S_4)-H(S_1S_2S_3)-H(S_1S_2S_4)\geq 0 \qquad (2.2.2)
\end{aligned}$$

But there exist non-linear random variables that do not satisfy 2.2.2.

Hammer et al. [50] also showed that all rank inequalities on 4 random variables can be derived from Shannon inequalities and Ingleton inequality together. And Dougherty, Freiling, and Zeger [39] gave a list of 24 inequalities, which together with all 4-variables inequalities, generate all rank inequalities on five variables. However for $r > 5$, to find all rank inequalities on r random variables is still an open problem.

2.3 Polymatroids and Matroids

Let Q be a finite set and $(S_x)_{x\in Q}$ be a family of random variables. Consider the entropy function on $(S_x)_{x\in Q}$ with $H(\emptyset)=0$, which has the following properties.

- $H(\emptyset) = 0$
- Monotonicity: $H(S_X|S_Y) \geq 0$, then $H(S_X S_Y) - H(S_Y) = H(S_X) - H(S_Y) \geq 0$ when $Y \subseteq X$
- Submodularity: To prove the entropy function is submodular, we only need to show $H(S_X S_Z) + H(S_Y S_Z) \geq H(S_X S_Y S_Z) + H(S_Z)$ with any disjoint subsets X, Y, Z. Observe that this inequality is just $I(S_X; S_Y|S_Z) \geq 0$.

These are called *polymatroids axioms*. Any function satisfying all three polymatroids axioms defines a polymatroid.

Definition 2.3.1. *A* polymatroid $\mathcal{S}$ *is a pair* (Q, f) *formed by a finite set* Q*, the* ground set*, and a* rank function $f : \mathcal{P}(Q) \to \mathbb{R}$ *satisfying*

1. $f(\emptyset) = 0$*, and*
2. f *is* monotone increasing*: if* $X \subseteq Y \subseteq Q$*, then* $f(X) \leq f(Y)$*, and*
3. f *is* submodular*: if* $X, Y \subseteq Q$*, then* $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y)$*.*

If the rank function f is integer-valued, we say that $\mathcal{S}$ is an *integer polymatroid*. An integer polymatroid such that $f(X) \leq |X|$ for every $X \subseteq Q$ is a *matroid*.

Consider a matroid $\mathcal{M} = (Q, r)$. The *independent sets* of $\mathcal{M}$ are the subsets $A \subseteq Q$ with $r(A) = |A|$, and the sets that are not independent are called *dependent*. A *basis* is a maximal independent set and a *circuit* is a minimal dependent set. A matroid is said to be *connected* if, for any two elements in Q, there is at least one circuit containing them.

Since a matroid can be uniquely determined by its independent sets, bases or circuits, alternative definitions of matroids are possible. In the following we give a definition of matroids by bases.

Definition 2.3.2. *A family $\mathcal{B} \subseteq \mathcal{P}(Q)$ is the family of bases of a matroid with ground set Q if and only if $\mathcal{B}$ is nonempty and the following* exchange condition *is satisfied.*

- *For every $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, there exists $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\}$ is in $\mathcal{B}$.*

From the exchange condition, a useful property is derived, that is, all the bases of a matroid have the same number of elements, which is the *rank of* $\mathcal{M}$, denoted by $r(\mathcal{M})$. Actually, $r(\mathcal{M}) = r(Q)$.

Next we introduce poly-entropic polymatroids and poly-linear polymatroids. Fujishige [45,46] firstly found that these axioms are equivalent to Shannon's basic inequality (in Proposition 2.1.3), so we have the following theorem.

Theorem 2.3.3. *Let $(S_x)_{x \in Q}$ be a family of random variables. Consider the mapping $h : \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(X) = H(S_X)$ if $\emptyset \neq X \subseteq Q$. Then h is the rank function of a polymatroid with ground set Q.*

Any polymatroid defined in such a way is called an *entropic* polymatroid. A *poly-entropic* polymatroid is a multiple of an entropic polymatroid. Since poly-entropic polymatroids are defined by entropy function, all information inequalities are satisfied. If $(\alpha_A)_{A \subseteq Q}$ defines an information inequality, then we have $\sum_{A \subseteq Q} \alpha_A h(A) \geq 0$.

Definition 2.3.4. *A polymatroid $\mathcal{S} = (Q, f)$ is said to be* linear *or* $\mathbb{K}$-representable *if there is a vector space V and a finite collection of subspaces $(V_i)_{i \in Q}$ over a finite field $\mathbb{K}$*

and $f(X) = \dim(V_X)$ *for any* $X \subseteq Q$*. A* poly-linear *polymatroid is a multiple of a linear polymatroid.*

Since a linear polymatroid is defined over a vector space, rank inequalities must be satisfied by this polymatroid. We have the following proposition about poly-entropic polymatroids and poly-linear polymatroids, and the proof can be derived similarly to the analysis that every information inequality is a rank inequality.

Proposition 2.3.5. *Every linear polymatroid is a poly-entropic polymatroid.*

But the converse is not true. Ingleton inequality is a rank inequality, and it is not always true for entropic polymatroids. See Theorem 4 in [50] as a counterexample.

If every V_i is spanned by at most one vector, then $f(\{i\}) \leq 1, i \in Q$, and f is a rank function of a $\mathbb{K}$-representable matroid. In the next example we will use Zhang and Yeung inequality(2.2.1) to prove Vámos matroid is not poly-entropic, and not poly-linear or representable either according to Proposition 2.3.5.

Example 2.3.6. *Vámos matroid is defined on the set* $V = \{v_1, v_2, \ldots, v_8\}$*. Its independent sets are all the sets of cardinality not more than 4, but except* $\{v_1, v_2, v_3, v_4\}$*,* $\{v_1, v_2, v_5, v_6\}$*,* $\{v_3, v_4, v_5, v_6\}$*,* $\{v_3, v_4, v_7, v_8\}$ *and* $\{v_5, v_6, v_7, v_8\}$*. This is the smallest matroid which is not representable over any field [73].*

Proof. Set $X_1 = \{v_1, v_2\}, X_2 = \{v_3, v_4\}, X_3 = \{v_5, v_6\}$ and $X_4 = \{v_7, v_8\}$. Let f be a rank function on V. We will prove that this polymatroid does not satisfy Zhang and Yeung inequality 2.2.1.

$$
\begin{aligned}
&3f(X_1X_2)+3f(X_1X_3)+3f(X_2X_3)+f(X_2X_4)+f(X_3X_4)-f(X_1)-2f(X_2)\\
&-2f(X_3)-f(X_1X_4)-4f(X_1X_2X_3)-f(X_2X_3X_4)\\
&=3*3+3*3+3*3+3+3-2-2*2-2*2-4-4*4-4=-1<0
\end{aligned}
$$

□

A detailed presentation about polymatroids can be found in [79, Chapter 44] or [52]. The following characterization of rank functions of polymatroids is a straightforward consequence of [79, Theorem 44.1]. Since the rank function can totally determine the polymatroid, this proposition can also be viewed as another definition of polymatroid.

Proposition 2.3.7. *A map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if the following properties are satisfied.*

- $f(\emptyset)=0$.
- *If $X \subseteq Q$ and $y \in Q$, then $f(X) \le f(X \cup \{y\})$.*
- *If $X \subseteq Q$ and $y,z \in Q$, then $f(X\cup\{y,z\})+f(X) \le f(X\cup\{y\})+f(X\cup\{z\})$.*

Duality

The *dual of a matroid* $\mathcal{M}=(Q,r)$ is a matroid $\mathcal{M}^*=(Q,r^*)$ with

$$r^*(X)=|X|-r(Q)+r(Q\setminus X), \text{ for any } X\subseteq Q.$$

Proposition 2.3.8. *Let $\mathcal{B}$ be the family of bases of the matroid $\mathcal{M}$, then $\mathcal{B}^* = \{Q \setminus B \colon B \in \mathcal{B}\}$ is the family of bases of the dual matroid $\mathcal{M}^*$.*

The proof of this proposition can be found in [73] naturally by using exchange condition. As discussed before, a matroid can uniquely determined by its bases and so it is easy to get $\mathcal{M}^{**} = \mathcal{M}$.

Example 2.3.9. *Consider the uniform matroid $U_{r,m}$ whose bases are size r subsets of Q with size m. By Proposition 2.3.8, we have $U^*_{r,m} = U_{m-r,m}$.*

Similar to matroids, the *dual of a polymatroid* $\mathcal{S} = (Q, f)$ is defined as $\mathcal{S}^* = (Q, f^*)$ with

$$f^*(X) = \sum_{x \in X} f(\{x\}) - f(Q) + f(Q \setminus X), \text{ for any } X \subseteq Q.$$

Proposition 2.3.10. *If $\mathcal{S} = (Q, f)$ is a polymatroid, then its dual $\mathcal{S}^* = (Q, f^*)$ is also a polymatroid.*

Proof. According to the definition of dual polymatroid, it is easy to check all three conditions for polymatroids.

1. $f^*(\emptyset) = -f(Q) + f(Q) = 0$

2. If $Y \subseteq X \subseteq Q$, then $f^*(X) - f^*(Y) = \sum_{x \in X - Y} f(\{x\}) + f(Q \setminus X) - f(Q \setminus Y) \geq f(X \setminus Y) + f(Q \setminus X) - f(Q \setminus Y) \geq 0$

3. For any $X, Y \subseteq Q$, $f^*(X) + f^*(Y) - f^*(X \cup Y) - f^*(X \cap Y) = f(Q \setminus X) + f(Q \setminus Y) - f(Q \setminus (X \cup Y)) - f(Q \setminus (X \cap Y)) \geq 0$.

This completes the proof. □

2.3.1 Boolean Polymatroids and Uniform Polymatroids

Next we will introduce two important types of integer polymatroids, Boolean and uniform polymatroids, which are both representable and have nice form.

Boolean polymatroids are very simple integer polymatroids that are representable over every finite field. Consider a finite set B and a family $(B_i)_{i \in Q}$ of subsets of B. Clearly, the map $f(X) = |\bigcup_{i \in X} B_i|$ for $X \subseteq Q$ is the rank function of an integer polymatroid $\mathcal{S}$ with ground set Q. A *Boolean polymatroid* is an integer polymatroid that can be defined in this way. Boolean polymatroids are representable over every field $\mathbb{K}$. If $|B| = r$, we can assume that B is a basis of the vector space $V = \mathbb{K}^r$. For every $i \in Q$, consider the vector subspace $V_i = \langle B_i \rangle$. Obviously, these subspaces form a $\mathbb{K}$-representation of $\mathcal{S}$. The *modular polymatroids* are those having a *modular rank function*, that is, $f(X \cup Y) + f(X \cap Y) = f(X) + f(Y)$ for every $X, Y \subseteq Q$. Every integer modular polymatroid is Boolean, and hence it is representable over every finite field. A Boolean polymatroid is modular if and only if the sets $(B_i)_{i \in Q}$ are disjoint. Observe that the rank function of an integer modular polymatroid is of the form $f(X) = \sum_{i \in X} b_i$ for some vector $b \in \mathbb{Z}_+^Q$.

We say that a polymatroid $\mathcal{S}$ with ground set Q is *uniform* if every permutation on Q is an automorphism of $\mathcal{S}$. In this situation, the rank $h(X)$ of a set $X \subseteq Q$ depends only on its cardinality, that is, there exist values $0 = h_0 \leq h_1 \leq \cdots \leq h_m$, where $m = |Q|$, such that $f(X) = f_i$ for every $X \subseteq Q$ with $|X| = i$. It is easy to see that such a sequence of values f_i defines a uniform polymatroid if and only if $f_i - f_{i-1} \geq f_{i+1} - f_i$ for every $i = 1, 2, \ldots, m-1$. Clearly, a uniform polymatroid is univocally determined by its *increment vector* $\delta = (\delta_1, \ldots, \delta_m)$, where $\delta_i = f_i - f_{i-1}$. Observe that $\delta \in \mathbb{R}^m$ is the increment vector of a uniform polymatroid if and only if $\delta_1 \geq \cdots \geq \delta_m \geq 0$. A uniform polymatroid is a matroid if and only if $\delta_i \in \{0, 1\}$ for every $i = 1, 2, \ldots, m$. In this case, we obtain the *uniform matroid* $U_{r,m}$, where $r = \max\{i : \delta_i = 1,\ 1 \leq i \leq m\}$. It is well known that $U_{r,m}$ is $\mathbb{K}$-representable whenever $|\mathbb{K}| \geq m$.

2.4 Secret Sharing Schemes

In this section we will give the definition and some classic examples of secret sharing schemes. Readers who are not familiar with secret sharing can refer to a survey [5] for an overview. As mentioned in the introduction, we just consider unconditionally secure perfect secret sharing schemes.

Let P be a finite set of participants, and $p_0 \notin P$ be the *dealer* who distributes the shares. And let $Q = P \cup \{p_0\}$ and these notations are generally used henceforth in this thesis.

We will first give a combinatorial description of secret sharing schemes and then we introduce a formal definition of secret sharing schemes based on Shannon entropies.

We take $P = \{1, 2, \ldots, n\}$ and $p_0 = 0$. 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

$\pi_i \colon E \to E_i$. A *secret sharing scheme* Σ on Q is a mapping $\Pi = (\pi_i)_{i \in Q}$:

$$\begin{array}{rcc} \Pi : E & \to & E_0 \times E_1 \times \cdots \times E_n \\ x & \mapsto & (\pi_0(x), \pi_1(x), \ldots, \pi_n(x)) \end{array}$$

such that

(i) there exist $x, y \in E$ with $\Pr(x),\ \Pr(y) > 0$ and $\pi_0(x) \neq \pi_0(y)$

(ii) for any two distinct elements $x, y \in E$, if $(\pi_1(x), \ldots, \pi_n(x)) = (\pi_1(y), \ldots, \pi_n(y))$, then $\pi_0(x) = \pi_0(y)$

Here $\pi_0(x) \in E_0$ is the *secret key* and $\pi_i(x) \in E_i$ is the *share* for participant i, $1 \leq i \leq n$. According to probability theory, E with its underlying probability function defines a probability space, and so is $E_0 \times E_1 \times \cdots \times E_n$ with the probability distribution induced by Π. Thus every map π_i naturally derives a random variable, denoted by $S_i, 0 \leq i \leq n$. Given $x \in E$, let $\pi_i(x) = s_i$ for $0 \leq i \leq n$. Then the tuple $(s_0, s_1, \ldots, s_n) \in E_0 \times E_1 \times \cdots \times E_n$ satisfies

$$\Pr[S_0 = s_0, S_1 = s_1, \ldots, S_n = s_n] > 0$$

and

$$\Pr[S_0 = s_0 | S_1 = s_1, \ldots, S_n = s_n] = 1.$$

The *access structure* Γ of a secret sharing scheme Σ can be described as

$$\Gamma = \{A \subseteq P\ : \text{there exists an } s_0 \in E_0 \text{ such that} \Pr[S_0 = s_0 | S_i = s_i, i \in A] = 1\}.$$

Since we study perfect secret sharing schemes, for every set $B \subseteq P$ that is not in Γ, we have $\Pr[S_0 = s_0 | S_i = s_i, i \in B] = \Pr[S_0 = s_0]$ for every $s_0 \in E_0$.

Example 2.4.1 (Shamir Secret Sharing [82]). *A (t,n)-threshold access structure is defined as*

$$\Gamma = \{A \subseteq P \colon |A| \geq t\}.$$

In [82], Shamir constructed a secret sharing scheme by using polynomials for this Γ and we restate the construction here.

Let $\mathbb{K}$ be a finite field with at least $n+1$ elements. Take $E = \mathbb{K}_{t-1}[x]$, all the polynomials over $\mathbb{K}$ with degree at most $t-1$, and $E_i = \mathbb{K}$ for every $i \in Q$. The dealer picks a tuple $(x_i)_{i \in Q}$ of distinct elements in $\mathbb{K}$ and then the scheme is

$$\Sigma \colon f \to (f(x_i))_{i \in Q}.$$

In this scheme $f(x_0)$ is the secret and $f(x_i)$ is the share for participant $i \in P$.

For a collection of random variables $\{S_i\}_{i \in Q}$ we introduce a function $h(\cdot)$ to define secret sharing scheme such that $h(A) = H(S_A)$ and $h(A|B) = H(S_A|S_B)$ for every $A, B \subseteq Q$. This notation will be used through this thesis since its clear connection with polymatroids.

Definition 2.4.2. *Let P be a finite set and $Q = P \cup \{p_0\}$. A* secret sharing scheme Σ *is a collection $(S_i)_{i \in Q}$ of discrete random variables such that $h(\{p_0\}) > 0$ and $h(\{p_0\}|P) = 0$. The* access structure Γ *is defined as $\Gamma = \{A \subseteq P : h(\{p_0\}|A) = 0\}$.*

If the subset $B \subseteq P$ is not in Γ, we have $h(\{p_0\}|B) = h(\{p_0\})$ which implies that the set of participants, that is not qualified, can get no information about secret.

This fact corresponds with the requirement of perfect secret sharing schemes. The access structures are monotone increasing since every superset of a qualified set is qualified. Thus every access structure is fully determined by the minimal qualified sets, denoted by $\min \Gamma$.

An access structure is *connected* if each participant is at least in one minimal qualified set. Only connected access structures are studied here. We say a secret sharing scheme is *connected* if it realizes a connected access structure. Karnin, Greene and Hellman [59] have showed that $h(\{i\}) \geq h(\{p_0\})$, that is, the information ratio of any connected and perfect secret sharing scheme is at least 1.

On the other hand, from the definition of secret sharing schemes and Theorem 2.3.3, we can easily get that entropies of secret and shares of a secret sharing scheme form a polymatroid.

Next we will give a definition of linear secret sharing schemes based on the definition of secret sharing scheme.

Definition 2.4.3. *For a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$, it is* linear *if all the random variables S_i, $i \in Q$ are linear on some finite field.*

Dual of access structures

Next we introduce the concepts of dual of an access structure. The *dual of an access structure* Γ on P is defined as $\Gamma^* = \{A \subseteq P \colon P \setminus A \notin \Gamma\}$. It is clear that the dual of a connected access structure is connected as well.

Proposition 2.4.4. $\Gamma = \Gamma^{**}$.

Proof. This proposition is directly derived from $\Gamma^* = \overline{\Gamma^c}$, where Γ^c is the complement of Γ on P, and $\overline{\Gamma^c}$ is the complement of Γ^c on $\mathcal{P}(P)$. □

Example 2.4.5. *Suppose $P = \{1,2,3,4,5\}$ and*

$$\min \Gamma = \{\{1,2\},\{1,3\},\{2,3,4\},\{2,3,5\},\{1,4,5\}\}.$$

According to the definition of dual of Γ,

$$\min \Gamma^* = \{\{1,2\},\{1,3\},\{2,3,4\},\{2,3,5\},\{1,4,5\}\}.$$

Since an access structure is determined by its minimal set, we have $\Gamma = \Gamma^*$. It is called self-dual *if $\Gamma = \Gamma^*$ under a permutation on P. For this example, no permutation is needed.*

2.5 Polymatroids and Secret Sharing

In this section we mainly introduce the connection between polymatroids and secret sharing schemes.

Refer to the connection between polymatroids and secret sharing schemes, the bond is more obvious as a result of Theorem 2.3.3. Every secret sharing scheme Σ with $\Gamma(\Sigma)$ defines a polymatroid $\mathcal{S} = (Q, h)$. And the access structure $\Gamma(\Sigma)$ can be written as

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

For a matroid $\mathcal{M} = (Q, r)$, define the *port* of the matroid $\mathcal{M}$ at point p_0 as

$$\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P \colon r(A \cup \{p_0\} = r(A))\}.$$

And in [23] Brickell and Davenport pointed out the connections between matroids ports and ideal access structures. The result is summarized in the following theorem.

Theorem 2.5.1 ([23]). *Any ports of representable matroids are ideal access structure; The access structure of ideal secret sharing scheme is a matroid port.*

For a general polymatroid $\mathcal{S} = (Q, f)$, we define Γ-polymatroid as 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 $p_0 \in Q$, the access structure on the set $P = Q \setminus \{p_0\}$, that is, $\Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P : f(A \cup \{p_0\}) = f(A)\}$, 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 $\Gamma = \Gamma_{p_0}(\mathcal{S})$.

Next we will give an important property, which is useful when we study the dual of secret sharing schemes.

Lemma 2.5.2. *Let Γ be an access structure on $P = Q \setminus \{p_0\}$ and $\mathcal{S} = (Q, f)$ be a Γ-polymatroid, then $\mathcal{S}^* = (Q, f^*)$ is a Γ^*-polymatroid. Moreover, $\Gamma(\mathcal{S}^*) = \Gamma(\mathcal{S})^*$.*

Proof. For every $X \subseteq P$,

$$f^*(X \cup \{p_0\}) = f(\{p_0\}) + \sum_{x \in X} f(\{x\}) - f(Q) + f(P \setminus X)$$

If $X \in \Gamma^*$, that is, $P - X \notin \Gamma$, then $f(Q \setminus X) = f(\{p_0\}) + f(P \setminus X)$. This means $f^*(X \cup \{p_0\}) = f^*(X)$. If $X \notin \Gamma^*$, that is, $P \setminus X \in \Gamma$, then $f(Q \setminus X) = f(P \setminus X)$. Thus, $f^*(X \cup \{p_0\}) = f(\{p_0\}) + f^*(X) = f^*(\{p_0\}) + f^*(X)$.

From the proof, it directly derives that $\Gamma(\mathcal{S}^*) = \Gamma(\mathcal{S})^*$. □

Given an access structure Γ, a polymatroid $\mathcal{S}_P = (P, f)$ is said to be *compatible with* Γ if there exists a Γ-polymatroid $\mathcal{S} = (Q, f)$ with $Q = P \cup \{p_0\}$ and $\mathcal{S}|_P = \mathcal{S}_P$. As noticed, every Γ-polymatroid $\mathcal{S} = (Q, h)$ has $h(\{p_0\}) = 1$. 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. Obviously, the associated polymatroid $\mathcal{S}(\Sigma) = (Q, f)$ is a Γ-polymatroid.

Proposition 2.5.3. *An access structure Γ on P is compatible with a polymatroid $\mathcal{S}_P = (P, f)$ if and only if the following conditions are satisfied.*

1. *If $X \subseteq P$ and $y \in P$ are such that $X \notin \Gamma$ and $X \cup \{y\} \in \Gamma$, then $f(X) \leq f(X \cup \{y\}) - 1$.*

2. *If $X \subseteq P$ and $y, z \in P$ are such that $X \notin \Gamma$ while both $X \cup \{y\}$ and $X \cup \{z\}$ are qualified, then $f(X \cup \{y, z\}) + f(X) \leq f(X \cup \{y\}) + f(X \cup \{z\}) - 1$.*

Proof. Suppose that $\mathcal{S}_P$ can be extended to a Γ-polymatroid $\mathcal{S}(\Gamma) = (Q, f)$. If $X \notin \Gamma$ and $X \cup \{y\} \in \Gamma$, then $f(X \cup \{y\}) \geq f(X \cup \{y, p_0\}) \geq f(X \cup \{p_0\}) = f(X) +$

1. If $X \notin \Gamma$ and $X \cup \{y\}$ and $X \cup \{z\}$ are qualified, then $f(X \cup \{y\}) + f(X \cup \{z\}) = f(X \cup \{y, p_0\}) + f(X \cup \{z, p_0\}) \geq f(X \cup \{y, z, p_0\}) + f(X \cup \{p_0\}) = f(X \cup \{y, z\}) + f(X) + 1$.

We prove now the converse. Assume that $\mathcal{S}_P = (P, f)$ satisfies the conditions in the statement and consider the extension $f : \mathcal{P}(Q) \to \mathbb{R}$ of f determined by $f(X \cup \{p_0\}) = f(X)$ if $X \in \Gamma$ and $f(X \cup \{p_0\}) = f(X) + 1$ otherwise. We have to prove that (Q, f) is a polymatroid. Clearly, $f(X) \leq f(X \cup \{p_0\})$ and $f(X \cup \{p_0\}) \leq f(X \cup \{p_0, y\})$ for every $X \subseteq P$ and $y \in P$. Therefore, the first condition in Proposition 2.3.7 is satisfied. Moreover, it is not difficult to prove that the second condition holds as well by checking that $f(X \cup \{y, p_0\}) + f(X) \leq f(X \cup \{y\}) + f(X \cup \{p_0\})$ and $f(X \cup \{p_0, y, z\}) + f(X \cup \{p_0\}) \leq f(X \cup \{p_0, y\}) + f(X \cup \{p_0, z\})$ for every $X \subseteq P$ and $y, z \in P$. □

As a consequence, the result by Csirmaz [30] in the following proposition can be got. Both propositions give a sufficient and necessary condition for a polymatroid that is compatible with a given access structure. Moreover, they are practical.

Proposition 2.5.4 ([30]). *A polymatroid $\mathcal{S}_P = (P, f)$ is compatible with an access structure Γ on P if and only if the following conditions are satisfied.*

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

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

2.5.1 Information ratio of secret sharing schemes

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 $n = |P|$. The *information ratio* or *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 information ratio* or *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. 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.

For every access structure Γ,

$$\sigma(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) : \mathcal{S} \text{ is a poly-entropic } \Gamma\text{-polymatroid}\} \tag{2.5.1}$$

and

$$\lambda(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) : \mathcal{S} \text{ is a poly-linear } \Gamma\text{-polymatroid}\}, \tag{2.5.2}$$

and the analogous properties apply to $\widetilde{\sigma}(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$. Obviously, $\sigma(\Gamma)$ is the infimum of information ratio of secret sharing schemes for given Γ.

If $\mathcal{S}$ is a poly-linear polymatroid, then the corresponding secret sharing scheme must be linear too. Thus, $\lambda(\Gamma)$ can be viewed as the infimum of the information ratio of linear secret sharing schemes for given Γ. At this point, we have $\lambda(\Gamma) \leq \sigma(\Gamma)$. However, a formal proof for this formula will present in the next theorem.

The parameter

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}, \tag{2.5.3}$$

which was introduced in [63], is a lower bound on the optimal complexity or information ratio. 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 $\widetilde{\kappa}(\Gamma)$, is defined analogously and it is a lower bound on the optimal average information ratio.

Theorem 2.5.5. *For a given access structure* Γ*, we have* $\kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$*.*

A generalized result of Theorem 2.5.1 is stated by Martí-Farré and Padró in [63], which gives a tighter criterion whether an access structure is a matroid port.

Theorem 2.5.6 ([63])**.** *An access structure* Γ *is a matroid port if* $\sigma(\Gamma) < 3/2$*.*

Some other results are given in [63], which will be used in Chapter 4. We present them here without proofs which can be found in [63] or [56].

Proposition 2.5.7. *Let* Γ *be an access structure and* Γ^* *be its dual, then* $\kappa(\Gamma) = \kappa(\Gamma^*)$*.*

This proof in [63] used Lemma 2.5.2. Besides this result, we also have $\lambda(\Gamma) = \lambda(\Gamma^*)$ because if there is a linear secret sharing scheme Σ with access structure Γ, then there exists a linear dual secret sharing scheme Σ^* for Γ^* with $\sigma(\Sigma) = \sigma(\Sigma^*)$ [56].

Chapter 3

New Families of Ideal Access Structures

3.1 Introduction

In this chapter, we will give some new and useful families of access structures, which are mainly included in our paper [44].

The Shamir secret sharing scheme presented in Example 2.4.1 is ideal and linear, in addition, the construction is efficient, that is, the distribution and reconstruction secrets algorithms are polynomial on the number of participants n. One problem pops up on efficiently constructing ideal linear secret sharing schemes for non-threshold access structures.

This line of research was initiated by Kothari [60], who presented some ideas to construct ideal linear secret sharing schemes with hierarchical properties. Simmons [87] introduced the multilevel and compartmented access structures, and presented geometric constructions of ideal linear secret sharing schemes for some of them. Brickell [22] formalized the ideas in previous works [17, 59, 60, 87] and introduced a powerful linear-algebraic method to construct ideal linear secret sharing schemes for non-threshold access structures. In addition, he used that method to construct such schemes for the families of access structures introduced by Simmons [87]. Tassa [90] and Tassa and Dyn [92] combined Brickell's [22] method with different kinds of polynomial interpolation to construct ideal linear secret sharing schemes for more general families of multilevel and compartmented access structures. Constructions for other interesting variants of compartmented access structures are given in [51, 72]. All these families of access structures have some common features that are enumerated in the following.

1. They are natural and useful generalizations of threshold access structures. In the threshold case, all participants are equivalent, while the access structures in those families are multipartite. In addition, they have some interesting properties for the applications of secret sharing. Some of them are useful for hierarchical organizations, while others can be used in situations requiring the agreement of several parties.

2. Similarly to the threshold ones, the access structures in those families admit a very compact description. Typically, they can be described by using a small number of parameters, at most linear on the number of parts.

3. They are ideal access structures. Actually, every one of those access structures admits a *vector space secret sharing scheme*, that is, an ideal linear secret sharing scheme constructed by using the method proposed by Brickell [22].

Moreover, the only restriction on the fields over which these schemes are constructed is their size, and hence there is no required condition about their characteristic. Observe that this is also the case for threshold access structures, which admit vector space secret sharing schemes over every finite field with at least as many elements as the number of participants.

4. Even though the existence of efficient ideal linear secret sharing schemes for those access structures has been proved, the known methods to construct such schemes are not efficient in general. This is an important difference to the threshold case, in which the construction proposed by Shamir [82] solves the problem. Exceptionally, Brickell [22] gave an algorithm for hierarchical threshold access structures that is efficient by using Shoup's algorithm [85] to compute a primitive polynomial over a finite field. Another efficient algorithm for the same class of access structures was presented by Tassa [90, Section 3.3]. Recently, efficient methods to construct ideal secret sharing schemes for some bipartite access structures have been given [4].

5. Determining the minimum size of the fields over which those schemes can be constructed is another open problem. It is unsolved even for threshold access structures, in which case the problem is equivalent to the main conjecture for maximum distance separable codes [3,53], or to determine over which fields uniform matroids are representable [73, Problem 6.5.12], or to determine the size of maximum arcs in projective spaces [80]. Much less is known for the general case. Differently to the threshold case, there is a huge gap between the known lower and upper bounds.

Two questions naturally arise at this point. The first one is the search for new families of access structures with the properties above. The second one is to determine the existence of efficient methods to construct ideal linear secret sharing schemes for them, and to find better bounds on the minimum size of the fields over which such schemes can be found.

Another related line of work deals with the characterization of the ideal access structures in several families of multipartite access structures. The bipartite access structures [74] and the weighted threshold access structures [12] were the first families for which such a characterization was given. Some partial results about the tripartite case were presented in [28, 51]. On the basis of the well known connection between ideal secret sharing schemes and matroids [23], integer polymatroids were introduced in [41] for the study ideal multipartite secret sharing schemes. The power of this new mathematical tool was demonstrated in the same work by using it to characterize the ideal tripartite access structures. Subsequently, the use of integer polymatroids made it possible to characterize the ideal hierarchical access structures [43].

This chapter is devoted to the search for new families of ideal access structures that are among the most natural generalizations of threshold secret sharing, and to the efficiency analysis of the methods to construct ideal secret sharing schemes for them.

Our results strongly rely on the connection between integer polymatroids and ideal multipartite secret sharing presented in [41], which is summarized here in Theorem 3.2.4. The concepts, notation and related facts that are required to understand this result are recalled Section 3.2. Actually, the use of this tool provides important advantages in comparison to the techniques applied in previous constructions of ideal multipartite secret sharing schemes [22, 51, 72, 74, 87, 90, 92].

While no strong connection between all those families was previously known, a remarkable common feature is made apparent by identifying the integer polymatroids that are associated to those ideal multipartite access structures. Namely, they are Boolean polymatroids or basic transformations and combinations of Boolean polymatroids. This is of course a useful clue when trying to find new families of ideal access structures satisfying the aforementioned requirements.

By using other Boolean polymatroids, and by combining them in several different ways, we present a number of new families of ideal multipartite access structures. Specifically, we present in Section 3.4 several generalizations of the compartmented access structures introduced in [22, 87, 92]. Section 3.5 deals with some families of partially hierarchical access structures that can be defined from Boolean polymatroids. For instance, we present a family of compartmented access structures in which every compartment has a hierarchy. Ideal (totally) hierarchical access structures, which were completely characterized in [43], are associated as well to a special class of Boolean polymatroids. Finally, we use another family of integer polymatroids, the uniform ones, to characterize in Section 3.6 the ideal members of another family of multipartite access structures: the ones that are invariant under every permutation of the parts.

All integer polymatroids that we use to find new families of ideal multipartite access structures can be defined by a small number of parameters, linear on the size of the ground set, and they are representable over every large enough finite field. Actually, these requirements are implied by the conditions we imposed on the access structures to be simple generalizations of threshold secret sharing. In Section 3.3 the basic integer polymatroids as well as the operations to modify and combine them that are used in our constructions. In particular, the result we prove in Proposition 3.3.5 is extremely useful.

We focus in this chapter on a few examples that can be useful for the applications of secret sharing, but many other families can be described by using other integer polymatroids with those properties, and surely some other useful families will be found in future works. For the sake of completeness, we give in Section 3.4.2 a detailed description of the process for constructing these schemes, and we illustrate it with an explicit example.

Differently from the aforementioned previous works, our proofs that the structures in these new families are ideal are extremely concise. Of course, this is due to the use of integer polymatroids. In addition, some easily checkable necessary conditions that are derived from the results in [41] make it possible to prove that certain given multipartite access structures are not ideal. An example of such a situation is given in Section 3.4.4. This simplifies as well the search for new families.

Even though the efficiency of the methods to construct actual ideal linear secret sharing schemes for those families of access structures has not been significantly improved by using the results from [41], they provide a unified framework in which the open problems related to that issue can be precisely stated. These open problems and some possible strategies to attack them are discussed in Section 3.7.

3.2 Multipartite Access Structures and Integer Polymatroids

3.2.1 Multipartite Access Structures and Their Representation

Here we recall the compact and useful representation of multipartite access structures that was introduced in [74] for the bipartite case.

We use $\mathbb{Z}_+$ to denote the set of the non-negative integers. For every $i, j \in \mathbb{Z}$ we write $[i,j] = \{i, i+1, \ldots, j\}$ if $i < j$, while $[i,i] = \{i\}$ and $[i,j] = \emptyset$ if $i > j$. For a positive integer m, we put $J'_m = [0,m]$ and $J_m = [1,m]$. Consider a finite set J. We notate J' for a set of the form $J' = J \cup \{j_0\}$ for some $j_0 \notin J$. For every two vectors $u = (u_i)_{i\in J}$ and $v = (v_i)_{i \in J}$ in $\mathbb{Z}^J$, the vector $w = u \vee v \in \mathbb{Z}^J$ is defined by $w_i = \max\{u_i, v_i\}$, while we put $w_i = \min\{u_i, v_i\}$ for $w = u \wedge v$. Given two vectors $u = (u_i)_{i\in J}$ and $v = (v_i)_{i\in J}$ in $\mathbb{Z}^J$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J$. The *modulus* $|u|$ of a vector $u \in \mathbb{Z}^J_+$ is defined by $|u| = \sum_{i\in J} u_i$. For every subset $X \subseteq J$, we notate $u(X) = (u_i)_{i\in X} \in \mathbb{Z}^X$. The *support of* $u \in \mathbb{Z}^J$ is defined as $\operatorname{supp}(u) = \{i \in J : u_i \neq 0\}$. Finally, we consider the vectors $\mathbf{e}^i \in \mathbb{Z}^J$ such that $\mathbf{e}^i_j = 1$ if $j = i$ and $\mathbf{e}^i_j = 0$ otherwise. A family $\Pi = (\Pi_i)_{i\in J}$ of subsets of P is called here a *partition of* P if $P = \bigcup_{i\in J} \Pi_i$ and $\Pi_i \cap \Pi_j = \emptyset$ whenever $i \neq j$. Observe that some of the parts may be empty. If $|J| = m$, we say that Π is an *m-partition* of P. For a partition Π of a set P, we consider the mapping $\Pi \colon \mathcal{P}(P) \to \mathbb{Z}^J_+$ defined by $\Pi(A) = (|A \cap \Pi_i|)_{i\in J}$. We write $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{u \in \mathbb{Z}^J_+ : u \leq (|\Pi_i|)_{i\in J}\}$. For a partition Π of a set P, a Π-*permutation* is a permutation σ on P such that $\sigma(\Pi_i) = \Pi_i$ for every part Π_i of Π. An access structure on P is said to be Π-*partite* if every Π-permutation is an automorphism of it. If the number of parts in Π is m, such an access structure is called *m-partite*.

A multipartite access structure can be described in a compact way by taking into account that its members are determined by the number of elements they have in each part. If an access structure Γ on P is Π-partite, then $A \in \Gamma$ if and only if $\Pi(A) \in \Pi(\Gamma)$. That is, Γ is completely determined by the partition Π and set of vectors $\Pi(\Gamma) \subseteq \mathbf{P} \subseteq \mathbb{Z}_+^J$. Moreover, the set $\Pi(\Gamma) \subseteq \mathbf{P}$ is monotone increasing, that is, if $u \in \Pi(\Gamma)$ and $v \in \mathbf{P}$ are such that $u \leq v$, then $v \in \Pi(\Gamma)$. Therefore, $\Pi(\Gamma)$ is univocally determined by $\min \Pi(\Gamma)$, the family of its minimal vectors, that is, those representing the minimal qualified subsets of Γ. By an abuse of notation, we will use Γ to denote both a Π-partite access structure on P and the corresponding set $\Pi(\Gamma)$ of points in $\mathbf{P}$, and the same applies to $\min \Gamma$.

Example 3.2.1. *For a bipartition $\Pi = (\Pi_1, \Pi_2)$ of the set P of participants, consider the access structure Γ formed by all subsets of P with at least 6 participants such that at least one of them is in Π_1, together with all subsets containing at least 4 participants from Π_1. This is obviously a Π-partite access structure. A vector $(u_1, u_2) \in \mathbf{P}$ is in $\Pi(\Gamma)$ if and only if $u_1 \geq 4$ or $|u| \geq 6$ and $u_1 \geq 1$. Therefore, $\min \Pi(\Gamma) = \{(1,5),(2,4),(3,3),(4,0)\} \cap \mathbf{P}$.*

Let $\mathcal{Z}$ be an integer polymatroid with ground set J. Consider the set $\mathcal{D}$ of the *integer independent vectors of $\mathcal{Z}$*, which is defined as

$$\mathcal{D} = \{u \in \mathbb{Z}_+^J \,:\, |u(X)| \leq h(X) \text{ for every } X \subseteq J\}.$$

Integer polymatroids can be characterized by its *integer bases*, which are the maximal integer independent vectors. A nonempty subset $\mathcal{B} \subseteq \mathbb{Z}_+^J$ is the family of integer bases of an integer polymatroid if and only if it satisfies the following *exchange condition*.

- For every $u \in \mathcal{B}$ and $v \in \mathcal{B}$ with $u_i > v_i$, there exists $j \in J$ such that $u_j < v_j$ and $u - \mathbf{e}^i + \mathbf{e}^j \in \mathcal{B}$.

In particular, all bases have the same modulus. Every integer polymatroid is univocally determined by the family of its integer bases. Indeed, the rank function of $\mathcal{Z}$ is determined by $h(X) = \max\{|u(X)| \,:\, u \in \mathcal{B}\}$.

Since only integer polymatroids and integer vectors will be considered, we will omit the term "integer" most of the times when dealing with the integer independent vectors or the integer bases of an integer polymatroid.

Example 3.2.2. *An integer polymatroid $\mathcal{Z} = (J, h)$ with ground set $J = \{1, 2\}$ is determined by the integer values $s = h(J)$ and $r_i = h(\{i\})$ for $i = 1, 2$. These triplets of integers are characterized by the inequalities $0 \le r_i \le s \le r_1 + r_2$. The family of independent vectors of such a polymatroid is formed by the vectors $u \in \mathbb{Z}_+^2$ such that $u \le (r_1, r_2)$ and $|u| \le s$. The basis are precisely the independent vectors with $|u| = s$. Every integer polymatroid with ground set $J = \{1, 2\}$ is representable over every field $\mathbb{K}$. Indeed, a representation is given by two subspaces $V_1, V_2 \subseteq \mathbb{K}^s$ such that* $\dim V_i = r_i$ *and $V_1 + V_2 = \mathbb{K}^s$.*

If $\mathcal{D}$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}$ on J, then, for every $X \subseteq J$, the set $\mathcal{D}|X = \{u(X) \,:\, u \in \mathcal{D}\} \subseteq \mathbb{Z}_+^X$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}|X$ with ground set X. Clearly, the rank function $h|X$ of this polymatroid satisfies $(h|X)(Y) = h(Y)$ for every $Y \subseteq X$.

Because of that, we will use the same symbol to denote both rank functions. Given two integer polymatroids $\mathcal{Z}$ and $\mathcal{Z}'$, we say that $\mathcal{Z}'$ is an *extension* of $\mathcal{Z}$ is $\mathcal{Z}'|X = \mathcal{Z}$ for some subset X of the ground set of $\mathcal{Z}'$.

For an integer polymatroid $\mathcal{Z}$ and a subset $X \subseteq J$ of the ground set, we write $\mathcal{B}(\mathcal{Z}, X)$ to denote the family of the independent vectors $u \in \mathcal{D}$ such that $\operatorname{supp}(u) \subseteq X$ and $|u| = h(X)$. Observe that there is a natural bijection between $\mathcal{B}(\mathcal{Z}, X)$ and the family of bases of the integer polymatroid $\mathcal{Z}|X$.

3.2.2 Integer Polymatroids and Multipartite Matroid Ports

The aim of this section is to summarize the results in [41] about ideal multipartite secret sharing schemes and their connection to integer polymatroids.

For a polymatroid $\mathcal{S}$ with ground set $J' = J \cup \{j_0\}$, the family

$$\Gamma_{j_0}(\mathcal{S}) = \{A \subseteq J \,:\, h(A \cup \{j_0\}) = h(A)\}$$

of subsets of J is monotone increasing, and hence it is an access structure on J. If $\mathcal{S}$ is a matroid, then the access structure $\Gamma_{j_0}(\mathcal{S})$ is called the *port of the matroid $\mathcal{S}$ at the point j_0*. As a consequence of the results by Brickell [22] and by Brickell and Davenport [23], matroid ports play a very important role in secret sharing. Specifically, the ports of representable matroids admit ideal secret sharing schemes [22] and the access structure of every ideal secret sharing scheme is a matroid port [23]. This latter result was generalized in [63] by proving that the access structure of a secret sharing scheme is a matroid port if the length of every share is less than 3/2 times the length of the secret. A detailed presentation of these results can be found in [88].

Brickell [22] provided a method to construct ideal schemes for ports of $\mathbb{K}$-representable matroids. These schemes are called a $\mathbb{K}$-*vector space secret sharing schemes*, and their access structures are $\mathbb{K}$-*vector space access structures*. In the following, we present this method as described by Massey [65,66] in terms of linear codes.

Consider a set P of n participants and $P' = P \cup \{p_0\}$ where $p_0 \notin P$ is considered as a special participant, usually called *dealer*. Let $\mathbb{K}$ be a finite field. Every $\mathbb{K}$-linear code C with length $n+1$ defines an ideal secret sharing scheme on P. Indeed, suppose that the entries of the codewords in C are indexed by the elements in P'. Then every random choice of a codeword $(c_x)_{x \in P'} \in C$ corresponds to a distribution of shares for the secret value $c_{p_0} \in \mathbb{K}$. Let M be a generator matrix of C, that is, a matrix over $\mathbb{K}$ whose rows span C. The columns of M, which are in one-to-one correspondence with the elements in P', determine a $\mathbb{K}$-representable matroid $\mathcal{M}$ with ground set P'. All generator matrices of C define the same matroid. A set $A \subseteq P$ is qualified if and only if the column of M corresponding to p_0 is a linear combination of the columns corresponding to the participants in A. Because of that, the access structure of the scheme is the matroid port of $\Gamma_{p_0}(\mathcal{M})$.

Given a partition $\Pi = (\Pi_i)_{i \in J}$ of the set P, consider $\Pi_{j_0} = \{p_0\}$ and the partition $\Pi' = (\Pi_i)_{i \in J'}$ of $P' = P \cup \{p_0\}$. Let $\mathcal{M}$ be a matroid with ground set P'. Then the matroid port $\Gamma_{p_0}(\mathcal{M})$ is Π-partite if and only if the matroid $\mathcal{M}$ is Π'-partite [41] (that is, every Π'-permutation is an automorphism of $\mathcal{M}$). In addition, every Π'-partite matroid $\mathcal{M}$ is associated to an integer polymatroid with ground set J' that, together with the partition Π', determines $\mathcal{M}$ [41]. A characterization of multipartite matroid ports in terms of integer polymatroids, which is given here in Theorem 3.2.4, is derived from these facts. An access structure is said to be *connected* if all participants are in at least one minimal qualified subset.

Definition 3.2.3. *Let $\Pi = (\Pi_i)_{i \in J}$ be a partition of a set P of participants. Consider an integer polymatroid $\mathcal{Z}'$ on J' with $h(\{j_0\}) = 1$ and $h(\{i\}) \leq |\Pi_i|$ for every $i \in J$, and take $\mathcal{Z} = \mathcal{Z}'|J$. We define a Π-partite access structure $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ in the following way: a vector $u \in \mathbf{P}$ is in $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ if and only if there exist a subset $X \in \Gamma_{j_0}(\mathcal{Z}')$ and a vector $v \in \mathcal{B}(\mathcal{Z}, X)$ such that $v \leq u$.*

Theorem 3.2.4 ([41]). *Let $\Pi = (\Pi_i)_{i \in J}$ be a partition of a set P. A Π-partite access structure Γ on P is a matroid port if and only if it is of the form $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ for some integer polymatroid $\mathcal{Z}'$ on J' with $h(\{j_0\}) = 1$ and $h(\{i\}) \leq |\Pi_i|$ for every $i \in J$. In addition, if $\mathcal{Z}'$ is $\mathbb{K}$-representable, then $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ is an $\mathbb{L}$-vector space access structure for every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$. Moreover, if Γ is connected, the integer polymatroid $\mathcal{Z}'$ is univocally determined by Γ.*

Example 3.2.5. *Let Γ be the Π-access structure defined in Example 3.2.1, with $(|\Pi_1|, |\Pi_2|) \geq (4, 5)$. By using Theorem 3.2.4, we show that Γ is ideal. Namely, we prove that it is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$. Consider $J = \{1, 2\}$ and the integer polymatroid $\mathcal{Z} = (J, h)$ described in Example 3.2.2 with $r_1 = 4$, $r_2 = 5$, and $s = 6$. Consider the only polymatroid $\mathcal{Z}' = (J', h)$ such that $\mathcal{Z}'|J = \mathcal{Z}$, and $h(\{j_0\}) = 1$, $h(\{j_0, 1\}) = r_1$, $h(\{j_0, 2\}) = r_2 + 1$ and $h(J') = s$. Observe that $\Gamma_{j_0}(\mathcal{Z}') = \{\{1\}, J\}$ and $\mathcal{B}(\mathcal{Z}, \{1\}) = \{(r_1, 0)\}$. Hence $\Gamma = \Gamma_{p_0}(\mathcal{Z}', \Pi)$ and Γ is a matroid port by Theorem 3.2.4. Given a finite field $\mathbb{K}$, Consider the $\mathbb{K}$-representation (V_1, V_2) of $\mathcal{Z}$ described in Example 3.2.2, a vector $\mathbf{v} \in V_1 \smallsetminus V_2$, and $V_{j_0} = \langle \mathbf{v} \rangle$. Then*

(V_{j_0}, V_1, V_2) *is a* $\mathbb{K}$*-representation of* $\mathcal{Z}'$. *If* $\mathbb{K}$ *is large enough,* Γ *is a* $\mathbb{K}$*-vector space access structure by Theorem 3.2.4.*

3.3 Operations on Integer Polymatroids

In order to find families of ideal multipartite access structures with the required properties, we need to find families of integer polymatroids that are representable over every large enough finite field and can be described in a compact way. To this end, we mainly use Boolean polymatroids and uniform polymatroids (Chapter 2), and several operations to obtain new polymatroids from given ones. Also some propositions of these polymatroids are presented here.

Two operations on polymatroids are presented here: the sum and the truncation. The first one is a binary operation, while the second one is unitary.

The *sum* $\mathcal{Z}_1 + \mathcal{Z}_2$ *of two polymatroids* $\mathcal{Z}_1, \mathcal{Z}_2$ on the same ground set J and with rank functions h_1, h_2, respectively, is the polymatroid on J with rank function $h = h_1 + h_2$. If $\mathcal{Z}_1, \mathcal{Z}_2$ are $\mathbb{K}$-representable integer polymatroids, then their sum is $\mathbb{K}$-representable too. Clearly, if $\mathcal{Z}_1$ is represented by the vector subspaces $(V_i)_{i \in J}$ of V and $\mathcal{Z}_2$ is represented by the vector subspaces $(W_i)_{i \in J}$ of W, then the subspaces $(V_i \times W_i)_{i \in J}$ of $V \times W$ form a representation of the sum $\mathcal{Z}_1 + \mathcal{Z}_2$. If $\mathcal{D}_1, \mathcal{D}_2 \subseteq \mathbb{Z}_+^J$ are the sets of independent vectors of $\mathcal{Z}_1$ and $\mathcal{Z}_2$, respectively, then, as a consequence of [79, Theorem 44.6 and Corollary 46.2c], the independent vectors of $\mathcal{Z}_1 + \mathcal{Z}_2$ are the ones in $\mathcal{D}_1 + \mathcal{D}_2 = \{u_1 + u_2 \ : \ u_1 \in \mathcal{D}_1, \, u_2 \in \mathcal{D}_2\}$. Therefore, the bases of $\mathcal{Z}_1 + \mathcal{Z}_2$ are the vectors in $\mathcal{B}_1 + \mathcal{B}_2$, where $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathbb{Z}_+^J$ are the families of bases of those polymatroids.

For an integer polymatroid $\mathcal{Z}$ on J with rank function h and a positive integer t with $t \leq h(J)$, it is not difficult to prove that the map h' defined by $h'(X) = \min\{h(X), t\}$ is the rank function of an integer polymatroid on J, which is called the *t-truncation of $\mathcal{Z}$*. Observe that a vector $x \in \mathbb{Z}_+^J$ is a basis of the t-truncation of $\mathcal{Z}$ if and only if x is an independent vector of $\mathcal{Z}$ and $|x| = t$.

Proposition 3.3.1. *Every truncation of a Boolean polymatroid is representable over every large enough finite field.*

Proof. For a field $\mathbb{K}$ and a positive integer t, we consider the map $\psi_t \colon \mathbb{K} \to \mathbb{K}^t$ defined by $\psi_t(x) = (1, x, \ldots, x^{t-1})$. Observe that, for every t different field elements $x_1, \ldots, x_t \in \mathbb{K}$, the set of vectors $\{\psi_t(x_i) : i = 1, \ldots, t\}$ is linearly independent. Let $\mathcal{Z}$ be a Boolean polymatroid with ground set J, take $r = h(J)$, and consider a field $\mathbb{K}$ with $|\mathbb{K}| \geq r$. Take $B \subseteq \mathbb{K}$ with $|B| = r$ and a family $(B_i)_{i \in J}$ of subsets of B such that $h(X) = |\bigcup_{i \in X} B_i|$ for every $X \subseteq J$. For a positive integer $t \leq r$ and for every $i \in J$, consider the vector subspace $V_i \subseteq \mathbb{K}^t$ spanned by the vectors in $\{\psi_t(x) : x \in B_i\}$. Clearly, these subspaces form a $\mathbb{K}$-representation of the t-truncation of the Boolean polymatroid $\mathcal{Z}$. □

The sum of uniform polymatroids is a uniform polymatroid whose increment vector is obtained by summing up the corresponding increment vectors. The next result was proved in [42], but we present its proof here because we are going to use it later.

Proposition 3.3.2 ([42], Proposition 10)**.** *Every uniform integer polymatroid is a sum of uniform matroids. In particular, every uniform integer polymatroid with ground set J is representable over every field $\mathbb{K}$ with $|\mathbb{K}| \geq |J|$.*

Proof. Consider a uniform integer polymatroid $\mathcal{Z}$ on J with increment vector $\delta = (\delta_1, \delta_2, \ldots, \delta_m)$. For every $k \in [0, \delta_1]$, take $r_k = \max\{i \in [1, m] : \delta_i \geq k\}$. Observe that $m = r_0 \geq r_1 \geq \cdots \geq r_{\delta_1} \geq 1$. Clearly $\delta_i = \max\{k \in [0, \delta_1] : r_k \geq i\}$ for every $i \in [1, m]$, and hence $\delta_i = \delta_i^1 + \cdots + \delta_i^{\delta_1}$, where δ^k is the increment vector of the uniform matroid $U_{r_k, m}$. Therefore, $\mathcal{Z} = U_{r_1, m} + \cdots + U_{r_{\delta_1}, m}$. □

3.3.1 Multipartite Access Structures from Bases of Integer Polymatroids

We present in the following a consequence of Theorem 3.2.4 that is very useful in the search of new ideal multipartite access structures. Namely, we prove that a multipartite access structure is ideal if its minimal vectors coincide with the bases of a representable integer polymatroid. We need the following two results. The first one is another version of Proposition 2.5.4 on integer polymatroids, while the second one is a basic linear algebra fact.

Proposition 3.3.3 ([30],Proposition 2.3)**.** *Let $\mathcal{Z}$ be an integer polymatroid with ground set J and let Λ be an access structure on J. Then there exists an integer polymatroid $\mathcal{Z}'$ on J' with $h(\{j_0\}) = 1$ and $\mathcal{Z} = \mathcal{Z}'|J$ such that $\Lambda = \Gamma_{j_0}(\mathcal{Z}')$ if and only if the following conditions are satisfied.*

1. *If $X \subseteq Y \subseteq J$ and $X \notin \Lambda$ while $Y \in \Lambda$, then $h(X) \leq h(Y) - 1$.*

2. *If $X, Y \in \Lambda$ and $X \cap Y \notin \Lambda$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y) - 1$.*

Lemma 3.3.4. *Let V be a vector space over a finite field $\mathbb{K}$ and let $V_1, \ldots, V_N$ be proper subspaces of V. Then $V_1 \cup \cdots \cup V_N \neq V$ if $N < |\mathbb{K}|$.*

Proposition 3.3.5. *Let $\mathcal{Z}$ be an integer polymatroid on J and let Γ be a Π-partite access structure whose minimal vectors coincide with the bases of $\mathcal{Z}$. Then Γ is a matroid port. Moreover, if $\mathcal{Z}$ is $\mathbb{K}$-representable, then Γ is an $\mathbb{L}$-vector space access structure for every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$.*

Proof. The polymatroid $\mathcal{Z} = (J, h)$ and access structure $\Lambda = \{X \subseteq J : h(X) = h(J)\}$ satisfy the conditions in Proposition 3.3.3. Let $\mathcal{Z}'$ be the integer polymatroid whose existence is given by Proposition 3.3.3. The minimal vectors of $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ coincide with the bases of $\mathcal{Z}$, and hence Γ is a matroid port by Theorem 3.2.4. Moreover, if $\mathcal{Z}$ is $\mathbb{K}$-representable, and $\mathbb{K}$ is large enough, then $\mathcal{Z}'$ is $\mathbb{K}$-representable. Indeed, consider a $\mathbb{K}$-vector space V and vector subspaces $(V_i)_{i \in J}$ forming a $\mathbb{K}$-representation of $\mathcal{Z}$. A representation of $\mathcal{Z}'$ is obtained by finding a vector $v_0 \in V$ such that $v_0 \notin \sum_{i \in X} V_i$ for every $X \subseteq J$ with $h(X) < h(J)$. Since $\sum_{i \in X} V_i \neq V$ if $h(X) < h(J)$, by Lemma 3.3.4 such a vector exists if $\mathbb{K}$ is large enough. Applying Theorem 3.2.4 again, $\Gamma = \Gamma_{j_0}(\mathcal{Z}', \Pi)$ is an $\mathbb{L}$-vector space access structure if $\mathbb{L}$ is a large enough finite extension of $\mathbb{K}$. □

3.4 Compartmented Access Structures

3.4.1 Compartmented Access Structures with Upper and Lower Bounds

Simmons [87] introduced the compartmented access structures in opposition to the hierarchical ones. Basically, compartmented access structures can be seen as a modification of threshold access structures to be used in situations that require the agreement of several parties. In a compartmented structure, all minimal qualified subsets have the same size, but other requirements are added about the number of participants in every part, or the number of involved parts.

The first examples of compartmented access structures were introduced by Simmons [87]. Brickell [22] introduced a more general family, the so-called *compartmented access structures with lower bounds*, and showed how to construct ideal secret sharing schemes for them. These are the Π-partite access structures defined by $\min \Gamma = \{u \in \mathbf{P} : |u| = t \text{ and } u \geq a\}$ for some vector $a \in \mathbb{Z}_+^J$ and some positive integer t with $t \geq |a|$. The *compartmented access structures with upper bounds* are the Π-partite access structures with $\min \Gamma = \{u \in \mathbf{P} : |u| = t \text{ and } u \leq b\}$, where $b \in \mathbb{Z}_+^J$ and $t \in \mathbb{Z}_+$ are such that $b_i \leq t \leq |b|$ for every $i \in J$. They were introduced by Tassa and Dyn [92], who constructed ideal secret sharing schemes for them.

We introduce in the following a new family of compartmented access structures that generalize the previous ones. Namely, we prove that the compartmented access structures that are defined by imposing both upper and lower bounds on the number of participants in every part are ideal.

For a positive integer t and a pair of vectors $a, b \in \mathbb{Z}_+^J$ with $a \leq b \leq \Pi(P)$, and $|a| \leq t \leq |b|$, and $b_i \leq t$, consider the Π-partite access structure Γ defined by

$$\min \Gamma = \{u \in \mathbf{P} : |u| = t \text{ and } a \leq u \leq b\}. \tag{3.4.1}$$

The compartmented access structures with upper bounds and the ones with lower bounds correspond to the compartmented access structures defined above with

$a = 0$ and with $b = \Pi(P)$, respectively.

We prove in the following that the access structures (3.4.1) are ideal by checking that they are of the form $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ for a certain family of representable integer polymatroids. Given a positive integer t and two vectors $a, b \in \mathbb{Z}_+^J$ with $a \leq b$ and $|a| \leq t \leq |b|$, consider the vector $c = b - a \in \mathbb{Z}_+^J$ and the integer $s = t - |a| \in \mathbb{Z}_+$. Let $\mathcal{Z}_1$ be the integer modular polymatroid defined by the vector a, and let $\mathcal{Z}_2$ be the s-truncation of the integer modular polymatroid defined by the vector c. Then the integer polymatroid $\mathcal{Z} = (J, h) = \mathcal{Z}_1 + \mathcal{Z}_2$ is representable over every large enough finite field. Since the family of bases of $\mathcal{Z}_1$ and $\mathcal{Z}_2$ are, respectively, $\mathcal{B}_1 = \{a\}$ and $\mathcal{B}_2 = \{u \in \mathbb{Z}_+^J : u \leq c \text{ and } |u| = s\}$, the family of bases of $\mathcal{Z}$ is $\mathcal{B} = \mathcal{B}_1 + \mathcal{B}_2 = \{u \in \mathbb{Z}_+^J : |u| = t \text{ and } a \leq u \leq b\}$. By Proposition 3.3.5, this proves that the compartmented access structures of the form (3.4.1) are vector space access structures over every large enough finite field.

3.4.2 A Construction of an Ideal Compartmented Secret Sharing Scheme

The previous proof does not provide a method to construct an ideal secret sharing scheme for the compartmented access structures with upper and lower bounds. The same applies to the proofs for the other families that are considered in this paper. As it is discussed in Section 3.7, for most of those families, no efficient method is known to construct ideal schemes. Nevertheless, non-efficient methods can be derived from the results in [41]. In order to illustrate them, we present an actual construction of an ideal secret sharing scheme for a particular compartmented access structure.

Consider a set of participants P and a 3-partition $\Pi = (\Pi_1, \Pi_2, \Pi_3)$ with $|\Pi_i| = 4$ for $i = 1,2,3$. Let Γ be the compartmented access structure with

$$\begin{aligned} \min \Gamma &= \{u \in \mathbf{P} : |u| = 5 \text{ and } (2,0,1) \leq u \leq (3,2,2)\} \\ &= \{(3,0,2), (3,1,1), (2,1,2), (2,2,1)\}. \end{aligned}$$

That is, Γ is of the form (3.4.1) for $a = (2,0,1)$, $b = (3,2,2)$ and $t = 5$. This access structure does not belong to any of the families of compartmented structures described in [22,87,92].

From Section 3.4.1, we know that Γ is a vector space access structure. Therefore, $\Gamma = \Gamma_{j_0}(\mathcal{Z}', \Pi)$ for some representable integer polymatroid $\mathcal{Z}'$. Our first step is to determine $\mathcal{Z}'$ and to find a representation for it. This is done by using the ideas and results from Section 3.4.1. Take $c = b - a = (1,2,1)$ and $s = t - |a| = 2$. Let $\mathcal{Z}_1$ be the integer modular polymatroid defined by the vector a and $\mathcal{Z}_2$ the s-truncation of the integer modular polymatroid defined by the vector c. The minimal vectors of Γ are the bases of the integer polymatroid $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$. Indeed, the families of bases of $\mathcal{Z}_1$ and $\mathcal{Z}_2$ are respectively, $\mathcal{B}_1 = \{(2,0,1)\}$ and

$$\mathcal{B}_2 = \{u \in \mathbb{Z}_+^3 : u \leq (1,2,1) \text{ and } |u| = 2\} = \{(1,0,1), (1,1,0), (0,1,1), (0,2,0)\}.$$

Then the family $\mathcal{B} = \mathcal{B}_1 + \mathcal{B}_2$ of bases of $\mathcal{Z}$ coincides with $\min \Gamma$. Consider the extension $\mathcal{Z}' = (J', h)$ of $\mathcal{Z}$ such that, for every $X \subseteq J = \{1,2,3\}$,

- $h(X \cup \{j_0\}) = h(X)$ if $h(X) = h(J)$, and

- $h(X \cup \{j_0\}) = h(X) + 1$ otherwise.

By Proposition 3.3.5, $\Gamma = \Gamma_{j_0}(\mathcal{Z}', \Pi)$.

The proof of Proposition 3.3.5 provides the tools to find a representation of $\mathcal{Z}'$. A representation of $\mathcal{Z}$ is needed and, since $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$, it is obtained from representations from these two polymatroids. Let $\mathbb{K}$ be a large enough finite field. More specific requirements on the size of $\mathbb{K}$ will be given in the following. The subspaces $W_1 = \langle (1,0,0),(0,1,0) \rangle$, $W_2 = \{0\}$, and $W_3 = \langle (0,0,1) \rangle$ of $\mathbb{K}^3$ form a $\mathbb{K}$-representation of the modular polymatroid $\mathcal{Z}_1$. Since $\mathcal{Z}_2$ is a 2-truncation of a modular polymatroid, a representation for it can be found from the proof of Proposition 3.3.1. Namely, given four different elements x_1, x_2, x_3, x_4 in $\mathbb{K}$, the vector spaces $W_1' = \langle \psi_2(x_1) \rangle$, $W_2' = \langle \psi_2(x_2), \psi_2(x_3) \rangle$, and $W_3' = \langle \psi_2(x_4) \rangle$ of $\mathbb{K}^2$ form a $\mathbb{K}$-representation of $\mathcal{Z}_2$. Nevertheless, in this case we can find a simpler representation for $\mathcal{Z}_2$ that works over every field. Namely, the one given by the vector spaces $W_1'' = \langle (1,0) \rangle$, $W_2'' = \mathbb{K}^2$, and $W_3'' = \langle (0,1) \rangle$ Therefore, the subspaces $V_i = W_i \times W_i''$ of $\mathbb{K}^5$ form a $\mathbb{K}$-representation of $\mathcal{Z}$, At this point, we use this representation of $\mathcal{Z}$ to construct a $\mathbb{K}$-representation of $\mathcal{Z}'$. Since $h(\{1,3\}) = h(J) = 5$ and $h(\{1,2\}), h(\{2,3\}) < 5$, we have to find a vector in $\mathbb{K}^5$ that is neither in $V_1 + V_2$ nor in $V_2 + V_3$. The vector $(1,1,1,0,0)$ satisfies these requirements. Summarizing, the subspaces

- $V_{j_0} = \langle (1,1,1,0,0) \rangle$,
- $V_1 = \langle (1,0,0,0,0), (0,1,0,0,0), (0,0,0,1,0) \rangle$,
- $V_2 = \langle (0,0,0,1,0), (0,0,0,0,1) \rangle$, and

- $V_3 = \langle (0,0,1,0,0), (0,0,0,0,1) \rangle$

form a $\mathbb{K}$-representation of $\mathcal{Z}'$.

The second step is to construct a $\mathbb{K}$-vector space secret sharing scheme for Γ from the representation $(V_i)_{i \in J'}$ of $\mathcal{Z}'$. This is done by using the results in [41, Section 6]. Namely, given $\Pi_{j_0} = \{p_0\}$ and the partition $\Pi' = (\Pi_{j_0}, \Pi_1, \Pi_2, \Pi_3)$ of $P' = P \cup \{p_0\}$, we have to find a $\mathbb{K}$-representation for the Π'-partite matroid $\mathcal{M} = (P', r)$ such that $\Gamma = \Gamma_{p_0}(\mathcal{M})$. Such a representation consists of a 5×13 matrix $M = (M_{j_0} | M_1 | M_2 | M_3)$ over $\mathbb{K}$, in which, for every $i \in J'$, the columns of M_i correspond to the players in Π_i. The matrix M must have the following properties.

1. M_i is a $5 \times |\Pi_i|$ whose columns are vectors in V_i.

2. If $u = (u_{j_0}, u_1, u_2, u_3)$ is a basis of $\mathcal{Z}'$, every 5×5 submatrix of M formed by u_i columns in every M_i is nonsingular.

The linear code generated by such a matrix defines a $\mathbb{K}$-vector space secret sharing scheme for Γ. According to [41, Corollary 6.7], such a matrix exists if $|\mathbb{K}| > \binom{13}{5} = 1287$, but we show next that it exists as well over much smaller fields. The submatrix M_{j_0}, which has only one column, is given by a nonzero vector in V_{j_0}. Since every 3 columns of M_1 must be linearly independent, they can be Vandermonde-like linear combinations of the vector in the above basis of V_1. We do the same for the columns of M_2 and M_3. Therefore, we take the columns of M_1, M_2 and M_3 of the forms $(1, \lambda, 0, \lambda^2, 0)$, $(0,0,0,1,\mu)$, and $(0,0,1,0,\gamma)$, respectively. At this point, we have to find values $(\lambda_i)_{1 \le i \le 4}$, $(\mu_i)_{1 \le i \le 4}$, and $(\gamma_i)_{1 \le i \le 4}$ in some finite field $\mathbb{K}$ such that the matrix

$$M = \left(\begin{array}{c|cccc|cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \lambda_4^2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \end{array} \right)$$

satisfies the second property above. The bases of $\mathcal{Z}'$ are $(0,2,1,2)$, $(0,2,2,1)$, $(0,3,0,2)$, $(0,3,1,1)$, $(1,1,1,2)$, $(1,2,0,2)$, $(1,2,1,1)$, $(1,1,2,1)$, $(1,2,2,0)$, $(1,3,0,1)$, and $(1,3,1,0)$. By using a simple computer program, one can check different sets of values of the parameters until a satisfactory one is found. A possible solution is the following matrix over $\mathbb{F}_{23}$.

$$M = \left(\begin{array}{c|cccc|cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 2 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 4 & -10 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 2 & -2 & 5 & -5 & 7 & 9 \end{array} \right)$$

Therefore, M is the generator matrix of a linear code that defines an $\mathbb{F}_{23}$-vector space secret sharing scheme with access structure Γ.

3.4.3 Compartmented Compartments

We introduce next another family of compartmented access structures. In this case, instead of an upper bound for every compartment, we have upper bounds for groups of compartments. Take $J = [1, m] \times [1, n]$ and a partition $\Pi = (\Pi_{ij})_{(i,j) \in J}$ of the set P of participants. Take vectors $a \in \mathbb{Z}_+^J$ and $b \in \mathbb{Z}_+^m$, and an integer t with $|a| \leq t \leq |b|$ and $\sum_{j=1}^n a_{ij} \leq b_i \leq t$ for every $i \in [1, m]$. Consider the Π-partite access structure Γ defined by

$$\min \Gamma = \left\{ u \in \mathbf{P} \,:\, |u| = t, \text{ and } a \leq u, \text{ and } \sum_{j=1}^n u_{ij} \leq b_i \text{ for every } i \in [1, m] \right\}.$$

That is, the compartments are distributed into m groups and we have an upper bound for the number of participants in every group of compartments, while we have a lower bound for every compartment.

We prove next that these access structures admit a vector space secret sharing scheme over every large enough finite field. Consider the vector $c \in \mathbb{Z}_+^m$ defined by $c_i = b_i - \sum_{j=1}^n a_{ij}$ and the integer $s = t - |a| \in \mathbb{Z}_+$. Let $\mathcal{Z}_1$ be the integer modular polymatroid with ground set J defined by the vector a. Let $\mathcal{Z}_3$ the integer polymatroid with ground set J and family of bases

$$\mathcal{B}_3 = \left\{ u \in \mathbb{Z}_+^J \,:\, \sum_{j=1}^n u_{ij} = c_i \text{ for every } i \in [1, m] \right\},$$

and let $\mathcal{Z}_2$ be the s-truncation of $\mathcal{Z}_3$. Finally, take $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$.

Lemma 3.4.1. *The minimal qualified sets of* Γ *coincide with the bases of* $\mathcal{Z}$*.*

Proof. Let $\mathcal{B}$ and $\mathcal{B}_2$ be the families of bases of $\mathcal{Z}$ and $\mathcal{Z}_2$, respectively. The bases of

$\mathcal{Z}$ are precisely the vectors of the form $u = a + v$ with $v \in \mathcal{B}_2$. Observe that a vector $v \in \mathbb{Z}_+^J$ is in $\mathcal{B}_2$ if and only if $|v| = s$ and $\sum_{j=1}^n v_{ij} \leq c_i$ for every $i \in [1, m]$. □

Lemma 3.4.2. *The integer polymatroid $\mathcal{Z}$ is representable over every large enough finite field.*

Proof. We only have to prove that this holds for $\mathcal{Z}_2$. By Proposition 3.3.1, for every large enough finite field $\mathbb{K}$ there exist subspaces $(V_i)_{i \in [1,m]}$ of a $\mathbb{K}$-vector space V that form a representation of the s-truncation of the modular polymatroid with ground set $[1, m]$ defined by the vector c. Then the subspaces $(W_{ij})_{(i,j) \in J}$ of V with $W_{ij} = V_i$ for every $j \in [1, n]$ form a representation of $\mathcal{Z}_2$. □

3.4.4 Other Compartmented Access Structures

The *dual* Γ^* of an access structure Γ on P is the access structure on the same set defined by $\Gamma^* = \{A \subseteq P : P \smallsetminus A \notin \Gamma\}$. Observe that $\Gamma^{**} = \Gamma$, and that Γ is Π-partite for some partition Π if and only if Γ^* is so. Moreover, Γ admits a $\mathbb{K}$-vector space secret sharing scheme for some finite field $\mathbb{K}$ if and only if Γ^* does [56].

Let Π be an m-partition of a set P of participants. Given $t' \in \mathbb{Z}_+$ and $a' \in \mathbb{Z}_+^J$ with $|a'| \leq t'$, consider the compartmented access structure with lower bounds

$$\Gamma = \{u \in \mathbf{P} : |u| \geq t' \text{ and } u \geq a'\}.$$

Take $t = |P| - t' + 1$ and the vector $a \in \mathbb{Z}_+^J$ defined by $a_i = |\Pi_i| - a'_i + 1$. Then the dual of Γ is the access structure

$$\Gamma^* = \{u \in \mathbf{P} \;\; |u| \geq t \text{ or } u_i \geq a_i \text{ for some } i \in J\}. \tag{3.4.2}$$

Therefore, for every $t \in \mathbb{Z}_+$ and $a \in \mathbb{Z}_+^J$ with $|a| \geq t + m - 1$, the access structure (3.4.2) admits a $\mathbb{K}$-vector space secret sharing scheme for every large enough field $\mathbb{K}$. This can be proved as well by checking that the access structure (3.4.2) is of the form $\Gamma_{j_0}(\mathcal{Z}', \Pi)$, being $\mathcal{Z}'$ the truncation of a Boolean polymatroid. Indeed, let B be a set with $|B| = |a| - m + 1$ and take subsets $(B_i)_{i \in J'}$ of B such that $|B_{j_0}| = 1$ and $|B_i| = a_i$ for every $i \in J$, and $B_i \cap B_j = B_{j_0}$ for every $i, j \in J$ with $i \neq j$. Let $\mathcal{Z}'$ be the t-truncation of the Boolean polymatroid defined by this family of subsets. Clearly $\Gamma_{j_0}(\mathcal{Z}', \Pi)$ is equal to the access structure (3.4.2).

Simmons [87] introduced another family of compartmented access structures, in which the authorized subsets must have at least a certain number of participants in a certain number of the parts. Specifically, given $s \in \mathbb{Z}_+$ with $1 \leq s \leq m$ and a vector $a \in \mathbb{Z}_+^J$, consider the m-partite access structure Γ such that a vector $u \in \mathbf{P}$ is in Γ if and only if $|\{i \in J : u_i \geq a_i\}| \geq s$. This access structure is in fact a composition of threshold structures, and hence it admits a $\mathbb{K}$-vector space secret sharing scheme for every $\mathbb{K}$ with $|\mathbb{K}| \geq \max\{m, |\Pi_1|, \ldots, |\Pi_m|\}$. Indeed, this is done by computing shares of the secret value according to an (s, m)-threshold scheme and redistributing each of the m shares according to an $(a_i, |\Pi_i|)$-threshold scheme.

We consider now a slightly modification of these structures, in which we additionally require the authorized subsets to have at least t participants. The resulting access structures are not ideal in general, and we can prove that by using as well the connection between ideal multipartite access structures and integer polymatroids. For instance, consider such an access structure Γ given by $m = 3$, $s = 2$, $t = 7$, and $a = (3, 3, 3)$. Suppose that it is ideal, and let $\mathcal{Z}'$ be the integer polymatroid such that $\Gamma = \Gamma_{j_0}(\mathcal{Z}', \Pi)$. Since $(3,3,1)$ and $(3,1,3)$ are in $\min \Gamma$, they are bases of $\mathcal{Z} = \mathcal{Z}'|J$. By the exchange property, $(3,2,2)$ is a basis of $\mathcal{Z}'$ too, a contradiction because $(3,2,2) \notin \Gamma$.

3.5 Ideal Partially Hierarchical Access Structures

3.5.1 Ideal Hierarchical Access Structures

For an access structure Γ on a set P, we say that a participant $p \in P$ is *hierarchically superior in* Γ to a participant $q \in P$, and we write $q \preceq p$, if $A \cup \{p\} \in \Gamma$ for every $A \subseteq P \smallsetminus \{p, q\}$ with $A \cup \{q\} \in \Gamma$. Two participants are *hierarchically equivalent* if $q \preceq p$ and $p \preceq q$. Observe that, if Γ is Π-partite, every pair of participants in the same part Π_i are hierarchically equivalent. Because of that, the relation $\preceq$ induces a partial order on Π.

An access structure is *hierarchical* if every pair of participants are hierarchically comparable. In this situation, the hierarchical order $\preceq$ is a total order on Π. *Weighted threshold access structures*, which were introduced by Shamir [82] in his seminal work, are hierarchical, but they are not ideal in general. The ideal weighted threshold access structures were characterized by Beimel, Tassa and Weinreb [12]. Other examples of hierarchical access structures are the the multilevel access structures introduced by Simmons [87], which were proved to be ideal by Brickell [22], and the hierarchical threshold access structures presented by Tassa [90]. These were the only known families of ideal hierarchical access structures before the connection between integer polymatroids and ideal multipartite secret sharing presented in [41] made it possible to characterize the ideal hierarchical access structures [43]. Actually, all ideal hierarchical access structures are obtained from a special class of Boolean polymatroids [43] and, because of that, they are vector space access structures over every large enough finite field. Moreover, they admit a very compact description, as we see in the following.

Consider two sequences $a = (a_0, \dots, a_m)$ and $b = (b_0, \dots, b_m)$ of integer numbers such that $a_0 = a_1 = b_0 = 1$ and $a_i \leq a_{i+1} \leq b_i \leq b_{i+1}$ for every $i \in [0, m-1]$. Take $J = [1, m]$ and $j_0 = 0$. Consider the Boolean polymatroid $\mathcal{Z}' = \mathcal{Z}'(a, b)$ with ground set $J' = [0, m]$, given the sets $B_i = [a_i, b_i]$ for $i \in [0, m]$ of the set $B = [1, b_m]$. It is proved in [43] that a vector $u \in \mathbf{P} \subseteq \mathbb{Z}_+^m$ is in the Π-partite access structure $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ if and only if there exists $i_0 \in [1, m]$ such that $\sum_{j=1}^{i_0} u_j \geq b_{i_0}$, and $\sum_{j=1}^{i} u_j \geq a_{i+1} - 1$ for all $i \in [1, i_0 - 1]$. Therefore, the participants in Π_i are hierarchically superior to the participants in Π_j if $i \leq j$, and hence every access structure of the form $\Gamma_0(\mathcal{Z}'(a, b), \Pi)$ is hierarchical. Moreover, every ideal hierarchical access structure is of this form or it can be obtained from a structure of this form by removing some participants [43].

In particular, if $a_i = 1$ for all $i \in [0, m]$ and $1 = b_0 \leq b_1 < \cdots < b_m$, then $u \in \Gamma_0(\mathcal{Z}'(a, b), \Pi)$ if and only if $\sum_{j=1}^{i_0} u_j \geq b_{i_0}$ for some $i_0 \in [1, m]$. These are precisely the *multilevel access structures* introduced by Simmons [87], also called *disjunctive hierarchical threshold access structures* by other authors [90]. They were proved to be ideal by Brickell [22]. On the other hand, the *conjunctive hierarchical threshold access structures* for which Tassa [90] constructs ideal secret sharing schemes are obtained by considering $1 = a_0 = a_1 < \cdots < a_m$ and $1 = b_0 < b_1 = \cdots = b_m$. In this case, $u \in \Gamma_0(\mathcal{Z}'(a,b),\Pi)$ if and only if $\sum_{j=1}^{i} u_j \geq a_{i+1} - 1$ for all $i \in [1, m-1]$ and $\sum_{j=1}^{m} u_j \geq b_m$. Observe that, in an access structure in the first family there may be qualified subsets involving only participants in the lowest level. This is not the case in any access structure in the second family, because every qualified subset must contain participants in the highest level.

By using the results in [43], we can find other ideal hierarchical access structures with more flexible properties. If we take, for instance, $a = (1,1,1,5,5)$ and $b = (1,4,6,10,12)$, every qualified subset in the hierarchical access structure $\Gamma_0(\mathcal{Z}'(a,b),\Pi)$ must contain participants in the first two levels, but some of them do not have any participant in the first level.

3.5.2 Partial Hierarchies from Boolean Polymatroids

Moreover, by considering other Boolean polymatroids, we can find other families of ideal access structures satisfying some given *partial hierarchy*, that is, Π-partite access structures in which the hierarchical relation $\preceq$ on Π is a partial order. We present next an example of such a family of ideal *partially hierarchical access structures*. Consider a family of subsets $(B_i)_{i \in [0,m]}$ of a finite set B satisfying:

- $|B_0| = 1$ and $B_0 \subseteq B_1$, while $B_0 \cap B_i = \emptyset$ if $i \in [2,m]$, and
- $B_1 \cap B_i \neq \emptyset$ for every $i \in [2,m]$, and
- $B_i \cap B_j = \emptyset$ for every $i, j \in [2,m]$ with $i \neq j$.

Let $\mathcal{Z}'$ be the Boolean polymatroid with ground set $J' = [0,m]$ defined from this family of subsets, and consider the Π-partite access structure $\Gamma = \Gamma_0(\mathcal{Z}',\Pi)$. Take

$t_1 = |B_1|$, and $t_i = |B_i \smallsetminus B_1|$ and $s_i = |B_i \cap B_1|$ for $i \in [2, m]$. Then a vector $x \in \mathbf{P}$ is in the access structure Γ if and only if there exist a vector $u \in \mathbf{P}$ such that

- $u \leq x$,
- $1 \in \operatorname{supp}(u) = X$, $|u| = \sum_{i \in X} t_i$,
- for every $Y \subseteq X$, $|u(Y)| \leq \sum_{i \in Y}(t_i + s_i)$, where $s_1 = 0$.

Clearly, $q \preceq p$ if $p \in \Pi_1$ and $q \in \Pi_i$ for some $i \in [2, m]$. On the other hand, any two participants in two different parts Π_i, Π_j with $i, j \in [2, m]$ are not hierarchically related.

3.5.3 Compartmented Access Structures with Hierarchical Compartments

We can consider as well compartmented access structures with hierarchical compartments. Take $J = [1, m] \times [1, n]$ and a partition $\Pi = (\Pi_{ij})_{(i,j) \in J}$ of the set P of participants. Consider a finite set B and a family of subsets $(B_{ij})_{(i,j) \in J}$ such that $B_{in} \subseteq \cdots \subseteq B_{i2} \subseteq B_{i1}$ for every $i \in [1, m]$, and $B_{11} \cup \cdots \cup B_{m1} = B$, and $B_{i1} \cap B_{j1} = \emptyset$ if $i \neq j$. Let $\mathcal{Z}$ be the t-truncation of the Boolean polymatroid defined by this family of subsets. If Γ is a Π-partite access structure such that its minimal vectors coincide with the bases of $\mathcal{Z}$, then Γ is a vector space access structure over every large enough finite field. We now describe Γ. For $(i, j) \in J$, take $b_{ij} = |B_{ij}|$. Consider the vector $b = (b_{11}, \ldots, b_{m1}) \in \mathbb{Z}_+^m$. Of course, $|b| = |B|$. Suppose $b_{i1} \leq t \leq |b|$ for every $i \in [1, m]$. It is not difficult to check that a vector $u \in \mathbb{Z}_+^J$ is a basis of $\mathcal{Z}$, and hence a minimal vector of Γ, if and only if $|u| = t$ and

$\sum_{k=j}^{n} u_{ik} \leq b_{ij}$ for every $(i,j) \in J$. Observe that Γ can be seen as a compartmented access structure with compartments $\Pi_i = \bigcup_{j=1}^{n} \Pi_{ij}$ for $i \in [1,m]$, because every minimal qualified subset has exactly t participants, and at most b_{i1} of them in compartment Π_i. In addition, we have a hierarchy within every compartment. Actually, $q \preceq p$ if $p \in \Pi_{ij}$ and $q \in \Pi_{ik}$ with $j \leq k$.

The ideal compartmented access structures introduced in Section 3.4.4 can be modified in a similar way to introduce a hierarchy in every compartment. Take $J = [1,m] \times [1,n]$, $J' = J \cup \{0\}$, and a partition $\Pi = (\Pi_{ij})_{(i,j)\in J}$ of the set P of participants. Consider a finite set B, a family of subsets $(B_{ij})_{(i,j)\in J}$ and B_0 such that $|B_0| = 1$, $B_0 \subseteq B_{i1} \subseteq \cdots \subseteq B_{in}$ for every $i \in [1,m]$, and $B_{in} \cap B_{jn} = B_0$ for $i \neq j$. For $(i,j) \in J$, take $b_{ij} = |B_{ij}|$. Let $\mathcal{Z}'$ be the t-truncation of the Boolean polymatroid on J' defined by this family of subsets. Then the access structure $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ is a vector space access structure over every large enough finite field. In this case, a vector $u \in \mathbb{Z}_+^J$ is a basis of $\mathcal{Z} = \mathcal{Z}'|J$ if and only if $|u| = t$ and $\sum_{k=j}^{n} x_{ik} \leq b_{ij}$ for every $(i,j) \in J$. Observe that $\mathcal{B}(\mathcal{Z}, X) \subseteq \Gamma$ for every nonempty subset $X \subseteq J$, so Γ can be described as follows

$$\Gamma = \left\{ u \in \mathbb{Z}^J \ : \ |u| \geq t \text{ or } \sum_{j=1}^{k} u_{ij} \geq b_{ik} \text{ for some } (i,k) \in J \right\}.$$

3.6 Ideal Uniform Multipartite Access Structures

Herranz and Sáez [51, Section 3.2] introduced a family of ideal multipartite access structures that can be seen as a variant of the compartmented ones. Specifically, given integers $1 \leq k \leq t$, consider the Π-partite access structure defined by

$$\Gamma = \{u \in \mathbf{P} : |u| \geq t \text{ and } |\operatorname{supp}(u)| \geq k\}. \tag{3.6.1}$$

It is proved in [51] that Γ is a vector space access structure over every large enough finite field. Observe that the parts in the partition $\Pi = (\Pi_i)_{i \in J}$ are symmetrical in Γ. That is, the minimal vectors of Γ are invariant under any permutation on J. In the following, we characterize all ideal multipartite access structures with this property.

A Π-partite access structure Γ is said to be *uniform* if the set $\min \Gamma \subseteq \mathbb{Z}_+^J$ of its minimal vectors is symmetric, that is, if $u = (u_i)_{i \in J} \in \min \Gamma$, then $\sigma u = (u_{\sigma i})_{i \in J} \in \min \Gamma$ for every permutation σ on J. In this section, we characterize the uniform multipartite access structures that admit an ideal secret sharing scheme. Moreover, we prove that all such access structures are vector space access structures over every large enough finite field. This is done by using the uniform integer polymatroids described in Section 2.3.1 to construct a family of uniform multipartite access structures that admit a vector space secret sharing scheme over every large enough finite field. Then we prove in Theorem 3.6.3 that every ideal uniform multipartite access structure is a member of this family.

Let $\mathcal{Z}$ be a uniform integer polymatroid with increment vector δ on a ground set J with $|J| = m$. For $i \in [1, m]$, consider $h_i = \sum_{j=1}^{i} \delta_j$ and $h_0 = 0$, the values of the rank function of $\mathcal{Z}$. Recall that the (k, m)-threshold access structure on J consists of all subsets of J with at least k elements.

Lemma 3.6.1. *For an integer $k \in [1, m]$, there exists an integer polymatroid $\mathcal{Z}'_k$ on $J' =$*

$J \cup \{j_0\}$ with $h(\{j_0\}) = 1$ and $\mathcal{Z} = \mathcal{Z}'_k|J$ such that $\Gamma_{j_0}(\mathcal{Z}'_k)$ is the (k, m)-threshold access structure on J if and only if $1 \le k \le m - 1$ and $\delta_k > \delta_{k+1}$, or $k = m$ and $\delta_m > 0$.

Proof. If there exists a polymatroid $\mathcal{Z}'$ with the required properties, then the first condition in Proposition 3.3.3 implies that $h_{k-1} < h_k$, while $h_{k+1} + h_{k-1} < 2h_k$ if $1 \le k \le m - 1$ by the second one. Therefore, our condition is necessary. We prove now sufficiency. Let Λ be the (k, m)-threshold access structure on J. Observe that $h_k > h_{k-1}$ because $\delta_k > 0$, and hence $h(X) < h(Y)$ if $X \subseteq Y \subseteq J$ and $X \notin \Lambda$ while $Y \in \Lambda$. Consider now two subsets $X, Y \in \Lambda$ such that $X \cap Y \notin \Lambda$. This implies in particular that $k < m$. Take $r_1 = |X| \ge k$, $r_2 = |Y| \ge k$, and $s = |X \cap Y| < k$. Then

$$h_{r_1+r_2-s} - h_{r_2} = \sum_{i=1}^{r_1-s} \delta_{r_2+i} < \sum_{i=1}^{r_1-s} \delta_{s+i} = h_{r_1} - h_s.$$

The inequality holds because $k = s + i_0$ for some $i_0 \in [1, r_1 - s]$, and hence $\delta_{s+i_0} > \delta_{r_2+i_0}$. Therefore, $h(X \cup Y) + h(X \cap Y) < h(X) + h(Y)$. By Proposition 3.3.3, this concludes the proof. □

Consider an integer $k \in [1, m]$ in the conditions of Lemma 3.6.1 and the corresponding integer polymatroid $\mathcal{Z}'_k$. For a partition $\Pi = (\Pi_i)_{i \in J}$ of a set P of participants, consider the Π-partite access structure $\Gamma = \Gamma_{j_0}(\mathcal{Z}'_k, \Pi)$. A vector $v \in \mathbf{P}$ is in Γ if and only if there exists a vector u with $0 \le u \le v$ such that

- $s = |\operatorname{supp}(u)| \ge k$ and $|u| = h_s$, and
- $|u(Y)| \le h_i$ for every $i \in [1, m]$ and for every $Y \subseteq J$ with $|Y| = i$.

As a consequence of the next lemma, $\Gamma = \Gamma_{j_0}(\mathcal{Z}'_k, \Pi)$ is a vector space access structure over every large enough finite field.

Lemma 3.6.2. *The integer polymatroid $\mathcal{Z}'_k$ is representable over every large enough finite field.*

Proof. The integer polymatroid $\mathcal{Z} = \mathcal{Z}'_k | J$ is uniform, and hence it is representable over every finite field with at least m elements. By the proof of Proposition 3.3.2, this polymatroid is of the form $\mathcal{Z} = U_{r_1,m} + \cdots + U_{r_{\delta_1},m}$, where $r_j = \max\{i \in J_m : \delta_i \geq j\}$. Consider a finite field $\mathbb{K}$ with $|\mathbb{K}| \geq \binom{m}{k-1}$. For an integer $r > 0$, consider the mapping $\psi_r \colon \mathbb{K} \to \mathbb{K}^r$ defined by $\psi_r(x) = (1, x, \ldots, x^{r-1})$. For every $i \in J$ take $x_i \in \mathbb{K}$ such that $x_i \neq x_j$ if $i \neq j$. Consider the vector space $V = \mathbb{K}^{h_m} = \mathbb{K}^{r_1} \times \cdots \times \mathbb{K}^{r_{\delta_1}}$ and, for every $i \in J$, the subspace $V_i \subseteq V$ spanned by the vectors $(\psi_{r_1}(x_i), 0, \ldots 0), \ldots, (0, \ldots, 0, \psi_{r_{\delta_1}}(x_i))$. These subspaces form a representation of $\mathcal{Z}$. We have to find now a vector $v_0 \in V$ to complete it to a representation of $\mathcal{Z}'_k$. This vector must satisfy that $v_0 \in \sum_{i \in X} V_i$ for every $X \subseteq J$ with $|X| = k$, while $v_0 \notin \sum_{i \in X} V_i$ for every $X \subseteq J_m$ with $|X| = k - 1$. Clearly, $\delta_k > 0$ and $r_{\delta_k} = k$. For every $X \subseteq J$, consider the subspace $W_X \subseteq \mathbb{K}^t$ spanned by the vectors $(\psi_k(x_i))_{i \in X}$. Then $W_X \subsetneq \mathbb{K}^k$ if $|X| = k - 1$. By Lemma 3.3.4, there exists a vector $v \in \mathbb{K}^t$ such that $v \notin W_X$ for every $X \subseteq J$ with $|X| = t - 1$. Then the vector $v_0 = (0, \ldots, 0, u_{\delta_k}, 0 \ldots, 0) \in V$ with $u_{\delta_k} = v$ satisfies the required conditions. □

Theorem 3.6.3. *Let $\Pi = (\Pi_i)_{i \in J}$ with $|J| = m$ be a partition of a set P of participants and let Γ be a uniform Π-partite access structure. Then Γ is a matroid port if and only if there exist a uniform integer polymatroid $\mathcal{Z}$ on J and an integer $k \in [1, m]$ in the conditions of Lemma 3.6.1 such that $\Gamma = \Gamma_{j_0}(\mathcal{Z}'_k, \Pi)$. In particular, every uniform multipartite matroid port is a vector space access structure over every large enough finite field.*

Proof. Without loss of generality, we can assume that all parts Π_i have the same cardinality. By Theorem 3.2.4, if Γ is a matroid port, there exists an integer polymatroid $\mathcal{Z}'$ with ground set $J' = J \cup \{j_0\}$ such that $\Gamma = \Gamma_{j_0}(\mathcal{Z}', \Pi)$. Consider $\mathcal{Z} = \mathcal{Z}'|J$. Every permutation τ on P such that for every $i \in J$ there is $j \in J$ with $\tau(\Pi_i) = \Pi_j$ is an automorphism of Γ. This implies that every permutation σ on J is an automorphism of $\mathcal{Z}$, and hence $\mathcal{Z}$ is a uniform integer polymatroid. Clearly, every permutation σ on J is also an automorphism of the access structure $\Gamma_{j_0}(\mathcal{Z}')$ on J, and hence $\Gamma_{j_0}(\mathcal{Z}')$ is the (k, m)-threshold access structure on J for some $k \in [1, m]$. This implies that the uniform integer polymatroid $\mathcal{Z}$ and the integer k satisfy the conditions in Lemma 3.6.1 and that $\mathcal{Z}' = \mathcal{Z}'_k$. □

The uniform multipartite access structures of the form (3.6.1) were proved to be ideal in [51]. By using the previous characterization, we obtain a shorter proof for this fact. Consider the uniform integer polymatroid $\mathcal{Z}$ on J with increment vector δ defined by $\delta_1 = t - k + 1$, and $\delta_i = 1$ if $i \in [2, k]$, and $\delta_i = 0$ if $i \in [k+1, m]$. Consider the integer polymatroid $\mathcal{Z}'_k$ whose existence is given by Lemma 3.6.1. We claim that every Π-partite access structure Γ of the form (3.6.1) is equal to $\Gamma_{j_0}(\mathcal{Z}'_k, \Pi)$. Indeed, a vector $v \in \mathbf{P}$ is in $\Gamma_{j_0}(\mathcal{Z}'_k, \Pi)$ if and only if there exists a vector u with $0 \leq u \leq v$ such that

- $s = |\operatorname{supp}(u)| \geq k$ and $|u| = h_s = t$, and
- $|u(Y)| \leq h_i$ for every $i \in [1, m]$ and for every $Y \subseteq J$ with $|Y| = i$.

Since $h_i = t - k + i$ for every $i \in [1, k]$, it is clear that every vector $u \in \mathbf{P}$ satisfying the first condition satisfies the second as well.

3.7 Efficiency of the Constructions of Ideal Multipartite Secret Sharing Schemes

Several families of ideal multipartite access structures have been presented in the previous sections. We proved that every one of these structures admits a vector space secret sharing scheme over every large enough finite field. Our proofs are not constructive, but a general method to construct vector space secret sharing schemes for multipartite access structures that are associated to representable integer polymatroids was given in [41]. Unfortunately, this method is not efficient, and no general efficient method is known.

Some issues related to the efficiency of the constructions of ideal schemes for several particular families of multipartite access structures have been considered [15, 22, 49, 90, 92]. We describe in the following a unified framework, derived from the general results in [41], in which those open problems can be more precisely stated.

Take $J = [1, m]$ and let $(\Pi_i)_{i \in J}$ be a partition of the set P of participants, where $|\Pi_i| = n_i$ and $|P| = n$. Take $J' = J \cup \{0\}$, that is, $j_0 = 0$ and consider an integer polymatroid $\mathcal{Z}' = (J', h)$ with $k_i = h(\{i\}) \leq n_i$ for every $i \in J$ and $k_0 = h(\{0\}) = 1$, and take $k = h(J')$. Consider as well a finite field $\mathbb{K}$ and a $\mathbb{K}$-representation $(V_i)_{i \in J'}$ of $\mathcal{Z}'$. In this situation, one has to find a matrix $M = (M_0 | M_1 | \cdots | M_m)$ over $\mathbb{K}$ with the following properties:

1. M_i is a $k \times n_i$ matrix ($n_0 = 1$) whose columns are vectors in V_i.

2. If $u = (u_0, u_1, \ldots, u_m)$ is a basis of $\mathcal{Z}'$, every $k \times k$ submatrix of M formed by

u_i columns in every M_i is nonsingular.

As a consequence of the results in [41], every such a matrix M defines a vector space secret sharing scheme for the multipartite access structure $\Gamma_0(\mathcal{Z}', \Pi)$.

One of the unsolved questions is to determine the minimum size of the fields over which there exists a vector space secret sharing scheme for $\Gamma_0(\mathcal{Z}', \Pi)$. An upper bound can be derived from [41, Corollary 6.7]. Namely, such a matrix M exists if $|\mathbb{K}| > \binom{n+1}{k}$. The best known lower bound is linear on the number of participants, and it can be derived from the known results about the existence of maximum distance separable codes. Even though very large fields are required in general to find such a matrix by using the known methods, the number of bits to represent the elements in the base field is polynomial on the number of participants, and hence the computation of the shares and the the reconstruction of the secret value can be efficiently performed in such a vector space secret sharing scheme.

Another open problem is the existence of efficient methods to construct a vector space secret sharing scheme for $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$, that is, the existence of polynomial-time algorithms to compute a matrix M with the properties above. One important drawback is that no efficient method is known to check whether a matrix M satisfying Property 1 satisfies as well Property 2. Moreover, this seems to be related to some problems about representability of matroids that have been proved to be co-NP-hard [78].

We discuss in the following some general construction methods that can be derived from the techniques introduced in previous works [15,22,49,74,90,92] for particular families of multipartite access structures.

The first method, which was used in [22,74] and other works, consists basically in constructing the matrix M column by column, checking at every step that all submatrices that must be nonsingular are so. Arbitrary vectors from the subspaces V_i can be selected at every step, but maybe a wiser procedure is to take vectors of some special form as, for instance, Vandermonde linear combinations of some basis of V_i. In any case, an exponential number of determinants have to be computed.

A probabilistic algorithm was proposed in [90,92] for multilevel and compartmented access structures. Namely, the vectors from the subspaces V_i are selected at random. This method applies as well to the general case and the success probability is at least $1 - \binom{n+1}{k} N |\mathbb{K}|^{-1}$, where $N = \sum_{i \in J} k_i n_i$. By using this method, a matrix M that, with high probability, defines a secret sharing scheme for the given access structure can be obtained in polynomial time. Nevertheless, no efficient methods to check the validity of the output matrix are known.

Brickell [22] and by Tassa [90] proposed efficient construction methods for the hierarchical threshold access structures. Other related solutions appeared in [15,49] for very particular cases of hierarchical threshold access structures. To better understand these methods, let us consider first the case of the threshold access structures. If the field $|\mathbb{K}|$ is very large, $n+1$ randomly chosen vectors from $\mathbb{K}^k$ will define with high probability an ideal (k,n)-threshold scheme. Nevertheless, no efficient algorithm to check the validity of the output is available. One can instead choose $n+1$ vectors of the Vandermonde form, and in this case an ideal (k,n)-threshold scheme is obtained, and of course we can check its validity in polynomial time. The solutions proposed in those works are based on the same idea. Namely, the vectors from the subspaces V_i have to be of some special form such that a matrix with the required properties is obtained and, in addition, the validity of the output can be efficiently checked. The solution proposed by Brickell [22], which requires to compute a primitive element in an extension field whose extension degree increases with the number of participants, is efficient by using Shoup's algorithm [85]. The one proposed in [90, Section 3.3], which works only for prime fields, provides a polynomial time algorithm to construct a vector space secret sharing scheme for every hierarchical threshold access structure. Recently, similar efficient constructions of representations for all bipartite matroids have been presented [4]. The existence of efficient methods for other families of multipartite access structures is an open problem.

Chapter 4

Lower Bounds on Information Ratio by Linear Programming

4.1 Introduction

In this chapter we focus on the information ratio of a secret sharing scheme Σ, that is $\sigma(\Sigma)$ defined in the Section 2.5, which is an important parameter for efficiency of constructing secret sharing schemes. We prefer ideal secret sharing scheme, whose information ratio is 1. However, there are much more access structures that does not admit any ideal access structure. We will give a general method by using linear programming to obtain the lower bounds of secret sharing schemes for a given access structure. This method is effectively done for access structures on a small number of participants and through this method we can get the best lower bound that can be found by combinatorial method.

Recall the definition of information ratio in Section 2.5. The *optimal information* *ratio* $\sigma(\Gamma)$ 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 ratios* $\widetilde{\sigma}(\Gamma)$ is defined analogously. Moreover, in every secret sharing scheme, the length of every share is at least the length of the secret [59]. 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 [19, 31–33, 35, 42, 57, 64] among other works. And a great achievement has been obtained recently by Csirmaz and Tardos [33] by determining the optimal information ratio 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 [89]. Because of that, it is also interesting to consider the parameters $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, the infimum of the (average) information ratios of all *linear* secret sharing schemes for Γ. Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$ (We also prove it in Proposition 2.5.5). In fact, almost all known upper bounds on the optimal information ratio are upper bounds on λ, 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 be in general more efficient than the linear ones [7, 11], not many examples of access structures with $\sigma(\Gamma) < \lambda(\Gamma)$ are known.

On the other hand, Csirmaz [30] explained how most of the known lower bounds on the optimal information ratio have been found by implicitly or explicitly using a combinatorial method based on the connection between the Shannon entropy and polymatroids presented by Fujishige [46]. The best known asymptotic lower bound [30] was obtained by using this method. The parameter $\kappa(\Gamma)$ was introduced in [63] 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 information ratio.

As far as we know, $\kappa(\Gamma) = \lambda(\Gamma)$ for all access structures whose optimal information ratio $\sigma(\Gamma)$ 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 [57] to determine the optimal (average) information ratios of almost all 180 non-isomorphic access structures on five participants. The same techniques were used by van Dijk [35] to find the the optimal information ratios 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 [27, 37].

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 [32, 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 [64] and on bipartite access structures [42].

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) information ratio, 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 information ratios have not been previously determined. Several known lower bounds are improved and, in a few cases, the value of the optimal (average) information ratio is determined. After the publication of the previous version of this paper [75], Gharahi and Dehkordi [48] presented lower bounds on the optimal information ratios 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 [48] that makes it possible to determine $\sigma(\Gamma)$.

The lower bound $\kappa(\Gamma)$ on the optimal information ratio is not tight in general.

The first found examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$ were the ports of the Vámos matroid [8]. An infinite family of graph access structures with $\kappa(\Gamma) < \lambda(\Gamma)$ was presented by Csirmaz [32]. These results are proved, respectively, by using the non-Shannon information inequality by Zhang and Yeung [95] and the Ingleton inequality [54]. These and other known information inequalities, as for instance the ones in [38–40, 69], 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 [9] proved that all known non-Shannon information inequalities cannot improve our knowledge on the asymptotic behavior of the optimal (average) information ratio.

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 [38, 95], we present other examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$. As in [8], 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 information ratio equal to $\kappa(\Gamma)$. For one of them, we prove the same result for the average information ratio. In particular, this implies that the techniques used by Jackson and Martin [57] are not sufficient to determine the optimal (average) information ratios of all access structures on five participants.

4.2 Linear Programming Approach

First we recall the definition of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ in Section 2.5. For a polymatroid $\mathcal{S} = (Q, f)$ with $Q = P \cup \{p_0\}$ and $|P| = n$. Define $\sigma_{p_0} = \max\{f(\{i\}) : i \in P\}$ and $\widetilde{\sigma}(\mathcal{S}) = (1/n)\sum_{i \in P} f(\{i\})$. Then for every access structure Γ,

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \ : \ \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}, \tag{4.2.1}$$

and

$$\widetilde{\kappa}(\Gamma) = \inf\{\widetilde{\sigma}_{p_0}(\mathcal{S}) \ : \ \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}. \tag{4.2.2}$$

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 [68]. Namely, $f : \mathcal{P}(Q) \rightarrow \mathbb{R}$ 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].

4.3 New Bounds

Jackson and Martin [57] determined the optimal (average) information ratios 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 information ratios of 170 of them and the optimal average information ratios of 165 of them. The techniques used in [57] 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 information ratio. 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 [57] reduce to the 13 ones that are listed in Table 4.1, which involve access structures on $P = \{1, 2, 3, 4, 5\}$ described in the following and their duals. They are enumerated as in [57]. The lower bound on $\widetilde{\sigma}(\Gamma_{73})$ was improved by van Dijk [36]. 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 4.1: Our results for access structures on five participants

Access structure	σ from [57]	$\widetilde{\sigma}$ from [36,57]	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 [57] by determining the values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ for all those access structures.

The obtained results are given in Table 4.1. 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 [57]. 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 4.4. We also included in the table the number of constraints that define the feasible region.

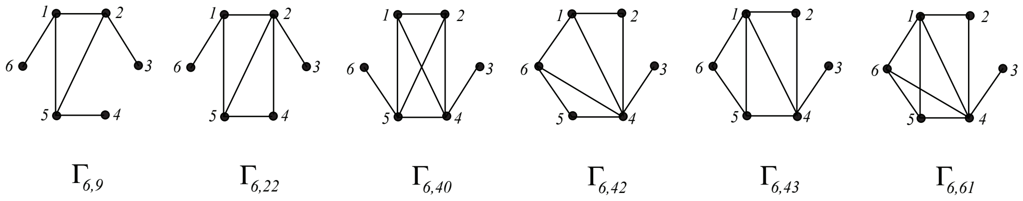

Figure 4.1: Graph access structures with six vertices.

The optimal information ratios of 94 of the 112 non-isomorphic graph access structures on six participants were determined by van Dijk [35], while lower and upper bounds were given for the remaining ones. Some of these upper bounds were improved in [27, 37]. By using linear programming, we have computed the values of $\kappa(\Gamma)$ for the 18 unsolved cases from [35], which improve the lower bounds for six of them, namely the ones in Figure 4.1. The results are shown in Table 4.2. We notice that, by mistake, we did not include the results about $\Gamma_{6,22}$ in the previous version of this paper [75]. 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 [75], Gharahi and Dehkordi [48] presented lower bounds on the optimal information ratios of all access structures in Figure 4.1 except $\Gamma_{6,9}$. Their bounds coincide with the values of $\kappa(\Gamma)$ that are given in Table 4.2, but they are proved by using the same techniques as in [35]. Moreover, they present a decomposition construction of a linear secret sharing scheme for $\Gamma_{6,61}$ that makes it possible to determine the optimal information ratio of this access structure.

Table 4.2: Our results for graph access structures on six vertices

Access structure	σ from [35]	σ from [27]	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
$\Gamma_{6,61}$	$[5/3,2]$	$[5/3,16/9]$	$7/4$	$7/4$ ([48])	707

4.4 Sharpening the Feasible Region

The lower bounds on the optimal (average) information ratio given by $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ are not tight in general. This is due to the fact that the sets in (2.5.1), (2.5.2) and (4.2.1) 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 [95] 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 [38, 40, 69]. Moreover, Zhang-Yeung inequality was used in [8] to present the first examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$. The bounds in [8] were improved in [71] by using the inequalities from [38]. 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 [54], and other such inequalities were given by Dougherty, Freiling and Zeger [39].

Beimel and Orlov [9] proved that all known non-Shannon information inequalities cannot improve our knowledge on the asymptotic behavior of the optimal (average) information ratio. Nevertheless, since all these inequalities are linear, they can be added to the linear programs that are discussed in Section 4.2. 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 (4.2.1), the sets in (2.5.1) and (2.5.2) cannot be described by a finite number of linear inequalities [39, 69], and hence the values of $\sigma(\Gamma)$ and $\lambda(\Gamma)$ cannot be only 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

$$I(f; A, B, C, D) \leq 0 \text{ for every } A, B, C, D \subseteq Q. \tag{4.4.1}$$

Moreover, according to the main result of [25], a polymatroid $\mathcal{S} = (Q, f)$ satisfies (4.4.1) 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 information ratios 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 4.2, 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 $\kappa(\Gamma_2) = \kappa(\Gamma_3) = 9/5$.

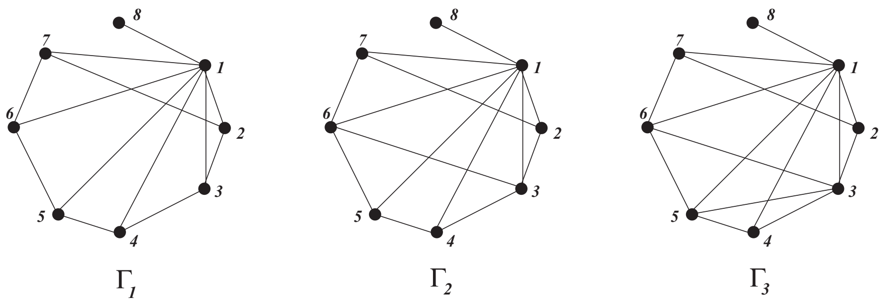

Figure 4.2: Graph access structures on 8 participants with $\kappa(\Gamma) < \lambda(\Gamma)$.

4.5 Ports of Non-representable Matroids

In this section, we use linear programming to extend the results in [8, 71, 81] about the ports of the Vámos matroid to the ports of other non-linear matroids. Seymour [81] 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 [95], lower bounds on the optimal information ratios of those access structures proving that $\sigma(\mathcal{V}_i) > \kappa(\mathcal{V}_i) = 1$ were presented in [8]. These bounds were improved in [71] by using some of the non-Shannon information inequalities given by Dougherty, Freiling and Zeger [38] (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 [8] from the Ingleton inequality. A construction given in [63] provides an upper bound on $\lambda(\mathcal{V}_i)$. Specifically, the results in [8,63,71] are summarized as follows.

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

These results were obtained without using linear programming. Nevertheless, linear programming was used in [71] 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 [73], 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.

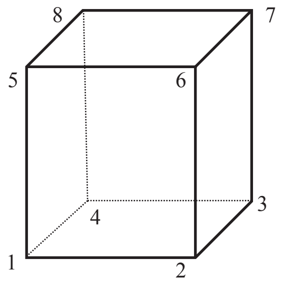

Figure 4.3: $AG(3,2)'$ and Q_8

Definition 4.5.1. *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 4.3.*

Definition 4.5.2. *The matroid Q_8 is defined on the set $V = \{1,\dots,8\}$. 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 4.3. 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 [95] implies that, for every poly-entropic polymatroid (Q, f) and for every $A, B, C, D \subseteq Q$,

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

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 4.3. In particular, these are new examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$.

Table 4.3: 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
$\mathcal{AG}_1$	$10/9$	$19/17$	$5/4$
$\mathcal{AG}_2$	$9/8$	$9/8$	$5/4$
$\mathcal{Q}_1$	$9/8$	$9/8$	$5/4$
$\mathcal{Q}_2$	$10/9$	$19/17$	$5/4$

4.6 An Impossibility Result

Since no better bounds on $\lambda(\Gamma)$ can be obtained for the access structures in Tables 4.1 and 4.2 by using Ingleton inequality, one could expect that there exist for those access structures linear secret sharing schemes with information ratio 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 information ratio equal to $\kappa(\Gamma)$. We find in Table 4.1 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 information ratio 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 information ratio. 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 4.4, are

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

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

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.

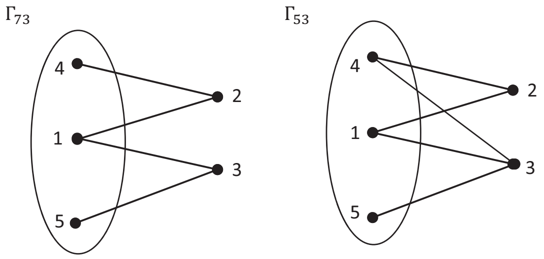

Figure 4.4: Access Structures Γ_{73} and Γ_{53}

Proposition 4.6.1. *There does not exist any linear secret sharing scheme Σ with access structure Γ_{53} or Γ_{73} with information ratio $\sigma(\Sigma) = 3/2$. There does not exist any linear secret sharing scheme Σ with access structure Γ_{73} with average information ratio $\widetilde{\sigma}(\Sigma) = 3/2$.*

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 4.6.2. We prove in Lemma 4.6.4 that these polymatroids are not poly-linear.

Definition 4.6.2. *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 4.6.3. *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 4.6.4. *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 4.6.3. Therefore $V_1 \cap V_4 = V_1 \cap V_5 = V_4 \cap V_5 \triangleq U_0$.

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 $3c \leq \dim W \leq 4c$. Indeed, on one hand,

$$\begin{aligned}
\dim W &= \dim\{[(V_1+V_2)\cap(V_2+V_4)]\cap[(V_1+V_3)\cap(V_3+V_5)]\} \\
&= \dim[(V_1+V_2)\cap(V_2+V_4)]+\dim[(V_1+V_3)\cap(V_3+V_5)] \\
&\quad -\dim\{[(V_1+V_2)\cap(V_2+V_4)]+[(V_1+V_3)\cap(V_3+V_5)]\} \\
&\leq 5c+5c-\dim[V_2+(V_1\cap V_4)]+[V_3+(V_1\cap V_5)] \\
&= 5c+5c-\dim(V_2+V_3+U_0) \\
&= 5c+5c-6c \\
&= 4c. \qquad (4.6.1)
\end{aligned}$$

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

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

$$\begin{aligned}
\dim[W\cap(V_2+V_5)] &= \dim W+\dim(V_2+V_5)-\dim(W+V_2+V_5) \\
&\leq \dim W+\dim(V_2+V_5)-\dim(V_0+V_2+V_5) \\
&\leq 4c+5c-7c \\
&= 2c. \qquad (4.6.2)
\end{aligned}$$

The other inequality is obtained by

$$\begin{aligned}
\dim[W\cap(V_2+V_5)] &= \dim\{(V_1+V_2)\cap(V_1+V_3)\cap(V_2+V_4)\\
&\quad \cap(V_3+V_5)\cap(V_2+V_5)\}\\
&= \dim\{[(V_1+V_2)\cap(V_2+V_5)\cap(V_2+V_4)]\\
&\quad \cap[(V_1+V_3)\cap(V_3+V_5)]\}\\
&\geq \dim[(V_2+U_0)\cap(V_3+U_0)]\\
&= \dim(V_2+U_0)+\dim(V_3+U_0)-\dim(V_2+V_3+U_0)\\
&= 4c+4c-6c\\
&= 2c \qquad (4.6.3)
\end{aligned}$$

In particular, all inequalities in (4.6.2) must be equalities, which implies that $\dim W = 4c$. Moreover, the inequality in (4.6.1) 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, $(V_1+V_2)\cap(V_2+V_4) \subseteq V_2+V_3+U_0$ and $(V_1+V_3)\cap(V_3+V_5) \subseteq V_2+V_3+U_0$.

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

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

$$\begin{aligned}
\dim[W \cap (V_2 + V_3)] &\geq \dim[(W \cap V_2) + (W \cap V_3)] \\
&= \dim(W \cap V_2) + \dim(W \cap V_3) - \dim(W \cap V_2 \cap V_3) \\
&\geq 2c + 2c - c \\
&= 3c \qquad (4.6.4)
\end{aligned}$$

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 4.6.7 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 [30], while the second one is proved by using the independent sequence technique [19].

Lemma 4.6.5. *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 4.6.6. *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 4.6.7. *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 4.6.6 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 4.6.5,

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

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 4.6.5 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 4.6.4 and 4.6.7 suffice to prove the first statement in Proposition 4.6.1. In order to prove the impossibility result about the average information ratio, 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 information ratio. By taking this into account, Lemma 4.6.8 concludes the proof of Proposition 4.6.1.

Lemma 4.6.8. *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 4.6.6, $f(ij) \geq 3$ 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 4.6.5,

$$f(23) + 1 \leq f(234) \leq f(23) + f(34) - f(3), \tag{4.6.5}$$

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,

$$\begin{aligned} f(124) &\leq f(12) + f(24) - f(2) - 1 \\ &\leq f(1) + f(2) + f(4) - 1 \\ &= 1/2 \times 15/2 + f(1)/2 - 1 \qquad (4.6.6) \\ &\leq 7/2. \end{aligned}$$

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

$$7/2 \leq f(1245) \leq \epsilon + f(145) \leq \epsilon + f(14) + f(15) - f(1) \leq 5 - \epsilon - f(1), \quad (4.6.7)$$

and hence $f(1) \leq 3/2 - \epsilon$. Now, inequality (4.6.6) 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 (4.6.7), 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 (4.6.7), 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 (4.6.5) 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 4.6.1. □

Chapter 5

Secret Sharing, Rank Inequalities and Information Inequalities

5.1 Introduction

This chapter deals with the problem of the size of the shares in secret sharing schemes for general access structures. The reader is referred to [5] for an up-to-date survey on this topic.

In this survey, Beimel put up with a conjecture represented in Conjecture 1.3.1, Chapter 1. However, not many results supporting this conjecture have been presented. No proof for the existence of access structures requiring shares of superpolynomial size has been found. In contrast, superpolynomial lower bounds on the size of the shares have been obtained for linear secret sharing schemes [2, 6, 47]. Because of their homomorphic properties, linear schemes are needed for many applications of secret sharing. Moreover, most of the known constructions of secret sharing schemes yield linear schemes.

Similarly to the works by Csirmaz [30] and by Beimel and Orlov [10], we analyze here the limitations of the technique that has been almost exclusively used to find lower bounds on the size of the shares. This is the case of the bounds in [18,24,30,57] and many other papers. Even though it was implicitly used before, the method was formalized by Csirmaz [30]. Basically, it consists of finding lower bounds on the solutions of certain linear programs. We have to mention that this method provides lower bounds on the information ratio of secret sharing schemes. These bound imply of course bounds on the size of the shares, but the converse does not hold. For instance, the bounds in [2, 6, 47] on the size of the shares in linear secret sharing schemes do not imply bounds on the information ratio of such schemes.

The constraints of those linear programs are derived from the fact that certain linear combinations of the values of the joint entropies of the random variables defining a secret sharing scheme must be nonnegative. These constraints can be divided into two classes.

1. The first class is formed by the constraints that are derived from the access structure. Namely, from the fact that the qualified subsets can recover the secret while the unqualified ones have no information about it.

2. The second class is formed by constraints derived from information inequalities that hold for every collection of random variables.

In the second class, the constraints derived from the Shannon inequalities 2.1.3 are always considered. These basic information inequalities are equivalent to the conditional mutual information being nonnegative, and equivalent as well to the fact that the joint entropies of a collection of random variables define a polymatroid [45,46].

Csirmaz [30] proved that, by taking only the Shannon inequalities in the second class, one obtains lower bounds that are at most linear on the number of participants. This was proved by showing that every such linear program admits a small solution.

One may expect that better lower bounds should be obtained by adding to the second class new constraints derived from the non-Shannon information inequalities. The existence of such inequalities was unknown when Csirmaz [30] formalized that method. When dealing with linear secret sharing schemes, one can improve the linear program by using rank inequalities, which apply to configurations of vector subspaces or, equivalently, to the joint entropies of collections of random variables defined from linear maps. It is well-known that every information inequality is also a rank inequality. Indeed, better lower bounds on the information ratio have been found for some families of access structures by using non-Shannon information and rank inequalities [8,32,71,75].

Nevertheless, Beimel and Orlov [10] presented a negative result about the power of non-Shannon information inequalities to provide better general lower bounds on the size of the shares. Specifically, they proved that the best lower bound that can be obtained by using all information inequalities on four and five variables, together with all inequalities on more than five variables that are known to date, is at most linear on the number of participants. Specifically, they proved that every linear program that is obtained by using these inequalities admits a small solution that is related to the solution used by Csirmaz [30] to prove his negative result. They used the fact that there exists a finite set of rank inequalities that, together with the Shannon inequalities, span all rank inequalities, and hence all information inequalities, on four or five variables [39,50]. By executing a brute-force algorithm using a computer program, they checked that Csirmaz's solution is compatible with every rank inequality in that finite set. In addition, they manually executed their algorithm on a symbolic representation of the infinite sequence of information inequalities given by Zhang [94]. This sequence contains inequalities on arbitrarily many variables and generalizes the infinite sequences from previous works.

In particular, the results in [10] imply that all rank inequalities on four or five variables cannot provide lower bounds on the size of shares in *linear* secret sharing schemes that are better than linear on the number of participants. Unfortunately, their algorithm is not efficient enough to be applied on the known rank inequalities on six variables.

We present here another negative result about the power of information inequalities to provide general lower bounds on the size of the shares in secret sharing schemes. Namely, we prove that, for every $r \geq 3$, the best lower bound that can be obtained by using all rank inequalities on at most r variables is polynomial on the number of participants. Since all information inequalities are rank inequalities, this negative result applies to the search of lower bounds for both linear and general secret sharing schemes. Therefore, information inequalities on arbitrarily many variables are needed to find superpolynomial lower bounds by using the method described above.

The proof is extremely simple and concise. Similarly to the proofs in [10, 30], it is based on finding small solutions to the linear programs that are obtained by using rank inequalities on a bounded number of variables. These solutions are obtained from a family of polymatroids that are uniform and Boolean. This family contains the polymatroids that were used in [10, 30].

In some sense, our results are weaker than the ones in [10], because for $r = 4$ and $r = 5$, our solutions to the linear programs do not prove that the lower bounds must be linear on the number of participants, but instead quadratic and cubic, respectively. Nevertheless, our result is much more general because it applies to all (known or unknown) rank inequalities.

In addition, we present another proof of Beimel and Orlov's result [10] on the limitations of non-Shannon information inequalities. We use the fact that many of the known rank inequalities can be derived from the so-called *common information property* of linear polymatroids, as it is mentioned in [39]. We prove that a wider family of inequalities cannot provide lower bounds that are better than cubic on the number of participants. Our proof does not require computer explorations and, more importantly, it provides an explanation to the limitations of non-Shannon information inequalities, and hence we shed some light on the search of better asymptotic lower bounds.

5.2 A Family of Uniform Boolean Polymatroids

We present a family of polymatroids that are uniform and Boolean. In addition, every member of this family is compatible to all access structure on its ground set.

The following results are straightforward consequences of Proposition 2.5.3.

Proposition 5.2.1. *A polymatroid $\mathcal{S}_P = (P, f)$ is compatible with all access structures on P if and only if the following conditions are satisfied.*

1. *If $X \subseteq P$ and $z \in P \smallsetminus X$, then $f(X) \le f(X \cup \{z\}) - 1$.*
2. *If $X \subseteq P$ and $y, z \in P \smallsetminus X$, then $f(X \cup \{y, z\}) + f(X) \le f(X \cup \{y\}) + f(X \cup \{z\}) - 1$.*

Proposition 5.2.2. *Let P be a set with $|P| = n$ and let $\mathcal{S}_P$ be a uniform polymatroid on P. Then $\mathcal{S}_P$ is compatible with all access structures on P if and only if its increment vector $(\delta_1, \ldots, \delta_n)$ is such that $\delta_i \ge \delta_{i+1} + 1$ for $i = 1, \ldots, n-1$ and $\delta_n \ge 1$.*

Given a set P and an integer $r \ge 2$, let $M(P, r)$ be the set of all multisets of size r from the set P. For example, if $P = \{a, b, c\}$, then

$$M(P, 3) = \{aaa, aab, aac, abb, abc, acc, bbb, bbc, bcc, ccc\}.$$

Observe that $|M(P, r)| = \binom{n+r-1}{r}$ if $|P| = n$. For every $x \in P$, let $M_x(P, r)$ be the set of the multisets in $M(P, r)$ that contain x. In the previous example,

$$M_a(P, 3) = \{aaa, aab, aac, abb, abc, acc\}.$$

Finally, we define $\mathcal{Z}(P, r) = (P, f)$ as the Boolean polymatroid on P defined by the family $(M_x(P, r))_{x \in P}$ of subsets of $M(P, r)$. As usual, we notate $M_X(P, r) = \bigcup_{x \in X} M_x(P, r)$ for every $X \subseteq Q$.

Clearly, every permutation on P is an automorphism of $\mathcal{Z}(P,r)$, and hence this polymatroid is uniform. For every $X \subseteq P$, the multisets in $M(P,r) \smallsetminus M_X(P,r)$ are the ones involving only elements in $P \smallsetminus X$. That is, $M(P,r) \smallsetminus M_X(P,r) = M(P \smallsetminus X, r)$, and hence

$$\begin{aligned} f(X) &= |M_X(P,r)| = |M(P,r)| - |M(P \smallsetminus X, r)| \\ &= \binom{|P| + r - 1}{r} - \binom{|P| - |X| + r - 1}{r}. \end{aligned}$$

Therefore, if $|P| = n$, the increment vector $(\delta_1, \ldots, \delta_n)$ of $\mathcal{Z}(P,r)$ is given by

$$\delta_i = \binom{n-i+r}{r} - \binom{n-i+r-1}{r} = \binom{n-i+r-1}{r-1}$$

for every $i = 1, \ldots, n$. Observe that $\delta_1 > \cdots > \delta_n > 0$, and hence $\mathcal{Z}(P,r)$ is compatible with all access structures on P. In particular, $\delta_i = n - i + 1$ if $r = 2$, and hence $\kappa(\Gamma) \leq n$ for every access structure Γ on n participants [30]. The *Csirmaz function* introduced in [10, Definition 3.10] coincides with the rank function of $\mathcal{Z}(P,2)$. The rank function of $\mathcal{Z}(P,2)$ is the smallest among the rank functions of all uniform polymatroids on P that are compatible with all access structures on P [10, Lemma 3.11]. Finally, observe that [10, Lemma 6.2] is a straightforward consequence of the fact that $\mathcal{Z}(P,2)$ is a Boolean polymatroid.

5.3 On Rank Inequalities on a Bounded Number of Variables

This section is devoted to prove our main result, Theorem 5.3.3.

We need the following technical result, which is a consequence of [10, Lemma 4.3]. Recall Definition 2.2.2 of rank inequality, first define $[r] = \{1, 2, \dots, r\}$ as a finite index, and then$(\alpha_I)_{I \in \mathcal{P}([r])}$ defines a rank inequality.

Lemma 5.3.1. *Let $(\alpha_I)_{I \in \mathcal{P}([r])}$ be a rank inequality. Then $\sum_{I : I \cap J \neq \varnothing} \alpha_I \geq 0$ for every $J \subseteq [r]$.*

Proof. Take $J \subseteq [r]$ and the family $(M_i)_{i \in [r]}$ of sets given by $M_i = \{0\}$ if $i \in J$ and $M_i = \varnothing$ otherwise. Let $([r], f)$ be the Boolean polymatroid defined by this family. Then $\sum_{I : I \cap J \neq \varnothing} \alpha_I = \sum_{I \subseteq [r]} \alpha_I f(I) \geq 0$ because Boolean polymatroids are linearly representable. □

Proposition 5.3.2. *Let P be a set of n participants, Γ an access structure on P, $r \geq 3$ an integer, and $\mathcal{Z}_{r-1} = \mathcal{Z}(P, r-1)$. Then the Γ-polymatroid $\mathcal{Z}_{r-1}(\Gamma)$ that is an extension of $\mathcal{Z}_{r-1}$ to $Q = P \cup \{p_0\}$ satisfies all rank inequalities on r variables.*

Proof. Let f be the rank function of $\mathcal{Z}_{r-1}(\Gamma)$ and $(\alpha_I)_{I \in \mathcal{P}([r])}$ a rank inequality on r variables. We have to prove that $\sum_{I \subseteq [r]} \alpha_I f(A_I) \geq 0$ for every r subsets $(A_i)_{i \in [r]}$ of Q. Take $B_i = A_i \smallsetminus \{p_0\}$. If $B_i \in \Gamma$ for every $i \in [r]$, then $\sum_{I \subseteq [r]} \alpha_I f(A_I) = \sum_{I \subseteq [r]} \alpha_I f(B_I) \geq 0$ because $\mathcal{Z}_{r-1}$ is Boolean. If $B_{[r]} \notin \Gamma$, then

$$\sum_{I \subseteq [r]} \alpha_I f(A_I) = \sum_{I \subseteq [r]} \alpha_I f(B_I) + \sum_{I : p_0 \in A_I} \alpha_I \geq 0$$

by Lemma 5.3.1 with $J = \{i \in [r] : p_0 \in A_i\}$. From now on, we assume that $B_{[r]} \in \Gamma$ and that $B_i \notin \Gamma$ for some $i \in [r]$.

Consider the polymatroid $\mathcal{S} = ([r], g)$ determined by $g(I) = f(B_I)$ for every $I \subseteq [r]$. In addition, consider the access structure Λ on $[r]$ formed by the sets $I \subseteq [r]$ such that $B_I \in \Gamma$. We prove next that $\mathcal{S}$ can be extended to a linearly representable Λ-polymatroid $\mathcal{S}(\Lambda) = ([r] \cup \{0\}, g)$. This concludes the proof. Indeed, since $\mathcal{S}(\Lambda)$ is a Λ-polymatroid, $f(A_I) = g(I \cup \{0\})$ if $p_0 \in A_I$, and hence

$$\begin{aligned}\sum_{I \subseteq [r]} \alpha_I f(A_I) &= \sum_{I : p_0 \notin A_I} \alpha_I f(B_I) + \sum_{I : p_0 \in A_I} \alpha_I f(A_I) \\ &= \sum_{I : p_0 \notin A_I} \alpha_I g(I) + \sum_{I : p_0 \in A_I} \alpha_I g(I \cup \{0\}).\end{aligned}$$

Consider the family $(C_i)_{i \in [r]}$ of subsets of $[r] \cup \{0\}$ given by $C_i = \{i, 0\}$ if $p_0 \in A_i$ and $C_i = \{i\}$ otherwise. Then

$$\sum_{I : p_0 \notin A_I} \alpha_I g(I) + \sum_{I : p_0 \in A_I} \alpha_I g(I \cup \{0\}) = \sum_{I \subseteq [r]} \alpha_I g(C_I) \geq 0$$

because $\mathcal{S}(\Lambda)$ is linearly representable.

The polymatroid $\mathcal{S}$ is Boolean. Indeed, take $M = M(P, r-1)$ and $M_X = M_X(P, r-1)$ for every $X \subseteq P$. Then $(M_{B_i})_{i \in [r]}$ is a Boolean representation of $\mathcal{S}$. Therefore, this polymatroid is linearly representable over every field, as proved in Subsection 2.3.1. For a field $\mathbb{K}$, take a basis $(\mathbf{e}^w)_{w \in M}$ of $\mathbb{K}^M$. Then the subspaces $(V_i)_{i \in [r]}$ with $V_i = \langle \mathbf{e}^w : w \in M_{B_i} \rangle$ form a $\mathbb{K}$-linear representation of $\mathcal{S}$.

Consider the dual access structure $\Lambda^* = \{J \subseteq [r] : [r] \smallsetminus J \notin \Lambda\}$. Take $J \in \min \Lambda^*$ and $I = [r] \smallsetminus J$. Observe that $B_I \notin \Gamma$ and $B_I \cup B_j \in \Gamma$ for every $j \in J$.

In particular, this implies that $J \neq \emptyset, [r]$. Therefore, we can take an element $x_j \in B_j \smallsetminus B_I$ for every $j \in J$. Consider a multiset $w_J \in M(P, r-1)$ containing exactly the elements in $\{x_j : j \in J\}$, repeating some of them if necessary. Take the vector

$$\mathbf{v}_0 = \sum_{J \in \min \Lambda^*} \mathbf{e}^{w_J} \in \mathbb{K}^M$$

and the subspace $V_0 = \langle \mathbf{v}_0 \rangle$. By adding this subspace to the collection $(V_i)_{i \in [r]}$, an extension $\mathcal{S}(\Lambda) = ([r] \cup \{0\}, g)$ of $\mathcal{S}$ is obtained. Obviously, $\mathcal{S}(\Lambda)$ is $\mathbb{K}$-linearly representable.

Finally, we prove that $\mathcal{S}(\Lambda)$ is a Λ-polymatroid. Clearly, $I \in \Lambda$ if and only if $I \cap J \neq \emptyset$ for every $J \in \min \Lambda^*$. If $I \in \Lambda$, then $w_J \in M_{B_I}(P, r-1)$ for every $J \in \min \Lambda^*$. Indeed, if $j \in I \cap J$, the element x_j in the multiset w_J is also in B_I. Therefore, $\mathbf{e}^{w_J} \in V_I$ for every $J \in \min \Lambda^*$, and hence $\mathbf{v}_0 \in V_I$ and $g(I \cup \{0\}) = g(I)$. Suppose now that $I \notin \Lambda$ and take $J \in \min \Lambda^*$ with $I \cap J = \emptyset$. Then $w_J \notin M_{B_I}(P, r-1)$ because $x_j \notin B_I$ for every $j \in J$. Therefore, $\mathbf{v}_0 \notin V_I$ and $g(I \cup \{0\}) = g(I) + 1$. □

Theorem 5.3.3. *For an access structure Γ on n participants, the best lower bound on $\lambda(\Gamma)$ that can be obtained by using rank inequalities on r variables is at most*

$$\binom{n+r-3}{r-2}, \tag{5.3.1}$$

and hence $O(n^{r-2})$. As an immediate consequence, the same applies to the lower bounds on the optimal information ratio $\sigma(\Gamma)$ that are obtained by using information inequalities on r variables.

Proof. By Proposition 5.3.2, the polymatroid $\mathcal{Z}_{r-1}(\Gamma)$ is a feasible solution to any linear program that is obtained from rank inequalities on r variables. Therefore, every lower bound on $\lambda(\Gamma)$ derived from such a linear program is at most $\sigma_{p_0}(\mathcal{Z}_{r-1}(\Gamma)) = \delta_1$, where δ_1 is the first component of the increment vector of $\mathcal{Z}(P, r-1)$. □

Observe that we are not assuming $r \leq n$ in Theorem 5.3.3. A smaller value for the bound (5.3.1) can be proved for the case $r \leq n$ by using in the same way the uniform Boolean polymatroid defined by the set M of all subsets (instead of multisets) of P with at most $r-1$ participants and the subsets $(M_x)_{x \in P}$, where M_x consists of the subsets in M that contain x. Nevertheless, asymptotically the new bound is not better than $O(n^{r-2})$.

5.4 On Rank Inequalities Derived from Common Informations

In this section, we introduce common information first, and then devote to prove main result Theorem 5.4.8. From now on, we use a more compact notation for unions of sets. So, we write XY for $X \cup Y$ Xx for $X \cup \{x\}$, and also xy for $\{x, y\}$.

5.4.1 Common Information Defined on Polymatroids

Given two random variables S_1 and S_2, We say that a random variable S_3 *conveys the common information* of the random variables S_1 and S_2 if $H(S_3|S_2) = H(S_3|S_1) = 0$ and $H(S_3) = I(S_1; S_2)$. In general, it is not possible to find a random variable conveying the common information of two given random variables. Nevertheless, if $S_1 = S|_{V_1}$ and $S_2 = S|_{V_2}$ for some vector subspaces $V_1, V_2 \subseteq E$, then $S_3 = S|_{V_1 \cap V_2}$ conveys the common information of S_1 and S_2.

Because of the connection between polymatroids and the Shannon entropy given by Theorem 2.3.3 and by analogy to the conditional entropy, we write $f(X|Y) = f(X \cup Y) - f(Y)$ if f is the rank function of a polymatroid. Clearly,

$$f(X_1 \cup \cdots \cup X_r) = \sum_{i=1}^{r} f(X_i | X_1 \cup \cdots \cup X_{i-1}) \tag{5.4.1}$$

for all $X_1, \ldots, X_r \subseteq Q$. Obviously, $f(X|Y) \geq 0$ and submodularity implies that $f(X|Y \cup Z) \leq f(X|Y)$. Moreover, $f(X|Y \cup Z) = f(X|Y)$ if $f(Z|Y) = 0$. The following definition is motivated by the concept of common information of a pair of random variables. Some basic properties that will be used later are given in Proposition 5.4.2.

Definition 5.4.1. *Consider a polymatroid $\mathcal{S} = (Q, f)$ and two sets $A, B \subseteq Q$. Then every $x_0 \in Q$ such that*

- $f(\{x_0\}|A) = f(\{x_0\}|B) = 0$ *and*
- $f(\{x_0\}) = f(A) + f(B) - f(A \cup B)$

is called a common information of the pair (A, B).

Proposition 5.4.2. *Let $\mathcal{S} = (Q, f)$ be a polymatroid, $A, B \subseteq Q$, and $x_0 \in Q$ a common information of (A, B). Consider a subset $Y \subseteq Q$ such that $f(Y|A) = f(Y|B) = 0$. Then $f(Y) \leq f(\{x_0\})$ and $f(Y|\{x_0\}) = 0$.*

Proof. By Equation (5.4.1), each of the following quantities is equal to $f(ABY)$.

$$f(A) + f(Y|A) + f(B|AY) \tag{5.4.2}$$

$$f(B) + f(Y|B) + f(A|BY) \tag{5.4.3}$$

$$f(A \cup B) + f(Y|AB) \tag{5.4.4}$$

$$f(Y) + f(AB|Y) \tag{5.4.5}$$

By equaling the sum of (5.4.2) and (5.4.3) to the sum of (5.4.4) and (5.4.5),

$$f(Y) = f(A) + f(B) - f(AB) + f(B|AY) + f(A|BY) - f(AB|Y).$$

Therefore, $f(Y) \leq f(\{x_0\})$ because $f(AB|Y) = f(B|Y) + f(A|BY) \geq f(B|AY) + f(A|BY)$. Finally, $f(Yx_0) \leq f(\{x_0\})$ because $f(Yx_0|A) = f(Yx_0|B) = 0$, and hence $f(Y|\{x_0\}) = 0$. □

Let $(V_x)_{x\in Q}$ be a collection of vector subspaces representing a $\mathbb{K}$-linear polymatroid $\mathcal{S} = (Q, f)$, and consider two subsets $A, B \subseteq Q$. By taking $V_{x_0} = V_A \cap V_B$, an extension of $\mathcal{S}$ to $Q \cup \{x_0\}$ is obtained in which x_0 is a common information of A and B. Obviously, this new polymatroid is $\mathbb{K}$-linear as well. In particular, if $\mathcal{S} = (Q, f)$ is a Boolean polymatroid defined by a family $(M_x)_{x\in Q}$ of sets, then the extension of $\mathcal{S}$ to $Q \cup \{x_0\}$ given by $M_{x_0} = M_A \cap M_B$ is a Boolean polymatroid in which x_0 is a common information of A and B.

Definition 5.4.3. *Let k be a positive integer. A polymatroid $\mathcal{S} = (Q, f)$ satisfies the* k-common information property *if, for every k pairs $(A_{i0}, A_{i1})_{i\in[k]}$ of subsets of Q, there* *exists an extension* $(Qy_1 \dots y_k, f)$ *of* $\mathcal{S}$ *such that* y_i *is a common information of* (A_{i0}, A_{i1}) *for every* $i \in [k]$.

Clearly, a poly-linear polymatroid satisfies the k-common information property for every k. Every rank inequality on four variables is a combination of the Shannon inequalities and the Ingleton inequality [50]. If a polymatroid satisfies the 1-common information property, then it satisfies the Ingleton inequality [39], and hence it satisfies all information inequalities on 4 variables. Moreover, there exist 24 rank inequalities on five variables that, together with the Ingleton and Shannon inequalities, generate all rank inequalities on five variables [39]. All these inequalities are satisfied by every polymatroid with the 2-common information property [39], and hence such polymatroids satisfy all information inequalities on 5 variables. In addition, this holds for all known infinite families of rank inequalities on an arbitrary number of variables [39]. Moreover, according to [39], all known rank inequalities are derived from the 2-common information property.

5.4.2 On Rank Inequalities Derived from 2-Common Information Property

Let P be a set of n participants, Γ an access structure on P, and $\mathcal{Z} = \mathcal{Z}(P,4)$. Consider the Γ-polymatroid $\mathcal{Z}(\Gamma)$ that is an extension of $\mathcal{Z}$ to $Q = P \cup \{p_0\}$. Take $M = M(P,4)$ and $M_x = M_x(P,4)$ for every $x \in P$. Then $(M_x)_{x \in P}$ is a boolean representation of $\mathcal{Z} = \mathcal{Z}(P,4) = (P,f)$. Consider a collection $(B_{i0}, B_{i1})_{i \in [k]}$ of pairs of subsets of P Consider the Boolean extension $\mathcal{S} = (P \cup \{y_1, \dots, y_k\}, f)$ of $\mathcal{Z}$ that is given by the sets $M_{y_i} = M_{B_{i0}} \cap M_{B_{i1}}$ for $i \in [k]$. Then y_i is a common information of (B_{i0}, B_{i1}) in $\mathcal{S}$. Consider the extension of Γ to $P \cup \{y_1, \ldots, y_k\}$ such that, for every $X \subseteq P$ and $\{i_1, \ldots, i_s\} \subseteq [k]$, the set $Xy_{i_1} \ldots y_{i_s}$ is qualified if and only if $XB_{i_1 j_1} \ldots B_{i_s j_s} \in \Gamma$ for every $(j_1, \ldots, j_s) \in \{0,1\}^s$. We use Γ to denote as well this extended access structure.

Lemma 5.4.4. *Let $(M_x)_{x \in Q}$ be a Boolean representation of a polymatroid (Q, f) and X, Y, Z disjoint subsets of Q. Then $f(XYZ) + f(X) = f(XY) + f(XZ)$ if and only if $M_Y \cap M_Z \subseteq M_X$*

Proof. Observe that $M_Y \cap M_Z \subseteq M_X$ if and only if $M_X \cap M_Z = M_{XY} \cap M_Z$. In addition, $|M_X \cap M_Z| = f(X) + f(Z) - f(XZ)$ while $|M_{XY} \cap M_Z| = f(XY) + f(Z) - f(XYZ)$. □

Lemma 5.4.5. *The polymatroid $\mathcal{S}$ and the access structure Γ on $P \cup \{y_1, \ldots, y_k\}$ are compatible.*

Proof. We begin by checking that the first condition in Proposition 2.5.3 is satisfied. Take $\widehat{P} = P \cup \{y_1, \ldots, y_k\}$ and consider $X \subseteq \widehat{P}$ and $y \in \widehat{P}$ such that $X \notin \Gamma$ and $Xy \in \Gamma$. Without loss of generality, we can assume that $X = Yy_1 \ldots y_s$ for some $Y \subseteq P$ and $0 \leq s \leq k$, and that $YB_{10} \ldots B_{s0} \notin \Gamma$. If $y \in P$, then $y \notin YB_{10} \ldots B_{s0}$, and hence $yyyy \in M_z \smallsetminus M_X$. If $y \notin P$, then $s < k$ and we can assume $y = y_k$. Then $YB_{10} \ldots B_{s0}B_{kj}$ is qualified for $j = 0, 1$. Therefore, there exist $u_j \in B_{kj} \smallsetminus YA_{10} \ldots A_{s0}$ for $j = 0, 1$ and $u_0u_0u_1u_1 \in M_y \smallsetminus M_X$. Therefore, $f(X) \leq f(Xy) - 1$.

We proceed now to check the second condition in Proposition 2.5.3. Consider $X \subseteq \widehat{P}$ and $y, z \in \widehat{P}$ are such that $X \notin \Gamma$ and $Xy, Xz \in \Gamma$, As before, we can assume that $X = Yy_1 \ldots y_s$ for some $Y \subseteq P$ and $0 \leq s \leq k$, and that $YB_{10} \ldots B_{s0} \notin \Gamma$. If $y, z \in P$, then $y, z \notin YB_{10} \ldots B_{s0}$, and hence $yyzz \in (M_y \cap M_z) \smallsetminus M_X$. If $y \notin P$

and $z \in P$, we can assume that $y = y_k$. Then there exist $u_j \in B_{kj} \smallsetminus YB_{10} \dots B_{s0}$ for $j = 0, 1$ and $u_0u_1zz \in (M_y \cap M_z) \smallsetminus M_X$. If $y, z \notin P$, we can assume that $y = y_{k-1}$ and $z = y_k$ Then $u_0u_1v_0v_1 \in (M_y \cap M_z) \smallsetminus M_X$ if $u_j \in B_{(k-1)j} \smallsetminus YB_{10} \dots B_{s0}$ and $v_j \in B_{kj} \smallsetminus YB_{10} \dots B_{s0}$. Therefore, $f(Xyz) + f(X) \leq f(Xy) + f(Xz) - 1$ by Lemma 5.4.4. □

Proposition 5.4.6. *Let Γ be an access structure on P and $(B_{i0}, B_{i1})_{i\in[k]}$ a collection of pairs of subsets of P. Take $\mathcal{Z} = \mathcal{Z}(P, 4)$. Then there exists a polymatroid $(Q \cup \{y_1, \dots, y_k\}, f)$, extension of $\mathcal{Z}(\Gamma)$, such that y_i is a common information of (B_{i0}, B_{i1}) for every $i \in [k]$.*

Proof. The polymatroid $\mathcal{S}(\Gamma)$ satisfies the required properties. □

Observe that Proposition 5.4.6 does not imply that $\mathcal{Z}(\Gamma)$ satisfies the k-common information property, because the existence of common informations is guaranteed only for pairs of subsets of P but not for pairs of subsets of Q. Some additional difficulties appear when dealing with pairs of subsets involving the element p_0. We discuss this issue in the following.

For a subset $X \subseteq Q$, a polymatroid (Q, f) can be extended to (Qx, f) by taking $f(Yx) = f(YX)$ for every $Y \subseteq Q$. In this case, we say that the element x is *identified* to the subset X.

Lemma 5.4.7. *Consider a pair (A_0, A_1) of subsets of Q with $p_0 \in A_0 \cap A_1$ and take $B_j = A_j \smallsetminus \{p_0\}$. Let (Q, g) be a Γ-polymatroid and let (Qy, g) be an extension such that y is a common information of (B_0, B_1). Finally, consider the polymatroid (Qyx, g), where x is identified to yp_0.*

1. *If both B_0 and B_1 are qualified, then y is a common information of the pairs (A_0, B_1), (A_1, B_0), and (A_0, A_1).*

2. *If $B_0 \in \Gamma$ and $B_1 \notin \Gamma$, then y is a common information of (A_0, B_1) and x is a common information of both (B_0, A_1) and (A_0, A_1).*

3. *If $B_0 \cup B_1 \notin \Gamma$, then y is a common information of both (A_0, B_1) and (A_1, B_0), while x is a common information of (A_0, A_1).*

Proof. Take $\Delta = g(A_0) + g(A_1) - g(A_0A_1) - (g(B_0) + g(B_1) - g(B_0B_1))$. If $B_0, B_1 \in \Gamma$, then $\Delta = 0$, and hence y is a common information of (A_0, A_1). Clearly, this implies that y is as well a common information of (A_0, B_1) and (A_1, B_0). On the other hand, $\Delta = 1$ if $B_0 \in \Gamma$ and $B_1 \notin \Gamma$. Obviously, $f(\{x\}|A_j) = f(yp_0|A_j) = 0$ for $j = 0, 1$. In addition, $f(\{x\}) = f(\{y\}) + 1$ because $f(\{x\}) = f(yp_0) = f(\{y\}) + f(\{p_0\}|\{y\})$ and $f(\{p_0\}|\{y\}) \geq f(\{p_0\}|B_1) = 1$. Therefore, x is a common information of (A_0, A_1). The other statements are proved analogously. □

One situation is missing in in Lemma 5.4.7, namely $B_0, B_1 \notin \Gamma$ and $B_0 \cup B_1 \in \Gamma$. In this case, none of the elements y, x considered in Lemma 5.4.7 is a common information of (A_0, A_1). A method to find such a common information is given in the proof of Theorem 5.4.8, the main result in this section. Observe that, for every $\alpha \geq 1$, the polymatroid $\alpha\mathcal{Z}(P, 4)$ is compatible with all access structures on P.

Theorem 5.4.8. *Take $\mathcal{Z}' = \alpha\mathcal{Z}(P, 4)$ for some large enough integer $\alpha \geq 1$. For every access structure Γ on P, the polymatroid $\mathcal{Z}'(\Gamma)$ satisfies the 2-common information property.*

Proof. Consider two pairs $(A_{i0}, A_{i1})_{i \in [2]}$ of subsets of Q and take $B_{ij} = A_{ij} \smallsetminus \{p_0\}$. For the pairs $(B_{i0}, B_{i1})_{i \in [2]}$, consider the extension $\mathcal{S} = (Py_1y_2, f)$ of $\mathcal{Z} = \mathcal{Z}(P, 4) = (P, f)$ and the extension of Γ to Py_1y_2 as defined at the beginning of this section. Recall that y_i is a common information of (B_{i0}, B_{i1}) for $i = 1, 2$ and that the polymatroid $\mathcal{S}$ is compatible with the access structure Γ. Obviously, these properties hold as well for the polymatroid $\mathcal{T} = \alpha\mathcal{S} = (Py_1y_2, g)$, which is an an extension of $\mathcal{Z}' = \alpha\mathcal{Z} = (P, g)$. If each of the pairs $(B_{i0}, B_{i1})_{i\in[2]}$ is in one of the cases considered in Lemma 5.4.7 (or the symmetric ones), then there exists an extension (Qx_1x_2, g) of $\mathcal{Z}'(\Gamma)$ such that x_i is a common information of (A_{i0}, A_{i1}) for $i = 1, 2$.

Assume that $p_0 \in A_{10}$ and $B_{10}, B_{11} \notin \Gamma$ while $B_{10} \cup B_{11} \in \Gamma$. Assume as well that $p_0 \notin A_{2j}$ for $j = 0, 1$, or $B_{20} \in \Gamma$, or $B_{20} \cup B_{21} \notin \Gamma$. Then, by Lemma 5.4.7, we can extend $\mathcal{Z}'(\Gamma)$ to Qy_1x_2, being x_2 a common information of (A_{20}, A_{21}). Extend $\mathcal{Z}'$ to Pz_1y_2 by taking, for every $X \subseteq Py_2$,

- $g(Xz_1) = g(Xy_1)$ if $XB_{10} \in \Gamma$, and
- $g(Xz_1) = g(Xy_1) + 1$ otherwise.

In addition, consider the extension of Γ to Pz_1y_2 such that, for every $X \subseteq Py_2$, the set Xz_1 is qualified if and only if $XB_{11} \in \Gamma$. We prove next that (Pz_1y_2, g) is indeed a polymatroid and that it is compatible with Γ. By combining Propositions 2.3.7 and 2.5.3, we have to prove the following claim.

Claim 5.4.9. *For every $X \subseteq Pz_1y_2$ and $y, z \in Pz_1y_2 \smallsetminus X$,*

$$g(Xyz) + g(X) \leq g(Xy) + g(Xz) - \delta,$$

where $\delta = 1$ if $X \notin \Gamma$ and $Xy, Xz \in \Gamma$, and $\delta = 0$ otherwise.

Once this claim is proved, it is not difficult to check that z_1 is a common information of (A_{10}, B_{11}). Indeed, since $B_{10}z_1 \in \Gamma$, we have that $g(A_{10}z_1) = g(B_{10}z_1) = g(B_{10}y_1) + 1 = g(B_{10}) + 1 = g(A_{10})$. In addition, $g(B_{11}z_1) = g(B_{11}y_1) = g(B_{11})$. Moreover, $g(\{z_1\}) = g(\{y_1\}) + 1 = g(B_{10}) + g(B_{11}) - g(B_{10}B_{11}) + 1 = g(A_{10}) + g(B_{11}) - g(A_{10}B_{11})$. In conclusion, z_1 is a common information of (A_{10}, B_{11}). In addition, if $p_0 \in A_{11}$, a common information x_1 of (A_{10}, A_{11}) is obtained by identifying x_1 to z_1p_0.

Assume now that $p_0 \in A_{i0}$ and $B_{i0}, B_{i1} \notin \Gamma$ while $B_{i0} \cup B_{i1} \in \Gamma$ for $i = 1, 2$. An element z_2 that is a common information of (A_{20}, B_{21}) in (Qy_1z_2, g) is obtained by symmetry. At this point, we have to extend $\mathcal{Z}'$ and Γ to Pz_1z_2 in some way that is compatible with the previous extensions. This is done as follows. For each set $X \subseteq P$, Let $N(X)$ be the number of pairs $(j,k) \in \{0,1\}^2$ such that $XB_{1j}B_{2k} \in \Gamma$. The following requirements define extensions of $\mathcal{Z}'$ and Γ to Pz_1z_2.

- If $N(X) = 0, 1$, then $g(Xz_1z_2) = g(Xy_1y_2) + 2$ and $Xz_1z_2 \notin \Gamma$.
- If $N(X) = 2$ and $XB_{11}B_{21} \notin \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2) + 1$ and $Xz_1z_2 \notin \Gamma$.
- If $N(X) = 2$ and $XB_{11}B_{21} \in \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2) + 2$ and $Xz_1z_2 \in \Gamma$.
- If $N(X) = 3$ and $XB_{11}B_{21} \notin \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2)$ and $Xz_1z_2 \notin \Gamma$.
- If $N(X) = 3$ and $XB_{11}B_{21} \in \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2) + 1$ and $Xz_1z_2 \in \Gamma$.
- If $N(X) = 4$, then $g(Xz_1z_2) = g(Xy_1y_2)$ and $Xz_1z_2 \in \Gamma$.

The last step in the proof is to check that (Pz_1z_2, g) is a polymatroid that is compatible with Γ. That is, we have to prove the following claim.

Claim 5.4.10. *For every $X \subseteq Pz_1z_2$ and $y, z \in Pz_1z_2 \smallsetminus X$,*

$$g(Xyz) + g(X) \leq g(Xy) + g(Xz) - \delta,$$

where $\delta = 1$ if $X \notin \Gamma$ and $Xy, Xz \in \Gamma$, and $\delta = 0$ otherwise.

In order to proof the two claims, we follow the same strategy. For a subset $X \subseteq Py_1y_2z_1z_2$, we notate $\overline{X}$ for the subset of Py_1y_2 that is obtaining by substituting z_i by y_i. We consider

- $\Delta_g(X, y, z) = g(Xy) + g(Xz) - g(Xyz) - g(X)$, and
- $\varepsilon = \Delta_g(X, y, z) - \Delta_g(\overline{X}, \overline{y}, \overline{z})$.

Then $\Delta_g(X, y, z) = \Delta_g(\overline{X}, \overline{y}, \overline{z}) + \varepsilon = \alpha\Delta_f(\overline{X}, \overline{y}, \overline{z}) + \varepsilon$. Since $\Delta_f(\overline{X}, \overline{y}, \overline{z}) \geq 0$, the claims are proved by checking that $\varepsilon \geq \delta$ if $\Delta_f(\overline{X}, \overline{y}, \overline{z}) = 0$. Recall that $\Delta_f(\overline{X}, \overline{y}, \overline{z}) = 0$, if and only if $M_{\overline{y}} \cap M_{\overline{z}} \subseteq M_{\overline{X}}$.

First, we prove Claim 5.4.9 by considering three cases.

Case 1. $y = z = z_1$. Then $\varepsilon = g(Xz_1) - g(Xy_1) \geq 0$. If $\delta = 1$ and $\varepsilon = 0$, then $X \notin \Gamma$ and $Xy_1 \in \Gamma$, and hence $\Delta_f(X, y_1, y_1) \geq 1$.

Case 2. $y \neq z = z_1$. Then $\varepsilon = g(Xz_1) - g(Xy_1) - (g(Xyz_1) - g(Xyy_1)) \geq 0$ and $\varepsilon = 0$ if and only if $XyB_{10} \notin \Gamma$ or $XB_{10} \in \Gamma$. If $\delta = 1$ and $\varepsilon = 0$, then $X \notin \Gamma$ while $Xy \in \Gamma$ and $Xy_1 \in \Gamma$, which implies that $\Delta_f(X, y, y_1) \geq 1$.

Case 3. $X = Yz_1$ with $Y \subseteq Py_2$. Then $\varepsilon \geq -1$. If $\varepsilon = -1$, then $YB_{10} \notin \Gamma$ while $YyB_{10}, YzB_{10} \in \Gamma$. This implies that $M_y \cap M_z \not\subseteq M_{YB_{10}}$, and hence $\Delta_f(X, y, z) \geq 1$

because $M_{Yy_1} \subseteq M_{YB_{10}}$. If $\delta = 1$, then $YB_{11} \notin \Gamma$ while $YyB_{11}, YzB_{11} \in \Gamma$ and, as before, $\Delta_f(X, y, z) \geq 1$.

We proceed now to prove Claim 5.4.10. We have to distinguish several cases.

Case 1. $y = z_1$ and $z = z_2$. For $i = 1, 2$, take $\varepsilon_i = g(Xz_i) - g(Xy_i)$, and also $\varepsilon_3 = g(Xz_1z_2) - g(Xy_1y_2)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3$. If $\varepsilon_3 = 2$, then $\varepsilon_1 = \varepsilon_2 = 1$. In addition, $\varepsilon_3 = 0$ if $\varepsilon_1 = \varepsilon_2 = 0$. Therefore, $\varepsilon \geq 0$. Suppose now that $\delta = 1$. In this case $\varepsilon_3 \leq 1$ because $XB_{11}, XB_{21} \in \Gamma$. If $\varepsilon_1 = \varepsilon_2 = 0$, then $XB_{10}, XB_{20} \in \Gamma$, And hence $Xy_1, Xy_2 \in \Gamma$. Since $X \notin \Gamma$, this implies that $\Delta_f(X, y_1, y_2) \geq 1$. If $\varepsilon_3 = 1$, then $XB_{10}B_{20} \notin \Gamma$, and hence $\varepsilon_1 = \varepsilon_2 = 1$ and $\varepsilon = 1$.

Case 2. $X = Yz_1$ and $y = z = z_2$, where $Y \subseteq P$. In this case, $\varepsilon = \varepsilon_1 - \varepsilon_0$, where $\varepsilon_0 = g(Yz_1) - g(Yy_1)$ and $\varepsilon_1 = g(Yz_1z_2) - g(Yy_1y_2)$. If $\varepsilon < 0$, then $\varepsilon_1 = 0$ and $\varepsilon_0 = 1$, and hence $YB_{10} \notin \Gamma$ while $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$. This implies that $M_{y_2} \not\subseteq M_{Yy_1}$, and hence $\Delta_f(Yy_1, y_2, y_2) \geq 1$. Suppose now that $\delta = 1$, that is, $YB_{11} \notin \Gamma$ and $Yz_1z_2 \in \Gamma$. If $\varepsilon_0 = \varepsilon_1 = 0$, then $Yy_1y_2 \in \Gamma$, and hence $\Delta_f(Yy_1, y_2, y_2) \geq 1$. If $\varepsilon_0 = \varepsilon_1 = 1$, then $N(Y) = 3$ and $YB_{1j} \notin \Gamma$ for $j = 0, 1$. This implies that $\Delta_f(Yy_1, y_2, y_2) \geq 1$.

Case 3. $X = Yz_1$ and $y \neq z = z_2$, where $Yy \subseteq P$. Take $\varepsilon_0 = g(Yz_1) - g(Yy_1)$, $\varepsilon_1 = g(Yyz_1) - g(Yyy_1)$, $\varepsilon_2 = g(Yz_1z_2) - g(Yy_1y_2)$ and $\varepsilon_3 = g(Yyz_1z_2) - g(Yyy_1y_2)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_0$. Observe that $0 \leq \varepsilon_1 \leq \varepsilon_0 \leq 1$ and $0 \leq \varepsilon_3 \leq \varepsilon_2 \leq 2$. Suppose that $\varepsilon < 0$. Then $\varepsilon_0 = 1$, $\varepsilon_1 = 0$, and $\varepsilon_2 = \varepsilon_3$. In particular, $YB_{10} \notin \Gamma$ and $YyB_{10} \in \Gamma$, and hence $\varepsilon_3 \leq 1$. If $\varepsilon_2 = \varepsilon_3 = 1$, then $YyB_{11}B_{20} \notin \Gamma$, and hence

$YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$. Since $YB_{10} \notin \Gamma$, this implies that $\Delta_f(Yy_1, y, y_2) \geq 1$. Similarly, $\Delta_f(Yy_1, y, y_2) \geq 1$ if $\varepsilon_2 = \varepsilon_3 = 0$. Suppose now that $\varepsilon = 0$ and $\delta = 1$. Then $YB_{11} \notin \Gamma$ while $YyB_{11} \in \Gamma$ and $Yz_1z_2 \in \Gamma$. If $\varepsilon_1 = 0$, then $Yyy_1 \in \Gamma$, and hence $\varepsilon_3 = 0$. If, in addition, $\varepsilon_0 = 1$, we have that $\varepsilon_2 = 1$ and, since $Yz_1z_2 \in \Gamma$, we have that $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$ or $YB_{11}B_{2k} \in \Gamma$ for $k = 0, 1$. Therefore, $\Delta_f(Yy_1, y, y_2) \geq 1$. If $\varepsilon_1 = \varepsilon_0 = 0$, Then $Yy_1y_2 \in \Gamma$. This implies that $\Delta_f(Yy_1, y, y_2) \geq 1$ because $YB_{11} \notin \Gamma$ while $YyB_{11} \in \Gamma$ and $YB_{11}B_{2k} \in \Gamma$ for $k = 0, 1$.

Case 4. $X = Yz_1z_2$, where $Yyz \subseteq P$. Take $\varepsilon_0 = g(Yz_1z_2) - g(Yy_1y_2)$, $\varepsilon_1 = g(Yz_1z_2y) - g(Yy_1y_2y)$, $\varepsilon_2 = g(Yz_1z_2z) - g(Yy_1y_2z)$ and $\varepsilon_3 = g(Yz_1z_2yz) - g(Yy_1y_2yz)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_0$. Observe that $0 \leq \varepsilon_3 \leq \varepsilon_1, \varepsilon_2 \leq \varepsilon_0$. Suppose that $\Delta_f(Yy_1y_2, y, z) = 0$, that is, $M_y \cap M_z \subseteq M_{Yy_1y_2}$. Without loss of generality, we can assume that $y \in B_{10} \cap B_{11}$ or $y \in B_{10}$ and $z \in B_{11}$. Suppose that $y \in B_{10} \cap B_{11}$ (observe that this covers the case $y = z$). Then $\varepsilon_1 = \varepsilon_0$ and $\varepsilon_3 = \varepsilon_2$, and hence $\varepsilon = 0$. Moreover, $\delta = 0$ because $Yy_1y_2y \notin \Gamma$ if $Yy_1y_2 \notin \Gamma$.

Suppose now that $y \in B_{10}$ and $z \in B_{11}$. We prove first that $\varepsilon \geq 0$. Three cases are considered.

1. If $\varepsilon_1 = 0$, then $YyB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, and hence $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, which implies that $\varepsilon_0 \leq 1$. If $\varepsilon_1 = 0$ and $\varepsilon_0 = 1$, then $YB_{11}B_{20} \notin \Gamma$ and $YzB_{11}B_{20} \notin \Gamma$, which implies that $\varepsilon_2 = 1$. Therefore, $\varepsilon = 0$ if $\varepsilon_1 = 0$.

2. Suppose now that $\varepsilon_1 = 1$ and $\varepsilon_2 = 0$. Then $YzB_{11}B_{20} \in \Gamma$, and hence $YB_{11}B_{20} \in \Gamma$. If $\varepsilon < 0$, then $\varepsilon_0 = 2$, and hence $YB_{10}B_{2k} \notin \Gamma$ for $k = 0, 1$, a contradiction with $\varepsilon_1 = 1$.

3. Consider now the case $\varepsilon_1 = \varepsilon_2 = 1$, and suppose that $\varepsilon < 0$. Then $\varepsilon_0 = 2$ and $\varepsilon_3 = 1$. Since $\varepsilon_1 = 1$, exactly one of the sets $YB_{10}B_{20}$, $YB_{10}B_{21}$ is in Γ. Moreover, $YB_{11}B_{20} \notin \Gamma$ while $YyB_{11}B_{20} \in \Gamma$. and $YzB_{10}B_{21} \in \Gamma$. This implies that $\varepsilon_3 = 0$, a contradiction.

Now, we have to prove that $\varepsilon \geq 1$ if $\delta = 1$. Suppose that, on the contrary, $\varepsilon = 0$ and $\delta = 1$. As before, we distinguish three cases.

1. If $\varepsilon_1 = 0$, then $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, and hence $Yz_1z_2 \in \Gamma$, a contradiction. Therefore, we assume from now on that $\varepsilon_1 \geq 1$, and hence $\varepsilon_0 \geq 1$.

2. If $\varepsilon_0 = 1$, then $N(Y) = 2$ and $YB_{11}B_{21} \notin \Gamma$ because $Yz_1z_2 \notin \Gamma$. This implies that $Yzz_1z_2 \notin \Gamma$, a contradiction.

3. If $\varepsilon_0 = 2$, then $N(Y) = 1$ and $YB_{11}B_{21} \in \Gamma$ because $Yzz_1z_2 \in \Gamma$. Therefore, $YyB_{10}B_{2k} \notin \Gamma$ for $k = 0, 1$, and hence $\varepsilon_1 = 2$. Moreover, $N(Yz) \geq 2$ and $YzB_{11}B_{20} \notin \Gamma$. If $YzB_{10}B_{20} \notin \Gamma$ or $YzB_{10}B_{21} \notin \Gamma$, then $\varepsilon_2 = 2$, and hence $\varepsilon_3 = 2$. This implies that $YyB_{11}B_{20} \notin \Gamma$, and hence $Yyz_1z_2 \notin \Gamma$, a contradiction. If $YzB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, then $\varepsilon_2 = 1$, and hence $\varepsilon_3 = 1$. Again, this implies that $Yyz_1z_2 \notin \Gamma$, a contradiction.

□

Chapter 6

Conclusion

In this thesis we have explored two main open problems in secret sharing schemes: the characterization of ideal access structures and the optimization of the length of shares.

6.1 New families of ideal access structures and secret sharing schemes

In Chapter 3 we devoted to study ideal multipartite secret sharing, in the way that new families of ideal multipartite access structures are found by different representable integer polymatroids. And due to the use of integer polymatroids, our proofs that the structures in these new families are ideal are extremely concise.

Notice that we summarize common features of existing constructions of ideal linear secret sharing schemes, while a remarkable common feature is that they are associated to Boolean polymatroids. To say the least, we use linear polymatroids, which are representable on every large enough finite fields. Due to Farràs, Martí-Farré and Padró's work [41], our research focuses on ideal multipartite access structures. Obviously, there remains many interesting work to do at every point of specializing. The study on any family of secret sharing schemes satisfying any common features mentioned in Section 3.1 or a few together will be interesting.

On the other hand, it is still an open problem to efficiently construct ideal linear secret sharing schemes for those families of access structures. This problem in general cases is connected the representability of matroids, which is an open problem.

The method to construct ideal multipartite secret sharing schemes firstly proposed by Brickell [22] is a linear algebra reformulation of the geometric ideas by Blakley [16] and Simmons [87]. Next the search for ideal multipartite secret sharing centered on interesting families of access structures also by other authors [12, 51, 72, 90, 92]. All these constructions give vector space secret sharing schemes, while in Section 3.7 we have represented them in a unified way.

Though a general method to construct those ideal multipartite access structures is presented in [41], an efficient method is unknown. Further work can be on constructing ideal secret sharing schemes for mentioned ideal access structure in Chapter 3 or other ones, and general constructions are more welcome.

6.2 Bounds on information ratio

In Chapter 4 and 5, optimization of the length of shares is discussed from particular cases and asymptotic behavior.

In Chapter 4 the information ratio of some access structures with small number of participants are studied, particularly, unsettled bounds of 5-participant access structures [57] and 6-participant graph access structures [48], while we give a general way to compute out the lower bounds of any small access structure; also we try to use information inequalities and rank inequalities to sharpen the known information ratio region, however, in most cases we tried those inequalities are helpless.

There are a few cases that are still open, that is, the optimal (average) information ratios are unsettled for some 5-participant access structures and 6-participant graph access structures. The impossibility result in Section 4.6 shows the difficulty of solving this problem. For linear secret sharing schemes, we can use rank inequalities to improve lower bounds and construct the schemes to improve upper bounds. However, for non-linear schemes, this problem becomes harder. Moreover, even if all information and rank inequalities are known, we are not sure that the cases discussed in Section 4.6 can be solved. Neither do we for other access structures.

In Chapter 5 we give two negative results, both of which show the limitation of the use of information inequalities and rank inequalities. We proved that all information inequalities on a bounded number r of variables only can provide lower bounds $\binom{n+r-3}{r-2}$ that are polynomial on the number of participants n. On the other hand, we proved theoretically all the rank inequalities derived from one or two common informations cannot get better lower bounds than $O(\binom{n+2}{3}) = O(n^3)$.

For general access structures, the gap between lower bounds and upper bounds is quite large. So far we are lack of techniques to solve this problem. Beimel probed into this difficult problem at the end of [5], and brought forward questions in order to settle Conjecture 1.3.1. And Beimel and Weinreb [11] presented infinite family (Γ_n) of access structures for which $\sigma(\Gamma_n)$ is polynomial on the number of participants while $\lambda(\Gamma_n)$ is superpolynomial. This separation result shows the gap between σ and λ for general access structures is at least from polynomial to superpolynomial. However, to narrow the gap between lower bounds and upper bounds for general access structure is a long way to go.

Observe that the method we use to study information ratio in both Chapter 4 and Chapter 5 actually is linear programming, which is the only method known. However, this method has entered a bottleneck due to two main limitations. One is many undiscovered information inequalities and rank inequalities and the other one is the limitation of those inequalities as Beimel and Orlov [10] and Chapter 5 showed. It is clear that new techniques are needed to significatively advance this area.

Bibliography

[1] I. Anderson. *Combinatorics of Finite Sets*. Oxford University Press, 1987. 82

[2] L. Babai, A. Gál, A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica* **19** (1999) 301-319. 103, 104

[3] S. Ball. On large subsets of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc.* **14** (2012) 733–748. 38

[4] S. Ball, C. Padró, Z. Weiner, C. Xing. On the representability of the bi-uniform matroid. Manuscript (2012). 38, 73

[5] A. Beimel. Secret-Sharing Schemes: A Survey. *IWCC'2011. Lect. Notes Comput. Sc.* **6639** (2011) 11–46. 9, 26, 103, 129

[6] A. Beimel, A. Gál, M. Paterson. Lower bounds for monotone span programs. *Comput. Complexity* **6** (1997) 29-35. 103, 104

[7] A. Beimel, Y. Ishai. On the power of nonlinear secret sharing schemes. *SIAM J. Discrete Math.* **19** (2005) 258–280. 76

[8] 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. 78, 86, 88, 89, 105

[9] A. Beimel, I. Orlov. Secret Sharing and Non-Shannon Information Inequalities. *Proc. of TCC'2009, Lect. Notes Comput. Sc.* **5444** (2009) 539–557. 78, 86

[10] A. Beimel, I. Orlov. Secret Sharing and Non-Shannon Information Inequalities. *IEEE Trans. Inform. Theory* **57** (2011) 5634–5649. iv, 4, 9, 13, 104, 105, 106, 107, 109, 110, 129

[11] A. Beimel, E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.* **34** (2005) 1196–1215. 7, 76, 129

[12] A. Beimel, E. Weinreb, T. Tassa. Characterizing Ideal Weighted Threshold Secret Sharing. *SIAM J. Discrete Math.* **22** (2008) 360–397. 39, 61, 127

[13] J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88. Lecture Notes in Comput. Sci.* **403** (1990) 27–35. iv, 6

[14] M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In *Proc. of the 20th ACM Symp. on the Theory of Computing* (1988) 1–10. 2

[15] A. Beutelspacher, F. Wettl. On 2-level secret sharing. *Des. Codes Cryptogr.* **3** (1993) 127–134. 70, 71, 72

[16] G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conf. Proc.* **48** (1979) 313–317. 2, 5, 7, 127

[17] J.R. Bloom. A note on Superfast Threshold Schemes. Preprint, Texas A&M. Univ., Dept. of Mathematics, 1981. 5, 37

[18] 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. 104

[19] 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. 10, 75, 98

[20] C. Blundo, A. de Santis, U. Vaccaro. On secret sharing schemes. *Inform. Process. Lett.* **65** (1998) 25-32.

[21] P. Bogetoft, D.L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard,J.D. Nielsen, J.B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, T. Toft. Secure Multiparty Computation Goes Live. *Financial Cryptography and Data Security* (2009) 325–343. 2

[22] E.F. Brickell. Some ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134. 6, 7, 37, 38, 40, 45, 46, 52, 54, 61, 62, 70, 71, 72, 73, 127

[23] E.F. Brickell, D.M. Davenport. On the Classification of Ideal Secret Sharing Schemes. *J. Cryptology* (1991) 123–134. 3, 4, 6, 7, 31, 39, 45

[24] R. M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the Size of Shares for Secret Sharing Schemes. *J. Cryptology* **6** (1993) 157–167. 104

[25] T.H. Chan, L. Guillé, A. Grant. The minimal set of Ingleton inequalities. *IEEE Trans. Inform. Theory* **57** (2011) 1849–1864. 87

[26] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure proto-cols. In *Proc. of the 20th ACM Symp. on the Theory of Computing* (1988) 11–19. 2

[27] B.L. Chen, H.M. Sun. Weighted Decomposition Construction for Perfect Secret Sharing Schemes. *Comput. Math. Appl.* **43** (2002) 877–887. 76, 84, 85

[28] M.J. Collins. A Note on Ideal Tripartite Access Structures. *Cryptology ePrint Archive*, Report 2002/193, `http://eprint.iacr.org/2002/193`. 39

[29] T. M. Cover, J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 1991. 14

[30] L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231. iv, 2, 3, 4, 9, 10, 13, 33, 50, 76, 98, 104, 105, 106, 107, 109

[31] L. Csirmaz. Secret sharing on the *d*-dimensional cube. *Cryptology ePrint Archive*, Report 2005/177, `http://eprint.iacr.org/2005/177`. 10, 75

[32] L. Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptogr.* **53** (2009) 195–209. 10, 75, 77, 78, 105

[33] L. Csirmaz, G. Tardos. Secret sharing on trees: problem solved. *Cryptology ePrint Archive*, Report 2009/071, `http://eprint.iacr.org/2009/071`. 10, 75

[34] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT'00*, Springer-Verlag (2000) 316–334. 2

[35] M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.* **6** (1995) 143–169. 10, 12, 75, 76, 84, 85

[36] M. van Dijk. More information theoretical inequalities to be used in secret sharing? *Inform. Process. Lett.* **63** (1997) 41–44. 82, 83

[37] M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls. Improved constructions of secret sharing schemes by applying-(λ, ω)-decompositions. *Inform. Process. Lett.* **99** (2006) 154–157. 10, 76, 84

[38] R. Dougherty, C. Freiling, K. Zeger. Six new non-Shannon information inequalities. *ISIT'2006*, 233–236. 17, 78, 86, 89

[39] R. Dougherty, C. Freiling, K. Zeger. Linear rank inequalities on five or more variables. Available at `arXiv.org`, arXiv:0910.0284v3 (2009). 13, 18, 19, 78, 86, 106, 107, 116

[40] R. Dougherty, C. Freiling, K. Zeger. Non-Shannon Information Inequalities in Four Random Variables. Available at `arXiv.org`, arXiv:1104.3602v1 (2011). 17, 78, 86

[41] O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *J. Cryptology* **25** (2012) 434–463. iii, 4, 7, 11, 39, 41, 45, 46, 47, 53, 56, 62, 70, 71, 127

[42] 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. 49, 75, 77

[43] O. Farràs, C. Padró. Ideal Hierarchical Secret Sharing Schemes. *IEEE Trans. Inform. Theory* **58** (2012) 3273–3286. 8, 39, 40, 62, 63

[44] O. Farràs, C. Padró, C.P. Xing, A. Yang. Natural Generalizations of Threshold Secret Sharing. *IEEE Trans. Inform. Theory* **60** (2014) 1652–1664. 36

[45] S. Fujishige. Entropy functions and polymatroids–combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18. 3, 21, 105

[46] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Inform. and Control.* **39** (1978) 55–72. 3, 21, 76, 105

[47] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Comput. Complexity* **10** (2001) 277–296. 103, 104

[48] M. Gharahi, M.H. Dehkordi. The complexity of the graph access structures on six participants. *Des. Codes Cryptogr.* **67** (2013) 169–173. 77, 85, 128

[49] M. Giuletti, R. Vincenti. Three-level secret sharing schemes from the twisted cubic. *Discrete Math.* **310** (2010) 3236–3240. 7, 70, 71, 72

[50] D. Hammer, A.E. Romashchenko, A. Shen, N.K. Vereshchagin. Inequalities for Shannon Entropy and Kolmogorov Complexity. *J. Comput. Syst. Sci.* **60** (2000) 442–464. 19, 22, 106, 116

[51] J. Herranz, G. Sáez. New Results on Multipartite Access Structures. *IEE Proceedings on Information Security* **153** (2006) 153–162. 37, 39, 40, 65, 66, 69, 127

[52] J. Herzog, T. Hibi. Discrete polymatroids. *J. Algebraic Combin.* **16** (2002) 239–268. 23

[53] J.W.P. Hirschfeld. The Main Conjecture for MDS Codes. *Cryptography and Coding. Lecture Notes in Comput.Sci.* **1025** (1995) 44–52. 38

[54] A.W. Ingleton. Representation of matroids. in: D.J.A Welsh (Ed.), Combinatorial Mathematics and its Applications, Academic Press, London (1971) 149–167. 19, 78, 86

[55] M. Ito, A. Saito. T. Nishizeki, Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87* 99–102. iv, 2, 5

[56] W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95. 5, 10, 35, 59

[57] W.A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286. 12, 75, 76, 78, 82, 83, 84, 104, 128

[58] M. Karchmer, A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory* (1993) 102–111. 5

[59] E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41. 5, 29, 37, 75

[60] S.C. Kothari. Generalized Linear Threshold Scheme. *Advances in Cryptology, CRYPTO'84. Lecture Notes in Comput. Sci.* **196** (1985) 231–241. 7, 36, 37

[61] A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725. 6

[62] K. Makarychev, Y. Makarychev, A. Romashchenko, N. Vereshchagin. A new class of non-Shannon-type inequalities for entropies. *Commun. Inf. Syst.* **2** (2002) 147–166. 17

[63] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) 95–120. 4, 35, 45, 76, 89

[64] 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. 75, 77

[65] J.L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory*, Molle, Sweden (1993) 269–279. 46

[66] J.L. Massey. Some applications of coding theory in cryptography, *Codes and Ciphers: Cryptography and Coding IV*, Formara Ltd, Essses, England (1995) 33–47. 46

[67] F. Matúš. Matroid representations by partitions. *Discrete Math.* **203** (1999) 169–194. 7

[68] F. Matúš. Adhesivity of polymatroids. *Discrete Math.* **307** (2007) 2464–2477. 4, 80

[69] F. Matúš. Infinitely many information inequalities. *IEEE International Symposium on Information Theory* (2007) 41–44. 17, 78, 86

[70] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomom codes. *Comm. ACM* **22** (1979) 612–613

[71] J.R. Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. *Discrete Math.* **311** (2011) 651–662. 86, 88, 89, 105

[72] S.-L. Ng. Ideal secret sharing schemes with multipartite access structures. *IEEE Proc.Commun.* **153** (2006) 165–168. 37, 40, 127

[73] J.G. Oxley, *Matroid Theory*. Second ed., Oxford University Press, New York, 2011. 22, 24, 38, 89

[74] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604. 39, 40, 42, 71, 72

[75] C. Padró, L. Vázquez, A.Yang. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Discrete Appl. Math.* **161** (2013) 1072–1084. 10, 77, 84, 85, 105

[76] M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th IEEE Symp. on Foundations of Computer Science* (1983) 403–409. 2

[77] R. Rado. Note on independence functions. *Proc. London Math. Soc. (3)* **7** (1957) 300–320. 18

[78] B. V. Raghavendra Rao, Jayalal M. N. Sarma. On the Complexity of Matroid Isomorphism Problems. *Computer Science - Theory and Applications, Lecture Notes in Comput. Sci.* **5675** (2009) 286–298. 71

[79] A. Schrijver. *Combinatorial optimization. Polyhedra and efficiency.* Springer-Verlag, Berlin, 2003. 23, 48

[80] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl.* **39** (1955) 357-379. 38

[81] P. D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B* **56** (1992) 69–73. 6, 88

[82] A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) 612–613. 2, 5, 7, 28, 38, 61

[83] B. Shankar, K. Srinathan, C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In *Proc. of ICDCN'08* 304–309. 2

[84] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal* **27** (1948) 379–423. 16

[85] V. Shoup. New algorithm for finding irreducible polynomials over finite fields. *Math. Coup.* **54** (1990) 435–447. 38, 73

[86] J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) 179–197. 7

[87] G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO'88, Lecture Notes in Comput. Sci.* **403** (1990) 390–448. 5, 7, 36, 37, 40, 51, 52, 54, 60, 61, 62, 127

[88] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390. 46

[89] D.R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory.* **40** (1994) 118–125. 75

[90] T. Tassa. Hierarchical Threshold Secret Sharing. *J. Cryptology* **20** (2007) 237–264. 7, 37, 38, 40, 61, 62, 70, 71, 72, 73, 127

[91] T. Tassa. Generalized oblivious transfer by secret sharing. *Des. Codes Cryptogr.* **58**, 2011. 2

[92] T. Tassa, N. Dyn. Multipartite Secret Sharing by Bivariate Interpolation. *J. Cryptology* **22** (2009) 227–258. 7, 37, 40, 52, 54, 70, 71, 72, 127

[93] R. W. Yeung. *A First Course in Information Theory*. Springer, 2002. 14, 16, 17

[94] Z. Zhang. On a new non-Shannon type information inequality. *Commun. Inf. Syst.* **3** (2003) 47–60. 106

[95] Z. Zhang, R.W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory* **44** (1998) 1440–1452. 17, 78, 85, 88, 90