Multipartite Secret Sharing Schemes

Oriol Farràs Ventura

Thesis submitted to the Universitat Politècnica de Catalunya
for the degree of Doctor of Mathematics

Thesis Director: Prof. Carles Padró Laimon

June 2010

Contents

Abstract

This thesis is dedicated to the study of secret sharing schemes, which are cryptographic methods to share information in a secure way. The topics that are considered herein are 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 general access structures. These open problems are studied for multipartite secret sharing schemes. In these schemes we consider that the set of participants is divided into parts and in each part the participants have the same rights to obtain the secret.

The results of the thesis are based on a new combinatorial property of secret sharing schemes that is presented herein, a connection between ideal multipartite secret sharing schemes and integer polymatroids. It provides new sufficient conditions and necessary conditions for an access structure to be ideal. Moreover, this connection is also used in the construction ideal linear multipartite secret sharing schemes. These results are useful for the study of multipartite access structures in which the number of parts is small in relation to the number of participants, and multipartite access structures in which the parts are related in a special way. This is the case of the family of hierarchical access structures, that are the ones in which the participants can be hierarchically ordered, and the family of tripartite access structures. We characterize the ideal access structures in these families.

All the ideal multipartite secret sharing schemes presented in the literature are related to a particular family of integer polymatroids, the boolean ones. The analysis of these polymatroids leads to the find of new ideal multipartite secret sharing schemes.

The optimization of the length of the shares is also studied for multipartite secret sharing schemes, in particular for the bipartite ones. The main results are a new method to find bound on the length of the shares that combines linear programming and polymatroids, and a new family of optimal bipartite linear secret sharing schemes.

Chapter 1

Introduction

1.1 Overview

A *secret sharing scheme* is a method to protect a piece of information or data by dividing it into pieces, which are called *shares*, in such a way that it can only be recovered from certain subsets of shares. Considering that each share is held by a *participant*, the *access structure* of the scheme is defined as the family of coalitions of participants that can recover the secret.

The first secret sharing schemes were constructed by Shamir [94] and Blakley [14] in 1979. The original motivation for constructing these schemes was to protect keys, and to safeguard information in general. However, secret sharing was soon used for many different cryptographic applications and became a very important primitive in cryptography. This is mainly due to the fact that secret sharing is an essential building block in multiparty computation protocols. Multiparty computation is a very general notion that covers many different kinds of protocols, as electronic elections, electronic biddings, data base access and data base computations, and joint signatures.

Besides, the study of secret sharing schemes and the search of efficient schemes to be used in cryptographic protocols have posed a number of open problems involving different fields of mathematics as algebra, combinatorics, information theory, complexity theory, and algebraic geometry. In the search of solutions, a rich mathematical theory has been developed.

In this thesis we consider two of the main open problems in secret sharing. The first one is the characterization of the access structures that admit an ideal scheme, the *ideal* access structures. The *ideal* secret sharing schemes are the ones in which the length of the shares is the smallest possible. Namely, the length of every share is the length of the secret. The second one is the optimization of the length of the shares for general access structures.

The schemes in [14, 94] are ideal and have threshold access structure, which means that the access structure consists of all the subsets whose size is greater than a certain threshold. A natural generalization of threshold secret sharing schemes are the multipartite secret sharing schemes. In these schemes, the set of participants is divided into different parts and the participants in each part play the same role in the scheme and have the same rights to obtain the secret. In the literature we find several families of ideal multipartite secret sharing schemes, but the problem of characterizing the ideal multipartite access

structures has only been considered for bipartite access structures and weighted threshold access structures.

This thesis is dedicated to multipartite secret sharing schemes. In particular, it is devoted to the characterization of ideal multipartite access structures, to the construction of efficient ideal multipartite secret sharing schemes, and to the optimization of non-ideal multipartite secret sharing schemes.

We present a new combinatorial property of the ideal multipartite secret sharing schemes that provides a new necessary condition and a new sufficient condition for a multipartite access structure to be ideal. Applying these results, we obtain a unified framework, that encloses all the constructions in the literature, to describe and analyze methods to construct ideal multipartite secret sharing schemes. In addition, we obtain general results on ideal multipartite access structures and a complete characterization of the ideal tripartite access structures.

We present a complete characterization of the ideal hierarchical access structures and we also present an ideal construction for them. The notion of hierarchy considered in this work is very natural. A scheme is hierarchical if the set of participants can be ordered in such a way that for every authorized coalition, if we replace a participant for a hierarchically superior one, the new coalition is also authorized. The family of hierarchical access structures includes several families of access structures studied in the literature, and in particular the family of weighted threshold access structures, for which we give a new characterization of the ideal ones. In addition, we study all the previous constructions of ideal multipartite secret sharing schemes and we present a new family, the compartmented secret sharing schemes, which generalizes several families previously studied.

On the optimization of bipartite secret sharing schemes, we present new results on the optimization of the length of the shares and we apply them to bipartite access structures obtaining optimal secret sharing schemes and a new method to find bounds on the optimal length of the shares for these access structures.

1.2 Secret Sharing

In a secret sharing scheme, we say that each share is held by a participant of the scheme, and the secret is held by a special participant, which is called the *dealer*. The dealer shares the secret among the set of participants, and the subsets of participants than can recover the secret constitute the *access structure* of the scheme, which is monotone increasing. A scheme *perfect* if it is *unconditionally secure*, which means that the security does not rely on any computational assumption, and the subsets of participants that are not in the access structure do not have any information about the secret. The schemes studied herein are perfect.

The schemes presented by Shamir [94] and Blakley [14] are called *threshold* secret sharing schemes because the authorized subsets are those whose size is greater than a certain threshold. The construction presented by Shamir is based on polynomial interpolation, while geometrical ideas are used in the one by Blakley. Ito, Saito, and Nishizeki [57] proved that there exists a secret sharing scheme for every access structure. However, the size of the shares in the schemes proposed in [57] is exponential on the number of participants. Hence, these constructions are considered inefficient. Benaloh and Leichter [12] improved the gen-

eral construction in [57], but the size of the shares in their construction is still exponential on the number of participants. Nevertheless, this is the best known general construction, and so one of the main open problems in secret sharing is the optimization of secret sharing schemes for general access structures.

Commonly, the efficiency of a secret sharing scheme is measured by the amount of information that is sent to each participant in order to share a secret. Other features, as the complexity of the computation of the shares and the complexity of the recovering of the secret are also worth considering. The *complexity* of a scheme is defined as the result of dividing the length of the largest share by the size of the secret.

In a perfect scheme, the size of each share must be bigger or equal than the size of the secret [62], so a scheme is called *ideal* if its complexity is equal to one. The access structures of ideal secret sharing schemes are also called *ideal*. Benaloh and Leichter [12] proved that there exist access structures that do not admit any ideal scheme and, as consequence of the results in [16, 35] and other works, in some cases the length of the shares must be much larger than the length of the secret. Actually, the open problem of optimizing the length of the shares in secret sharing schemes for general access structures is very far from being solved, and there is a wide gap between the best known lower and upper bounds on the complexity.

The techniques used by Shamir [94] and Blakley [14] to construct ideal schemes were analyzed by Kothari [63], Simmons [96] and Brickell [19] with the purpose of constructing ideal schemes for other access structures. Generalizing the geometric method by Blakley [14], Brickell [19] found a method to construct ideal secret sharing schemes for general access structures. These schemes are *linear* because the shares are determined by linear mappings of the secret and some random values. Linear secret sharing schemes have some homomorphic properties that are very interesting for cryptographic applications. Moreover, due to linearity, the computation of the shares and the reconstruction of the secret are efficient. This construction was generalized for non-ideal schemes by Karchmer and Wigderson [61]. Linear schemes have also been called geometric schemes [59, 96] and monotone span programs [61].

The interest of the homomorphic properties due to linearity of the Shamir secret sharing scheme were previously highlighted in [11]. Moreover, due to some special homomorphic properties with respect to multiplication, the Shamir scheme was used to construct the first unconditionally secure multiparty computation protocols. In 1988, Ben-Or, Goldwasser, Wigderson [10] and Chaum, Crepeau and Damgård [24] presented a general method to construct an unconditionally secure multiparty computation protocol for any function. After this breakthrough result, secret sharing schemes became an important building block in cryptography. Cramer, Damgård, and Maurer [31] abstracted the properties of the Shamir scheme that are used in the construction of unconditionally secure multiparty computation protocols and generalized these protocols for general linear schemes. They defined the family of *multiplicative* and *strongly multiplicative* linear secret sharing schemes, which can replace the Shamir scheme in the construction of multiparty computation protocols. The efficiency of these protocols depends on the length of the shares, which is determined by the complexity of the scheme and the size of the field. Chen and Cramer [25] found an interesting family of linear schemes that are constructed from algebraic-geometric codes. These schemes have multiplicative properties and have had important repercussions in mul-

tiparty computation [26, 30, 88]. By using this kind of schemes, it is possible to improve extraordinarily the efficiency of the constructions in [10, 24].

Most of the applications that use secret sharing require schemes with homomorphic properties, and so the linear schemes are the most used. Actually, some of the applications require linear schemes with some special properties. Several public key cryptosystems require secret sharing schemes defined over rings and groups instead of finite fields. This need motivated the construction of linear schemes defined over rings and the *black box* secret sharing schemes [33,34,38,39]. For key distribution, there exist schemes in which the shares contain information about multiples secrets [15, 58, 84]. Recently, the construction of cryptosystems that are secure under the perspective of game theory motivated the construction of *non-cooperative* secret sharing schemes [50, 51].

In addition, the linear secret sharing schemes have played an important role in the search of optimal secret sharing schemes for general access structures [18, 21, 99]. Brickell and Davenport [20] presented in 1989 an essential result for the study of ideal secret sharing schemes, they proved that the access structure of every ideal secret sharing scheme is related to a matroid, it is a *matroid port*. Seymour [93] proved that this condition is not sufficient but as a consequence of the results by Brickell [19], if an access structure is related to a linearly representable matroid, then the access structure admits a linear ideal secret sharing scheme. Therefore, the connection with matroids provides a sufficient and a necessary condition for an access structure to be ideal.

The characterization of representable matroids is an open problem in matroid theory and so the problem of characterizing the ideal access structures is unsolved. However, this connection with matroids provide very interesting tools for secret sharing that have been used to find efficient constructions and bounds on the efficiency of the schemes, for instance [1–4, 6, 32, 64, 66–69, 81, 83]. Generalizing the connection between ideal access structures and matroids in [20], Csirmaz [35] proved that the entropies of the shares of a secret sharing scheme determine a polymatroid. Polymatroids have been used to find bounds on the efficiency of secret sharing schemes, as for instance in [5, 35, 68, 73, 100]. In the study the efficiency, Karchmer and Wigderson [61] applied results of complexity theory. These techniques have been used to find many important results on the optimization of secret sharing [2, 8, 88].

1.3 State of the Art

In this section we present the previous results on the topics of this thesis, which are the construction of ideal linear secret sharing schemes, the characterization of the ideal access structures, and the optimization of secret sharing schemes.

1.3.1 Constructing Ideal Secret Sharing Schemes

Due to the difficulty of constructing efficient schemes for general access structures, many studies are dedicated to particular access structures that are interesting for practical issues. The method to construct ideal secret sharing schemes proposed by Brickell [19] has been used in the vast majority of the constructions of ideal secret sharing schemes in the literature. Most of these constructions are *multipartite secret sharing schemes*, schemes in which the

set of participants is divided into several parts and all participants in the same part play an equivalent role in the scheme. Since we can always consider as many parts as participants, every access structure is multipartite, but it is specially interesting to consider situations in which the number of parts is smaller than the number of participants or in situations in which the partition is derived from some special organization of the participants. For two parts, Padró and Sáez constructed ideal secret sharing schemes for all ideal bipartite access structures. For three parts, there are just constructions for some of these structures [89].

The families of structures studied for practical situations are *hierarchical*, in which there is a hierarchical relation among the participants, or *compartmented*, in which the presence of participants from different parts is limited or guaranteed. The first hierarchical scheme was constructed by Shamir [94], but it is not ideal. Brickell [19] presented the first ideal constructions for families of hierarchical and compartmented access structures. Tassa [101] and Tassa and Dyn [102] used different techniques to construct alternative schemes for these access structures and for other kinds of compartmented access structures. A particular kind of hierarchical access structures, the weighted threshold ones, has been studied in [77, 85], and the characterization of the ideal ones was presented by Beimel, Tassa and Weinreb [6]. Constructions of ideal secret sharing schemes for variants of the compartmented and multilevel access structures were presented in [80, 89]. Moreover, there is an efficiency question that have been studied for some multilevel access structures, which is the minimization of the size of the field in which the scheme is defined [13, 49].

Another family of ideal secret sharing schemes are the ones defined from algebraic-geometric codes [25–27, 88]. Due to their multiplicative properties and fact that the number of participants can be extremely high in relation to the size of the field, these schemes are interesting for the construction of efficient multiparty computation protocols.

1.3.2 Characterization of Ideal Access Structures

The characterization of ideal access structures is one of the main open problems in secret sharing. During the eighties, as we have detailed above, several authors constructed ideal secret sharing schemes with non-threshold access structures, and so found particular families of ideal access structures. In 1989, Brickell and Davenport [20] made an important contribution to the study of ideal access structures. They presented a connection between matroids and ideal access structures. Namely, they proved that ideal access structures are matroid ports. This result provides a necessary condition for an access structure to be ideal and a sufficient condition for an access structure to admit an ideal linear secret sharing scheme. However, after these results, the problem of characterizing the ideal access structures is still not solved, because in order to solve it by means of this connection, it would be necessary to characterize the entropic matroids, which is an open problem in matroid theory that is far to be solved.

The connection between matroids and ideal access structures is a combinatorial tool that has been used in many works to prove the non-ideality of access structures [6, 66, 67, 69, 93]. The sufficient condition for an access structure to be ideal in [20] states that the access structures related to linearly representable matroids are ideal. The construction of ideal schemes over different fields has been studied in [1]. However, the characterization of linearly representable matroids is also an open problem in matroid theory.

Far from being solved in general, the problem of characterizing the ideal access structures has been studied for particular families. That is, access structures with a small number of participants [60, 98], access structures defined by graphs [16, 20, 23, 36, 100], and structures with certain combinatoric properties [66, 67, 69]. Among multipartite access structures the families for which this problem has been solved are the family of bipartite access structures [85] and the weighted threshold access structures [6]. For access structures with three parts there are only some partial results on the characterization of the ideal ones in [6,28,89]. All these works use different combinatorial techniques, most of them related to matroid theory, to obtain necessary conditions for an access structure to be ideal. These conditions are used to show the non-ideality of access structures. However, in order to prove the ideality of access structures there are not specific techniques apart from constructing explicitly an ideal secret sharing scheme for them.

Among ideal access structures, the characterization of the ones that admit an multiplicative or strongly multiplicative ideal scheme is an interesting open problem for secret sharing and multiparty computation. Nevertheless, apart from some necessary conditions [55], very little is known about it. Another open problem related to this one is the characterization of the self-dual matroids that are represented by self-dual codes. This problem was solved for particular families of access structures in [32,83]. The access structure of algebraic geometric schemes [25], which have multiplicative properties, is in general difficult to compute. The access structure has only been characterized for algebraic schemes defined from elliptic curves [27].

1.3.3 Optimization of Secret Sharing

In general, for any access structure it is not known which is the most efficient scheme for the structure, and the infimum of the complexity that can be attained for these schemes is also unknown. We define the *optimal complexity* of an access structure as the infimum on the complexity of the secret sharing schemes with such access structure and we note it by σ. The general upper bound on the complexity of the best scheme is exponential on the number of participants [57], and for every set of n participants, there exist families of access structures whose complexity is about $n/\log n$ [35]. Actually, the open problem of optimizing the length of the shares in secret sharing schemes for general access structures is very far from being solved, and there is a wide gap between the best known lower and upper bounds.

There are two parameters that are interesting for the study of this open problem. A lower bound on the optimal complexity of an access structure is the bound derived from the Shannon inequalities that the entropy of the shares of the scheme must satisfy. Due to the interest of linear schemes, an interesting upper bound on the complexity of an access structure is the infimum on the complexity of the linear schemes for it. These two parameters are noted by κ and λ, respectively.

The connection between matroids and ideal access structures [20] is also interesting for the study of non-ideal access structures. The separation between matroid ports and ideal access structures has been studied in [1–4,64,75]. Generalizing the connection between ideal access structures and matroids [20], Csirmaz [35] proved that the entropies of the shares of a secret sharing scheme determine a polymatroid. Polymatroids have been used to find

bounds on the complexity of secret sharing schemes and to find results on the parameter κ, as for instance in [35, 68, 100]. In particular, the study of entropic and linear polymatroids provide better bounds [73]. There are also other results on κ derived directly from the Shannon inequalities [16, 17, 23, 60]. Non-Shannon information inequalities [110] have also been used in secret sharing. New results on the separation between the parameters κ and σ in [4,75] are based on these inequalities. Beimel and Orlov [5] studied the power of the non-Shannon inequalities known until now and proved that from these inequalities the general lower bound on the complexity obtained by Csirmaz [35] cannot be improved.

Csirmaz proved that for every access structure κ is smaller or equal than the number of participants. However, λ does not have a similar asymptotic behavior. Several results show that λ grows faster [2,7,48]. In particular, a separation result between the parameters σ and λ was given in [7]. Other results on λ have been obtained from constructions of schemes with low complexity, as for instance in [18, 21, 60, 99, 105]. It is worth to mention that for certain access structures it has been proved that the use of nonlinear schemes is more efficient [2, 7]. However, very little is known about the construction of non-linear schemes, and by now their applications are very limited.

1.4 Contributions

The main results presented in this thesis are described in the following. We divide them into two classes: results on ideal multipartite secret sharing schemes, and results on the optimization of multipartite secret sharing schemes.

1.4.1 Ideal Multipartite Secret Sharing Schemes

On the basis of the connection between ideal access structures and matroids presented in [20], we present in Chapter 3 a new combinatorial property of the ideal multipartite secret sharing schemes. We show that every ideal multipartite access structure defines an integer polymatroid. This result improves the connection with matroids for multipartite access structures, and by means of this result we present a new necessary condition for a multipartite access structure to be ideal, and a new sufficient condition for a multipartite access structure to admit an ideal linear secret sharing scheme. By means of this new connection, we present a new theory that generalizes and formalizes the previous results in this field and allows to find new ideal access structures among interesting families. The applications of these results to different families of access structures are presented in Chapters 4 and 5. In these chapters we present a characterization of the ideal tripartite access structures and the characterization of the ideal hierarchical access structures, which were open problems, a new characterization of the ideal weighted threshold access structures, and a new family of ideal multipartite secret sharing schemes that generalizes several previous constructions. Moreover, all the previous results on ideal multipartite access structures are analyzed and reinterpreted in terms of the new connection.

We consider the notion of multipartite matroid and we show that every matroid of this kind is related to an integer polymatroid in which the size of the ground set is the number of parts. Moreover, we show that a multipartite matroid is linearly representable if and only if the associated integer polymatroid is linearly representable. As result, we present

a sufficient condition for a multipartite access structure to admit an ideal linear secret sharing scheme and a necessary condition for a multipartite access structure to be ideal. These conditions are consequences of the results by Brickell and Davenport [20], but the use of a special description of multipartite access structures that was introduced in [85] makes the new conditions easier to check. Consequently, we obtain new properties of the ideal multipartite access structures. The new sufficient condition is specially useful for the construction of ideal schemes. In the previous works, the ideality of an access structures was proved by constructing an ideal linear scheme for it, which is equivalent to find a representation of the matroid associated to the scheme. Now we use the connection with integer polymatroids and, in order to prove that a multipartite access structure is ideal, it is enough to find a small number of vector subspaces (as many subspaces as parts in the access structure) representing the integer polymatroid defined by the access structure. The efficiency of the ideal linear schemes constructed by means of this method is also discussed. Therefore the new combinatorial connection between ideal multipartite access structures and integer polymatroids provides a unified framework to characterize the ideal multipartite access structures and to describe and analyze methods to construct ideal multipartite secret sharing schemes.

In Chapter 5 we formalize the notion of hierarchy in a secret sharing scheme and we analyze the combinatorial properties of their access structures. The class of hierarchical access structures contain many different kinds of access structures studied previously as the multilevel access structures, the hierarchical threshold access structures, and the weighted threshold access structures. In order to characterize the ideal hierarchical access structures, first we characterize the hierarchical matroid ports and then we show that the integer polymatroids associated to them are representable. This result is also used to give a more simple proof of the characterization of the ideal weighted threshold secret sharing schemes. The other family of ideal access structures characterized in this thesis is the family of ideal tripartite access structures. The ideal bipartite access structures were characterized by Padró and Sáez [85], but the characterization of ideal tripartite access structures was an open problem. In this characterization, we also provide an explicit way to construct ideal linear schemes for these access structures.

Both ideal tripartite access structures and ideal hierarchical access structures are related to a particular kind of integer polymatroids that admit a simple linear representation, the boolean polymatroids. These integer polymatroids are studied in Chapter 4 and we show that all the previous constructions of ideal secret sharing schemes in the literature are related to integer polymatroids of this kind. This relation provides a unified and simple view of all these schemes and their access structures. Moreover we present a new family of ideal multipartite secret sharing schemes, the compartmented access structures, which includes several families of access structures that have been studied previously [19, 96, 102].

The results in Chapter 3 and the characterization of ideal tripartite access structures in Chapter 4 have been published in [41]. The rest of the results in Chapter 4 are from [43], and the results in Chapter 5 have been published in [44].

1.4.2 Optimization of Bipartite Secret Sharing Schemes

In Chapter 6 we consider the problem of optimizing secret sharing schemes. We focus our study on multipartite schemes. Although we consider this problem with all generality, we center our attention on the study of the parameters σ, κ, and λ for bipartite access structures. We show a method to compute κ for multipartite access structures, and new optimal secret sharing schemes for bipartite access structures.

In order to study the complexity of bipartite access structures, we show an efficient method that combines the connection between secret sharing schemes and polymatroids presented by Csirmaz [35], the description of multipartite access structures that was introduced in [85], and linear programming. Concretely this method computes the parameter κ for every bipartite access structure, and can be easily extended to multipartite access structures with more parts. Studying different bipartite access structures, we have found properties of the parameter κ that were unknown and new results on the gap between κ, σ, and λ.

The ideal bipartite secret sharing schemes were characterized in [85]. However, very little is known about optimal constructions for bipartite access structures. In this thesis we present a family of optimal linear secret sharing schemes. In order to prove the optimality of the schemes, we present general lower bounds on the complexity of bipartite access structures, which are obtained by means of the independent sequence method [16, 68, 85]. We show that for these access structures λ, κ, and σ coincide. These results improve and generalize the previous results on non-ideal bipartite secret sharing schemes presented in [76, 85].

The results in Chapter 6 have been published in [42].

Chapter 2

Preliminaries

2.1 Secret Sharing Schemes

In this section we give a definition of the secret sharing schemes based on probability theory. For every probability distribution (Ω, p) and set E, we say that a random variable $X : \Omega \to E$ is a random variable on Ω that takes values in E. Hence, for $x \in E$, $X = x$ denotes the event $\{\omega \in \Omega : X(\omega) = x\}$, and $p(X = x) = \sum_{\omega \in X^{-1}(x)} p(\omega)$. The reader is referred to [22, 95] for an introduction to discrete probability theory.

Definition 2.1.1. Let (Ω, p) be a finite probability distribution and $P = \{1, \ldots, n\}$ the set of participants. A *secret sharing scheme* on P consists of random variables $S_0, \ldots, S_n$ on Ω that take values, respectively, in some finite sets $E_0, \ldots, E_n$ such that for every event $\{S_1 = s_1, \ldots, S_n = s_n\}$ with

$$p(S_1 = s_1, \ldots, S_n = s_n) > 0,$$

there exists a unique element $s_0 \in E_0$ such that

$$p(S_0 = s_0 \mid S_1 = s_1, \ldots, S_n = s_n) = 1.$$

A subset $A = \{i_1, \ldots, i_r\} \subseteq P$ is *authorized* if it can determine S_0 from $S_{i_1}, \ldots, S_{i_r}$. That is, if for every event $\{S_{i_1} = s_{i_1}, \ldots, S_{i_r} = s_{i_r}\}$ with

$$p(S_{i_1} = s_{i_1}, \ldots, S_{i_r} = s_{i_r}) > 0,$$

there exists a unique element $s_0 \in E_0$ such that

$$p(S_0 = s_0 \mid S_{i_1} = s_{i_1}, \ldots, S_{i_r} = s_{i_r}) = 1.$$

The subset A is called *non-authorized* if the random variables $S_{i_1}, \ldots, S_{i_r}$ do not give any information about S_0. That is, if for every event $\{S_{i_1} = s_{i_1}, \ldots, S_{i_r} = s_{i_r}\}$ with

$$p(S_{i_1} = s_{i_1}, \ldots, S_{i_r} = s_{i_r}) > 0$$

and for every $s_0 \in E_0$ it follows that

$$p(S_0 = s_0 \mid S_{i_1} = s_{i_1}, \ldots, S_{i_r} = s_{i_r}) = p(S_0 = s_0).$$

The family of authorized subsets of a scheme Σ is called the *access structure*. It is denoted by $\Gamma(\Sigma)$, or simply by Γ. And the family of non-authorized subsets is noted by Δ. From now on, all the secret sharing schemes considered in this work are *perfect*, which means that every subset of P is in Γ or is in Δ.

The access structure of a secret sharing scheme is *monotone increasing*. That is, every subset of P containing a qualified subset is itself qualified. Analogously, the adversary structure is monotone decreasing.

2.1.1 Shamir Secret Sharing Scheme

Shamir [94] presented in 1979 the following scheme. Let $P = \{1, \ldots, n\}$ be the set of participants of the scheme, $\mathbb{K}$ a finite field with $|\mathbb{K}| \geq n$, and $x_1, \ldots x_n$ different nonzero elements from $\mathbb{K}$. The Shamir secret sharing scheme consists of the random variables $S_0, \ldots, S_n$ on $\mathbb{K}^t$ that take values in $\mathbb{K}$, defined as follows:

- $S_0 : (a_0, \ldots, a_{t-1}) \mapsto a_0$,
- $S_i : (a_0, \ldots, a_{t-1}) \mapsto a_0 + a_1 x_i + \ldots + a_t x_i^{t-1}$ for all $i = 1, \ldots, n$,

and the uniform probability distribution is taken on $\mathbb{K}^t$.

In the original paper [94], Shamir describes this scheme in terms of polynomials as follows. Given a secret $s_0 \in \mathbb{K}$, the dealer chooses at random a polynomial $q \in \mathbb{K}[x]$ of degree at most $t-1$ whose 0-degree term equals to s_0. Then the dealer sends privately $q(x_i)$ to the i-th participant for every $i = 1, \ldots, n$. Taking into account the description in terms of polynomials, it is clear that every subset of at least t participants has enough information to compute s_0, and if it has less than t participants then they do not have enough information to determine the secret, and all the elements in $\mathbb{K}$ have the same possibilities of being the secret. Hence the access structure consists of all those subsets of size larger than t, and the rest of subsets are non-authorized.

2.1.2 Shannon Entropy

The entropy of a random variable is a measure of its randomness. It is a useful tool to study the properties of secret sharing schemes. The reader is referred to [29, 109] for a textbook containing basic information about Shannon entropies.

The *Shannon entropy* of a random variable X with probability distribution (Ω, p) that takes values in E is defined by

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

The logarithm is base 2 and the entropy is expressed in bits. By convention, $0 \log 0 = 0$. Observe that $H(X) \geq 0$ for any random variable X, and that the lower bound is reached if there exists $x \in E$ with $p(X = x) = 1$. Moreover, by the Jensen's inequality (see [29], for instance),

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

with equality if and only if is p is uniform.

For every two random variables X, Y taking values in E and E' with joint probability distribution (Ω, p), we define the *joint entropy* of X and Y by

$$H(XY) = -\sum_{x \in E,\, y \in E'} p(X = x, Y = y) \log p(X = x, Y = y).$$

The definition of the joint entropy of more than two random variables is straightforward.

The entropy of X conditioned on a random variable Y with probability distribution (Ω', p') that takes values in E' is

$$H(X \mid Y) = -\sum_{y \in E'} p'(Y = y) H(X \mid Y = y),$$

where $H(X \mid Y = y)$ denotes the entropy of X computed from the conditional probability distribution $(\Omega, p(\cdot \mid Y = y))$. The following property is called the *chain rule*.

Proposition 2.1.2. *For every random variables X, Y,*

$$H(XY) = H(Y) + H(X \mid Y) = H(X) + H(Y \mid X).$$

Another measure of the randomness is the mutual information, which is the amount of uncertainty of a random variable that is lost by knowing another one. The *mutual information* of X and Y is defined by

$$I(X;Y) = H(X) - H(X \mid Y),$$

with the property that $I(X;Y) = I(Y;X)$. The mutual information of X and Y given a random variable Z is defined by

$$I(X;Y \mid Z) = H(X \mid Z) - H(X \mid YZ).$$

As a consequence of the Jensen's inequality, the mutual information of any two random variables X and Y is always nonnegative, and so

$$H(X) \geq H(X \mid Y),$$

with equality if and only if X and Y are independent.

It is known that for any random variable X with probability distribution (Ω, p) that takes values in E satisfies $L \geq H(X)$, where $L = \sum_{x \in E} p(X = x) l(x)$, being $l(x)$ the number of bits needed to describe x. Moreover, it is known that the best possible description satisfies $L \leq H(X) + 1$.

Now, we give an alternative definition of the access structure of a secret sharing scheme in terms of the entropy. Let Σ be a secret sharing scheme on the set of participants P that is defined by the random variables $S_0, \ldots, S_n$. The access structure $\Gamma(\Sigma)$ is the family of subsets $A \subseteq P$ satisfying

$$H(S_0 \mid S_A) = 0,$$

where S_A denotes $\{S_i\}_{i \in A}$. Conversely, $\Delta(\Sigma)$ is the family of subsets $A \subseteq P$ satisfying

$$H(S_0 \mid S_A) = H(S_0).$$

2.1.3 Efficiency of a Scheme

The efficiency of a secret sharing scheme is commonly measured by the length of the shares. Therefore, this parameter depends on the description of the elements in $E_0, \ldots, E_n$. For the purpose of obtaining an efficient scheme, it is preferred a description of $E_0, \ldots, E_n$ as short as possible according to the probability distribution. This is, in fact, a data compression problem. The Shannon entropy is a fundamental measure for this study.

Taking into account the relation between the length of the description of a random variable and the Shannon entropy, we approximate the average length of the elements in E by $H(X)$, assuming the best description of E. Therefore, we measure the efficiency of a scheme in terms of the entropy of its random variables.

The *complexity* of a secret sharing scheme Σ defined by the random variables $S_0, \ldots, S_n$ is

$$\sigma(\Sigma) = \frac{\max_{i \in P} H(E_i)}{H(E_0)},$$

that is, the maximum length of the shares in relation to the length of the secret. In this thesis, the efficiency of the secret sharing schemes is discussed in terms of this parameter. The use of the complexity or its inverse, which is called *information rate*, as a measure of efficiency is standard in the literature, but in some works it is measured in terms of other rates, as the average of the entropies of the shares divided by the entropy of the secret.

Lemma 2.1.3. *Let Σ be a secret sharing scheme on P defined by the random variables $S_0, \ldots, S_n$. If its access structure is connected, then $H(S_i) \geq H(S_0)$ for every $i = 1, \ldots, n$.*

Proof. Let $i \in P$ and $A \subset P$ such that $A \notin \Gamma(\Sigma)$ and $A \cup \{i\} \in \Gamma(\Sigma)$. By the properties of the entropy function,

$$H(S_A) + H(S_0 \mid S_A) + H(S_i \mid S_0 S_A) = H(S_i) + H(S_A \mid S_i) + H(S_0 \mid S_A S_i).$$

Since $H(S_0 \mid S_A) = H(S_0)$ and $H(S_0 \mid S_A S_i) = 0$,

$$\begin{aligned} H(S_0) &= H(S_i) + H(S_A \mid S_i) - H(S_A) - H(S_i \mid S_0 S_A) \\ &= H(S_i \mid S_A) - H(S_i \mid S_0 S_A) \\ &\leq H(S_i). \end{aligned}$$

□

As consequence of this lemma, $\sigma(\Sigma) \geq 1$ for every perfect scheme Σ. If the complexity of a scheme is 1, which is the best possible case, then the scheme is said to be *ideal*. In this case, its access structure is called *ideal* as well.

Not all access structures are ideal, so for any access structure $\Gamma \subseteq \mathcal{P}(P)$ we define the *optimal complexity* of Γ as

$$\sigma(\Gamma) = \inf\{\sigma(\Sigma) \,:\, \Gamma(\Sigma) = \Sigma\},$$

the infimum of the complexities of the secret sharing schemes with access structure Γ. If a secret sharing scheme Σ is not ideal but $\sigma(\Sigma) = \sigma(\Gamma(\Sigma))$, then the scheme is called *optimal*.

2.2 Linear Secret Sharing Schemes

This section is dedicated to the *linear secret sharing schemes*, which are schemes whose random variables are linear applications. These schemes have been also called geometric schemes [59, 96] and monotone span programs [61].

Let Σ be a secret sharing determined by the random variables $S_0, \ldots, S_n$ with probability distribution (Ω, p) that take values, respectively, in $E_0, \ldots, E_n$. If $\Omega, E_0, \ldots, E_n$ are $\mathbb{K}$-vector spaces with finite dimension for some finite field $\mathbb{K}$, the probability distribution is uniform, and the random variables $S_0, \ldots, S_n$ are surjective linear mappings, then Σ is a $\mathbb{K}$-*linear secret sharing scheme*. In this case, we usually describe Σ by the $(n+1)$-tuple $\pi = (\pi_0, \pi_1, \ldots, \pi_n)$ of surjective linear mappings defined by $S_0, \ldots, S_n$ and the $\mathbb{K}$-vector spaces $E_0, \ldots, E_n$, and $E = \Omega$. We denote $\Sigma = \Sigma_0(\pi)$. Since the probability distribution on E is uniform, for every $i = 0, \ldots, n$ the linear mapping π_i induces a probability distribution in each E_i that is also uniform.

Brickell [19] presented a wide family of ideal linear secret sharing schemes, the *vector space secret sharing schemes*, that generalize the constructions of Shamir [94] and Blakley [14]. A $\mathbb{K}$-*vector space secret sharing scheme* is an ideal linear schemes with $E_i = \mathbb{K}$ for all $i = \{0, \ldots, n\}$. The access structure of these schemes is a $\mathbb{K}$-*vector space access structure*. Next, we present an equivalent definition of these schemes due to Massey [71, 72], which highlights the relation between secret sharing schemes and codes.

Let $P = \{1, \ldots, n\}$ be the set of participants. Consider C an $[n+1, k]$-linear code over a finite field $\mathbb{K}$ and M, its generator matrix, which is a $k \times (n+1)$ matrix over $\mathbb{K}$ whose rows span C. Every random choice of a codeword $(s_0, s_1, \ldots, s_n) \in C$ corresponds to a distribution of shares for the secret value $s_0 \in \mathbb{K}$, in which $s_i \in \mathbb{K}$ is the share of the participant i. Every such an ideal scheme is a $\mathbb{K}$-vector space secret sharing scheme. The access structure of this scheme is determined from the linear dependencies among the columns of the matrix M. A subset $A \subseteq P$ is qualified if and only if the column of M with index 0 is a linear combination of the columns whose indices correspond to the players in A. In order to calculate the secret, for every authorized subset $A \subseteq P$ there is a vector $\lambda = (\lambda_i)_{i \in A} \in \mathbb{K}^{|A|}$ such that for all $x \in E$,

$$\pi_0(x) = \sum_{i \in A} \lambda_i \pi_i(x). \tag{2.1}$$

Example 2.2.1. Let Σ be a Shamir secret sharing scheme with threshold t on the set of participants $P = \{1, \ldots, n\}$ (Section 2.1.1). The random variables of the scheme are linear mappings, and so the scheme is linear. If $x_0, \ldots, x_n$ are the elements in $\mathbb{K}$ corresponding to the participants and the dealer, the i-th column of the generator matrix of the scheme is

$$(1, x_i, \ldots, x_i^{t-1})^T.$$

The matrices of this kind are called *Vandermonde* matrices, and have the property that any subset of at most t columns is linearly independent.

By identifying $\mathbb{K}^t$ with $\mathbb{K}[X]^{t-1}$, the vector space of polynomials of degree at most $t-1$, by means of this natural mapping

$$(a_0, \ldots, a_{t-1}) \mapsto a_0 + a_1 X + \ldots + a_t X^{t-1},$$

the Shamir secret sharing scheme can be described by the mappings $(\pi_0, \ldots, \pi_n)$ defined as

$$\begin{array}{rccc} \pi_i : & \mathbb{K}[X]^{t-1} & \longrightarrow & \mathbb{K} \\ & f & \mapsto & f(x_i). \end{array}$$

Let $s_1, \ldots, s_n$ be the shares received by the participants and s_0 the secret. It is clear that any subset $A \subseteq P$ of at least t participants can recover the unique polynomial $f \in \mathbb{K}[X]$ of degree at most $t-1$ satisfying $f(x_i) = s_i$ for all $i \in A$. This polynomial is defined as

$$f(X) = \sum_{i \in A} s_i \cdot f_i(X) \qquad \text{where} \qquad f_i(X) = \prod_{j \in A, j \neq i} \frac{X - x_j}{x_i - x_j}.$$

Note that to recover the secret in the Shamir secret sharing scheme, it is sufficient to compute $f(x_0)$, and is not necessary to reconstruct the full polynomial $f(X)$. Therefore, it is enough to compute

$$s_0 = \sum_{i \in A} s_i \cdot \lambda_i,$$

where $\lambda_i = f_i(x_0)$ for every $i \in A$.

More generally, any linear secret sharing schemes can be described in terms of the matrix that is defined by the linear applications $\pi_0, \pi_1, \ldots, \pi_n$, because these applications can be defined in terms of elements in E^*, the dual vector space of E. If the scheme is not a vector space secret sharing scheme, then this matrix has more than $n+1$ columns. In this case, analogously to vector spaces schemes, a subset $A \subseteq P$ is qualified if and only if the columns of the matrix corresponding to 0 are a linear combination of the columns corresponding to the players in A. Moreover, for every authorized subset $A \subseteq P$ the secret can be obtained as a linear combination of the shares. That is, for every $i \in A$, there exists a mapping $\lambda_i : E_i \to E_0$ such that the equation 2.1 is satisfied for each $x \in E$.

As a consequence of this property, the sum of two secrets can be shared by using the shares of the secrets. That is, for every $x_1, x_2 \in E$,

$$\pi_0(x_1) + \pi_0(x_2) = \sum_{i \in A} \lambda_i(\pi_i(x_1) + \pi_i(x_2)) \tag{2.2}$$

for all $A \in \Gamma$. Therefore, in a linear secret sharing scheme, the sum of the secrets can be shared without having to reveal them, and so share $\pi_0(x_1) + \pi_0(x_2)$ keeping secret both $\pi_0(x_1)$ and $\pi_0(x_2)$. This property has an special interest in the scope of multiparty computation.

Next we present some algebraic properties of the access structure of linear secret sharing schemes that were presented in [84].

Theorem 2.2.2. *Let Σ be a linear secret sharing scheme on the set of participants $P = \{0, \ldots, n\}$ determined by the mappings $\pi_0, \pi_1, \ldots, \pi_n$ defined on the vector space E. For every subset $A \subseteq P$,*

1. *$A \in \Gamma$ if and only if*

$$\bigcap_{i \in A} \ker \pi_i \subseteq \ker \pi_0. \tag{2.3}$$

2. *$A \in \Delta$ if and only if*

$$\bigcap_{i \in A} \ker \pi_i + \ker \pi_0 = E. \tag{2.4}$$

Recall that in this work we just consider perfect secret sharing schemes. Hence, a subset $A \subseteq P$ satisfies the property (2.3) if and only if does not satisfy the property (2.4). Therefore, as a corollary of this theorem we obtain the following characterization of the linear secret sharing schemes.

Corollary 2.2.3. *Let $\mathbb{K}$ be a finite field, and let $E, E_0, \ldots, E_n$ be $\mathbb{K}$-vector spaces. An $(n+1)$-tuple $\pi = (\pi_0, \pi_1, \ldots, \pi_n)$ of surjective linear mappings with $\pi_i : E \to E_i$ for $i = 0, \ldots, n$ defines a $\mathbb{K}$-linear secret sharing scheme on the set of participants $P = \{1, \ldots, n\}$ if and only if*

- *$\bigcap_{i \in P} \ker \pi_i \subseteq \ker \pi_0$, and*
- *for every $A \subseteq P$,*

$$\bigcap_{i \in A} \ker \pi_i \subseteq \ker \pi_0 \qquad \text{or} \qquad \bigcap_{i \in A} \ker \pi_i + \ker \pi_0 = E.$$

As a consequence of the Theorem 2.2.2, the description of the non-authorized subsets of a vector space secret sharing scheme is very simple.

Lemma 2.2.4. *Let Σ be a vector space secret sharing scheme determined by $\pi_0, \pi_1, \ldots, \pi_n$ defined on the vector space E. A subset $A \subseteq P$ is unqualified for Σ if and only if there exists a vector $\mathbf{x} \in E$ such that $\pi_0(\mathbf{x}) = 1$ while $\pi_i(\mathbf{x}) = 0$ for every $i \in A$.*

Every access structure allows a linear construction [57], so we notate $\lambda(\Gamma)$ for the infimum of the complexities of the linear secret sharing schemes with access structure Γ.

Lemma 2.2.5. *For every access structure Γ it follows $\sigma(\Gamma) \leq \lambda(\Gamma)$.*

In any linear scheme Σ defined by $\pi = (\pi_0, \pi_1, \ldots, \pi_n)$ with $\pi_i \colon E \to E_i$ for every $i = 1, \ldots, n$ the probability distribution induced by these mappings in $E_0, \ldots, E_n$ is uniform, so the complexity of the scheme can be computed in terms of the dimension of the vector spaces $E_0, \ldots, E_n$. That is,

$$\sigma(\Sigma) = \frac{\max_{i \in P} \dim E_i}{\dim E_0}.$$

2.3 Matroids and Polymatroids

2.3.1 Matroids

Matroids were defined by Whitney [107] in 1935 and were conceived as an abstraction of matrices. These combinatorial objects abstract and generalize many concepts from linear algebra, including ranks, independent sets, bases, and subspaces, and have many applications in different areas of combinatorics and algebra. The reader is referred to [82, 106] for general references on matroid theory.

First we give a definition of a matroid in terms of its rank function. There are many equivalent ways to define matroids, and we will just present some of them.

Definition 2.3.1. A *matroid* is a pair $\mathcal{M} = (Q, r)$, where Q is a non-empty finite set and r is a mapping $r : \mathcal{P}(Q) \to \mathbb{Z}$ satisfying the following properties for all $X, Y \subseteq Q$:

1. $0 \leq r(X) \leq |X|$, and
2. r is monotone increasing: if $X \subset Y$, then $r(X) \leq r(Y)$, and
3. r is submodular: $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

The set Q and the mapping r are called, respectively, the *ground set* and the *rank function* of the matroid $\mathcal{M}$. If a nonempty subset $X \subseteq Q$ satisfies that $r(X) > r(X \setminus \{p\})$ for every $p \in X$, then X is *independent*. If not, it is *dependent*. The maximal independent subsets are called *bases*, and the minimal dependent subsets are called *circuits*. A matroid is said to be *connected* if, for every two points in the ground set, there exists a circuit containing them.

Proposition 2.3.2. *A collection $\mathcal{I} \subseteq \mathcal{P}(Q)$ is the family of independent sets of a matroid if and only if the following conditions are satisfied.*

1. *$\emptyset \in \mathcal{I}$.*
2. *If $X \in \mathcal{I}$ and $Y \subset X$, then $Y \in \mathcal{I}$.*
3. *If X and Y are in $\mathcal{I}$ and $|X| < |Y|$, then there exists $x \in Y \setminus X$ such that $X \cup \{x\} \in \mathcal{I}$.*

Moreover, for every family $\mathcal{I} \subseteq \mathcal{P}(Q)$ satisfying these conditions, there exists a unique matroid whose independent sets are the subsets in $\mathcal{I}$. The rank function of this matroid r is defined by taking $r(X)$ as the maximum cardinality of the subsets of X in $\mathcal{I}$. Therefore, given such a family $\mathcal{I}$, we can write $\mathcal{M} = (Q, \mathcal{I})$ for the matroid that is determined by it. Note that for every $X \subseteq Q$, a matroid has the property that every maximal independent subset of X has the same cardinality, which is $r(X)$. Similarly to the independent sets, the family $\mathcal{B}$ of the bases determines the matroid.

Proposition 2.3.3. *A non-empty collection $\mathcal{B} \subseteq \mathcal{P}(Q)$ is the family of bases of a matroid on Q if and only if satisfies the* exchange condition*:*

- *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 $\mathcal{B}$.*

All bases have the same number of elements, which is the *rank* of $\mathcal{M}$ and is denoted by $r(\mathcal{M})$. Actually, $r(\mathcal{M}) = r(Q)$. The independent subsets of the matroid determined by $\mathcal{B}$ is defined as

$$\mathcal{I} = \bigcup_{B \in \mathcal{B}} \{I \subseteq B\}$$

A matroid $\mathcal{M} = (Q, r)$ is said to be $\mathbb{K}$-*linearly representable* (or $\mathbb{K}$-*representable* for short) if there exists a matrix M with coefficients in $\mathbb{K}$ and columns $\{v_i\}_{i \in Q}$, such that

$$r(X) = \dim_{\mathbb{K}} \langle v_i \rangle_{i \in X}$$

for every $X \subseteq Q$. In this case, a subset $X \subseteq Q$ is independent if and only if the corresponding columns of M are linearly independent. The following result is a necessary condition for a matroid to be representable and is due to Ingleton [56].

Theorem 2.3.4. *If a matroid $\mathcal{M} = (Q, r)$ is representable, then for any subsets $A, B, C, D \subseteq Q$,*

$$r(A) + r(B) + r(A \cup B \cup C) + r(A \cup B \cup D) + r(C \cup D) \leq \\ \leq r(A \cup B) + r(A \cup C) + r(A \cup D) + r(B \cup C) + r(B \cup D).$$

Example 2.3.5. The Vamos matroid [103] is the matroid of rank four $V = (\{1, \ldots, 8\}, r)$ such that $r(A) = 4$ for every subset$A \subseteq \{1, \ldots, 8\}$ of size 4 except $\{1, 2, 3, 4\}$, $\{1, 2, 5, 6\}$, $\{3, 4, 5, 6\}$ $\{3, 4, 7, 8\}$ and $\{5, 6, 7, 8\}$. This is one of the smallest matroids that are not representable over any field.

2.3.2 Polymatroids

Polymatroids are a generalization of matroids and were defined by Edmonds [40]. As matroids, polymatroids can be defined in several equivalent ways. Here we present the one in terms of the rank function. The reader is referred to [106] for more information.

Definition 2.3.6. A polymatroid is a pair $\mathcal{S} = (Q, h)$, where Q is a non-empty finite set and h is a mapping $h : \mathcal{P}(Q) \to \mathbb{R}^+$ satisfying the following properties:

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

The set Q and the mapping h are called, respectively, the *ground set* and the *rank function* of the polymatroid $\mathcal{S}$. If h is integer-valued, we say that $\mathcal{S}$ is an *integer* polymatroid. Observe that a matroid is an integer polymatroid $\mathcal{M} = (Q, r)$ such that $r(X) \leq |X|$ for every $A \subseteq Q$.

Let $\mathcal{S}_1 = (Q, h_1)$ and $\mathcal{S}_2 = (Q, h_2)$ be two polymatroids on the same ground set. Clearly, $h = h_1 + h_2$ is the rank function of a polymatroid on Q, which is called the *sum* of $\mathcal{S}_1$ and $\mathcal{S}_2$ and is denoted by $\mathcal{S}_1 + \mathcal{S}_2 = (Q, h)$. For every polymatroid (Q, h), the pair (Q, ah) is also a polymatroid for any $a \in \mathbb{R}$ with $a > 0$.

For an integer $m \geq 1$, we notate $J_m = \{1, \ldots, m\}$. Let $\mathbb{Z}_+^m$ denote the set of vectors $u = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ with $u_i \geq 0$ for every $i \in J_m$. If $u, v \in \mathbb{Z}_+^m$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J_m$, and we write $u < v$ if $u \leq v$ and $u \neq v$. The *modulus* of a vector $u \in \mathbb{Z}_+^m$ is $|u| = u_1 + \cdots + u_m$. For every subset $X \subseteq J_m$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^X$ and $|u(X)| = \sum_{i \in X} u_i$.

The points $x \in \mathbb{R}_+^Q$ satisfying that $x(A) \leq h(A)$ for all $A \subseteq Q$ are called the *independent points* of $\mathcal{S}$. Analogously to matroids, for every $x \in \mathbb{R}_+^Q$, the maximal independent points smaller or equal than x have the same modulus. The region of $\mathbb{R}_+^Q$ determined by the independent points is called the *independence polytope* of the polymatroid.

Edmonds [40] gave a description of the vertices of the polyhedron determined by this polytope. For any permutation $\pi = (i_1, \ldots, i_n)$ of Q, define $A_\pi^1 = \{i_1\}, A_\pi^2 = \{i_1, i_2\}, \ldots, A_\pi^n =$

$\{i_1, \ldots, i_n\}$. The vertices of the independence polytope are all the points $x = x(k, \pi) \in \mathbb{R}_+^Q$ where

$$\begin{aligned} x_{i_1} &= h(A_\pi^1), \\ x_{i_2} &= h(A_\pi^2) - h(A_\pi^1), \\ &\vdots \\ x_{i_k} &= h(A_\pi^k) - h(A_\pi^{k-1}) \\ x_{i_{k+1}} &= 0 \\ &\vdots \\ x_{i_n} &= 0 \end{aligned}$$

and k ranges over the integers 0 to n and π ranges over all permutations of Q.

2.3.3 Integer Polymatroids

For every $u, v \in \mathbb{Z}_+^m$, the vector $w = u \vee v$ is defined by $w_i = \max\{u_i, v_i\}$, and $z = u \wedge v$ by $z_i = \min\{u_i, v_i\}$.

An integer polymatroid $\mathcal{S} = (Q, h)$ is $\mathbb{K}$-*linearly representable* for a finite field $\mathbb{K}$ (or $\mathbb{K}$-*representable* for short) if there exist a vector space E with finite dimension over $\mathbb{K}$, and a subspace $V_i \subseteq E$ for every $i \in Q$ such that

$$h(A) = \dim_{\mathbb{K}} \left(\sum_{i \in A} V_i \right)$$

for every $A \subseteq Q$.

We define the *integer points* of an integer polymatroid $\mathcal{Z} = (J, h)$ as the independent points with integer coordinates of the polytope determined by $\mathcal{Z}$. The family of independent points is denoted by $\mathcal{D}$. That is,

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

Then $\mathcal{D}$ satisfies the following properties.

1. $\mathcal{D}$ is nonempty and finite.
2. If $u \in \mathcal{D}$ and $v \in \mathbb{Z}_+^m$ is such that $v \leq u$, then $v \in \mathcal{D}$.
3. For every pair of vectors $u, v \in \mathcal{D}$ with $|u| < |v|$, there exists $w \in \mathcal{D}$ with $u < w \leq u \vee v$.

Conversely, for every set $\mathcal{D} \subset \mathbb{Z}_+^m$ satisfying these properties, there exists a unique integer polymatroid $\mathcal{Z} = (J_m, h)$ such that $\mathcal{D} = \mathcal{D}(\mathcal{Z})$. Actually, the rank function $h \colon \mathcal{P}(J_m) \to \mathbb{Z}$ of this integer polymatroid is determined by

$$h(X) = \max\{|u(X)| \,:\, u \in \mathcal{D}\}.$$

Herzog and Hibi [53] defined a *discrete polymatroid* as the set of integer points of an integer polymatroid. In this work, we use the results on discrete polymatroids, but we don't use this notation, we call $\mathcal{D}(\mathcal{Z})$ the set of integer points of $\mathcal{Z}$.

An *integer basis* of an integer polymatroid $\mathcal{Z} \subseteq \mathbb{Z}_+^m$ is a maximal element in $\mathcal{D}(\mathcal{Z})$, that is, a vector $u \in \mathcal{Z}$ such that there does not exist any $v \in \mathcal{D}$ with $u < v$. Since we are not going to consider here any other kind of bases of integer polymatroids, from now on integer bases will be called simply bases. Similarly to matroids, all the bases have the same modulus. In addition, an integer polymatroid is determined by its bases. The next proposition is proved in [53, Theorem 2.3].

Proposition 2.3.7. *A nonempty subset $\mathcal{B} \subset \mathbb{Z}_+^m$ is the family of bases of a integer polymatroid if and only if it satisfies the following property, that is called the* exchange condition.

- *For every $u \in \mathcal{B}$ and $v \in \mathcal{B}$ with $u_i > v_i$, there exists $j \in J_m$ such that $u_j < v_j$ and $u - \mathbf{e}_i + \mathbf{e}_j \in \mathcal{B}$, where $\mathbf{e}_i$ denotes the i-th vector of the canonical basis of $\mathbb{R}^m$.*

Since the family of bases determine the integer points of an integer polymatroid, integer polymatroids can also be defined by this condition.

There are some combinatorial structures, related to the polymatroids restricted to subsets of the ground set, that will be frequently used is the following chapters. For every subset $X \subseteq J$, the integer polymatroid $\mathcal{Z}(X) = (X, h)$ has ground set X and its rank function is the one of $\mathcal{Z}$ restricted to $\mathcal{P}(X)$. In this situation $\mathcal{Z}(X)$ is called the *restriction* of $\mathcal{Z}$ to X, and $\mathcal{Z}$ is an *extension* of $\mathcal{Z}(X)$. We consider as well $\mathcal{D}(\mathcal{Z}(X))$, the set of integer points of $\mathcal{Z}(X)$, $\mathcal{D}(\mathcal{Z}(X)) = \{u(X) : u \in \mathcal{D}\} \subset \mathbb{Z}_+^{|X|}$, and the set $\mathcal{B}(\mathcal{Z}, X) \subset \mathbb{Z}_+^{|J|}$ of the vectors $u \in \mathbb{Z}_+^{|J|}$ such that $u(X)$ is a basis of $\mathcal{Z}(X)$ and $u_i = 0$ for every $i \in J \smallsetminus X$. Note that $\mathcal{B}(\mathcal{Z}, X)$ is not the set of bases of $\mathcal{Z}(X)$ but there is a clear correspondence between these structures. These definitions simplify considerably the notation.

As we have seen in Section 2.3, polymatroids can be defined as well in terms of convex polytopes. It is clear that the rank function is integer valued if and only if all the vertices of the convex polytope are integer. Therefore, the polytope associated to an integer polymatroid is the convex hull of its integer points.

2.4 Secret Sharing Schemes and Polymatroids

This section is a survey of the main results about the relation between secret sharing schemes and polymatroids and matroids.

Let Σ be a secret sharing scheme on the set of participants $P = Q \smallsetminus \{0\}$ with access structure Γ, and let $\{S_i\}_{i \in Q}$ be the random variables associated to the shares and the secret.

Proposition 2.4.1. *The set Q together with the mapping $h : \mathcal{P}(Q) \to \mathbb{R}$ defined by*

$$h : X \to H(S_X)/H(S_0).$$

is a polymatroid

This proposition is a consequence of the fact that the entropies of any set of random variables determine a polymatroid, which was proved by Fujishige [46]. We note this polymatroid by $\mathcal{S}(\Sigma)$.

Let $\mathcal{S} = (Q, h)$ be a polymatroid. We say that $p_0 \in Q$ is an *atomic point* of $\mathcal{S}$ if, for every $X \subseteq Q$, either

$$h(X \cup \{p_0\}) = h(X) \quad \text{or} \quad h(X \cup \{p_0\}) = h(X) + 1.$$

Every polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$ defines an access structure $\Gamma_{p_0}(\mathcal{S})$ on the set $P = Q \setminus \{p_0\}$ by

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

In this situation, we say that $\mathcal{S}$ is a Γ-*polymatroid*.

Therefore, every secret sharing scheme Σ defines the polymatroid $\mathcal{S}(\Sigma) = (Q, h)$ in which the dealer p_0 is an atomic point of $\mathcal{S}$. Moreover, the access structure Γ of Σ is univocally determined by the polymatroid $\mathcal{S}$ because $\Gamma = \Gamma_{p_0}(\mathcal{S})$. For a polymatroid $\mathcal{S} = (Q, h)$, we define

$$\sigma(\mathcal{S}) = \max\{h(\{i\}) \,:\, i \in Q\}.$$

Observe that $\sigma(\Sigma) = \sigma(\mathcal{S}(\Sigma))$ for every secret sharing scheme Σ.

A polymatroid $\mathcal{S} = (Q, h)$ is *entropic* if there exist some random variables $\{E_i\}_{i \in Q}$ and a real number $a > 0$ such that $h(A) = aH(E_A)$ for every $A \subseteq Q$. If these random variables are $\mathbb{K}$-*linear*, that is, if they are defined from surjective linear maps $\pi_i \colon E \to E_i$, where E and E_i for $i \in Q$ are $\mathbb{K}$-vector spaces and the uniform probability distribution is taken on E, then the polymatroid $\mathcal{S}$ is said to be $\mathbb{K}$-*linearly entropic*. By considering the subspaces $(\ker \pi_i)^\perp \subseteq E^*$ for $i \in Q$, it is easy to prove that a polymatroid $\mathcal{S} = (Q, h)$ is $\mathbb{K}$-linearly entropic if and only if there exist a real number $b > 0$ such that (Q, bh) is a $\mathbb{K}$-representable integer polymatroid.

Let Γ be an access structure on the set $P = Q \setminus \{p_0\}$ and let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid. Then $\mathcal{S}$ is entropic if and only if there exists a secret sharing scheme Σ with access structure Γ such that $\mathcal{S} = \mathcal{S}(\Sigma)$. Moreover, $\mathcal{S}$ is linearly entropic if and only if there exists a linear secret sharing scheme with these properties. Because of that,

$$\sigma(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \mathcal{S} \text{ is an entropic } \Gamma\text{-polymatroid}\}$$

and

$$\lambda(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \mathcal{S} \text{ is a linearly entropic } \Gamma\text{-polymatroid}\}.$$

In addition, we define

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

Clearly, $\kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$ for every access structure Γ.

If $\mathcal{S} = (Q, h)$ is a polymatroid and $Q' \subseteq Q$, we consider the polymatroid $\mathcal{S}(Q') = (Q', h)$ defined by restricting the rank function h to the subsets of Q'. In this situation, $\mathcal{S}$ is an extension of $\mathcal{S}(Q')$. A polymatroid $\mathcal{S} = (P, h)$ is said to be *compatible* with an access structure Γ on P if there exists a Γ-polymatroid $\mathcal{S}' = (Q, h)$ with $Q = P \cup \{p_0\}$ and $\mathcal{S} = \mathcal{S}'(P)$. Clearly,

$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \mathcal{S} \text{ is a polymatroid compatible with } \Gamma\}.$$

Similar results do not hold for the parameters σ and λ because the extensions of a (linearly) entropic polymatroid are not necessarily (linearly) entropic. The next result, which is a consequence of [35, Proposition 2.3], characterizes the polymatroids that are compatible with a given access structure.

Proposition 2.4.2 ([35]). *A polymatroid $\mathcal{S} = (P, h)$ is compatible with an access structure Γ on P if and only if the following conditions are satisfied.*

1. *If $A \subset B \subseteq P$ and $A \notin \Gamma$ while $B \in \Gamma$, then $h(A) \leq h(B) - 1$.*
2. *If $A, B \in \Gamma$ and $A \cap B \notin \Gamma$, then $h(A \cup B) + h(A \cap B) \leq h(A) + h(B) - 1$.*

Now we present the results on secret sharing schemes and matroids. These results are based on the following connection, that was found by Brickell and Davenport [20].

Theorem 2.4.3. *If Σ is an ideal secret sharing scheme, then the polymatroid $\mathcal{S}(\Sigma)$ is a matroid.*

All elements in the ground set of a matroid are atomic points. An access structure Γ on P is a *matroid port* if there exists a matroid $\mathcal{M} = (Q, r)$ with $Q = P \cup \{p_0\}$ such that:

$$\Gamma = \Gamma_{p_0}(\mathcal{M}) = \{X \subseteq Q \smallsetminus \{p_0\} \,:\, r(X \cup \{p_0\}) = r(X)\}.$$

Observe that the minimal subsets of Γ are in correspondence with the circuits of $\mathcal{M}$ containing the point p_0. Matroid ports were introduced in 1964 by Lehman [65] to solve the Shannon switching game, but note that the original definition was slightly different.

We say that an access structure is *connected* if every participant is in a minimal qualified subset. If Γ is a connected matroid port, then there exists a unique connected matroid $\mathcal{M}$ with $\Gamma = \Gamma_{p_0}(\mathcal{M})$. This is a consequence of the following two facts. First, by [82, Proposition 4.1.2], the matroid $\mathcal{M}$ is connected if and only if one of its ports is connected, and in this case all the ports of $\mathcal{M}$ are connected. Second, a connected matroid is determined by the circuits that contain some given point [82, Theorem 4.3.2].

As a corollary of Theorem 2.4.3, every ideal access structure is a matroid port. Hence, being a matroid port is a necessary condition for an access structure to be ideal, but it is not sufficient. There are matroid ports that do not admit ideal secret sharing schemes, as the ports of the Vamos matroid [4, 20], defined in Example 2.3.5.

Matroids that are obtained from ideal secret sharing schemes are said to be *secret sharing representable*, or *ss-representable* for short. Clearly, ideal access structures are the ports of ss-representable matroids. Moreover, by taking into account the linear construction by Brickell [19] (presented in Section 2.2), we obtain the following result.

Theorem 2.4.4. *The ports of representable matroids are ideal access structures.*

Actually, the ports of representable matroids coincide with the vector space access structures. If a matroid $\mathcal{M}$ is $\mathbb{K}$-representable, then every $\mathbb{K}$-representation M is the generator matrix of a $\mathbb{K}$-vector space secret sharing scheme. However, this condition is not necessary because of the non-Pappus matroid, which is not representable but was proved to be ss-representable by Simonis and Ashikhmin [97]. Concretely, they presented an access structure that does not admit a vector space secret sharing scheme but admits an ideal linear secret sharing scheme in which the dimension of the shares and the secret is 2. The matroids that are associated with an ideal linear secret sharing scheme are called *multilinearly representable*, a class that contains the linearly representable matroids. The non-Pappus matroid is not linearly representable, but is multilinearly representable. The existence of ss-representable matroids that are not multilinearly representable is an open problem.

Martí-Farré and Padró [68] improved Theorem 2.4.3 by using a characterization of the forbidden minors of matroid ports that Seymour [92] presented in 1976.

Theorem 2.4.5. *If an access structure Γ is not a matroid port, then $\kappa(\Gamma) \geq 3/2$. In particular, every access structure with $\sigma(\Gamma) < 3/2$ is a matroid port.*

2.5 Operations

In this section we introduce three operations that are important in secret sharing, dual, minors and composition. The main interest comes from the behavior of the parameters of the schemes and the access structure under these operations.

2.5.1 Minors

Minors of secret sharing schemes and of access structures correspond to a natural scenario. Namely, if several participants leave the scheme and maybe some of them reveal their shares, then the new access structure will be a minor of the original one.

Let Γ be an access structure on a set P. For any $B \subseteq P$, we consider on the set $P \setminus B$ the access structures $\Gamma \setminus B$ and Γ/B defined by $\Gamma \setminus B = \{A \subseteq P \setminus B : A \in \Gamma\}$ and $\Gamma/B = \{A \subseteq P \setminus B : A \cup B \in \Gamma\}$. These operations are called *deletion* and *contraction*, respectively. Any access structure obtained by a sequence of deletions and contractions of subsets of P is a *minor* of Γ.

Deletion and contraction can also be applied to polymatroids and, in particular, to matroids. For a polymatroid $\mathcal{S} = (Q, h)$ and a subset $B \subseteq Q$, we consider the polymatroids $\mathcal{S} \setminus B = (Q \setminus B, h_{\setminus B})$ and $\mathcal{S}/B = (Q \setminus B, h_{/B})$ with $h_{\setminus B}(X) = h(X)$ and $h_{/B}(X) = h(X \cup B) - h(B)$ for every $X \subseteq Q \setminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by a sequence of such operations is a *minor* of $\mathcal{S}$.

If $\mathcal{S}$ is a Γ-polymatroid, then $\mathcal{S} \setminus B$ is a $(\Gamma \setminus B)$-polymatroid and $\mathcal{S}/B$ is a (Γ/B)-polymatroid. Because of that, $\kappa(\Gamma') \leq \kappa(\Gamma)$ if Γ' is a minor of Γ. In addition, the aforementioned connection between minors and secret sharing implies that $\sigma(\Gamma') \leq \sigma(\Gamma)$ and $\lambda(\Gamma') \leq \lambda(\Gamma)$.

2.5.2 Duals

The *dual* Γ^* of an access structure Γ on P is the access structure on the same set defined by

$$\Gamma^* = \{A \subseteq P : P \setminus A \in \Gamma\}.$$

The minimal authorized subsets of Γ^* are in correspondence with the maximal non authorized subsets of Γ.

From every linear secret sharing scheme Σ for Γ, a linear secret sharing scheme Σ^* for the dual access structure Γ^* with $\sigma(\Sigma^*) = \sigma(\Sigma)$ can be constructed [45, 59]. However, in general, the relation between $\sigma(\Sigma^*)$ and $\sigma(\Sigma)$ is an open problem, and so the relation between $\sigma(\Gamma)$ and $\sigma(\Gamma^*)$ is also an open problem.

The dual of a matroid $\mathcal{M} = (Q, r)$ is the matroid $\mathcal{M}^* = \{Q, r*\}$ whose rank function $r^* : \mathcal{P}(Q) \to \mathbb{Z}$ is defined by

$$r^*(X) = |X| - r(Q) + r(Q - X).$$

Equivalently, it can be defined by its set of bases, which is $\{Q \setminus B : B \in \mathcal{B}(\mathcal{M})\}$. Since for every $p \in Q$ it follows $\Gamma_p(\mathcal{M}^*) = (\Gamma_p(\mathcal{M}))^*$, a dual of a matroid port is a matroid port.

The concept of duality can also be applied to polymatroids [106], but the definition of the dual polymatroid is not unique. By choosing a proper definition, which we present below, Martí-Farré and Padró [68] proved that $\kappa(\Gamma) = \kappa(\Gamma^*)$ for every access structure Γ. For every polymatroid $\mathcal{S} = (Q, h)$, its dual is noted by $\mathcal{S}^* = (Q, h^*)$ and for every $X \subseteq Q$ h^* is defined by

$$h^*(X) = \sum_{x \in X} h(\{x\}) - h(Q) + h(Q \setminus X).$$

2.5.3 Composition

Let $Q_1 = P_1 \cup \{D_1\}$ and $Q_2 = P_2 \cup \{D_2\}$ be, respectively, the sets of participants and the dealers of two $\mathbb{K}$-linear secret sharing schemes Σ_1 and Σ_2 with $Q_1 \cap Q_2 = \emptyset$. Let $\pi_1 = (\pi_i)_{i \in Q_1}$ and $\pi_2 = (\pi_i)_{i \in Q_2}$ be the sequences of mappings defining Σ_1 and Σ_2, and let $\Gamma_1 = \Gamma(\Sigma_1)$ and $\Gamma_2 = \Gamma(\Sigma_2)$.

For any $p \in P_1$ we define $\Sigma' = \Sigma_1[\Sigma_2; p]$ as the composition of Σ_1 and Σ_2 at p. In this scheme, loosely speaking, the secret is shared among $P_1 \setminus \{p\}$ by using Σ_1, and the share of the participant p is reshared among P_2 by using Σ_2. Hence, the access structure of Σ', which is noted by $\Gamma = \Gamma_1[\Gamma_2; p]$, contains all the subsets $A \subseteq Q'$ that satisfy the following properties:

1. $A \cap P_1 \in \Gamma_1$, or
2. $A \cup \{p\} \cap P_1 \in \Gamma_1$ and $A \cap P_2 \in \Gamma_2$.

The set of participants of Σ' is $P' = P_1 \cup P_2 \setminus \{p\}$ and the dealer is D_1. The access structures that can be expressed as the composition of two access structures on sets with at least two participants are called *decomposable*.

In this work we just consider the composition of vector space secret sharing schemes, but this operation can be defined for any pair of secret sharing schemes in which the set of secrets of the latter coincides with the set of shares of a participant in the former. We present the general construction for any two vector space secret sharing schemes, but by choosing the appropriate matrices for the computation of the schemes, the composition can be simplified [32].

Assume that $\pi_i : \mathbb{K}^{d_j} \to \mathbb{K}$ for every $i \in Q_j$ and $j = 1, 2$. Let $\pi' = (\pi'_i)_{i \in Q'}$ be the sequence of linear mappings that define $\Sigma' = \Sigma_0(\pi')$, where $Q' = P' \cup \{D_1\}$. Consider ϕ an isomorphism between $\mathbb{K}^{d_2 - 1}$ and $\ker \pi_{D_2}$, and ψ an isomorphism between $\mathbb{K}$ and $(\ker \pi_{D_2})^\perp$ such that for every $x \in \mathbb{K}$, $\psi(x)$ is the unique element in the intersection of $\pi_{D_2}^{-1}(z)$ and $(\ker \pi_{D_2})^\perp$.

The applications $\pi'_i : \mathbb{K}^{d_1} \times \mathbb{K}^{d_2 - 1} \to \mathbb{K}$ are defined as follows:

1. $\pi'_i(x, y) = \pi_i(x)$ for $i \in Q_1 \setminus \{p\}$

2. $\pi'_i(x, y) = \pi_i(\psi(\pi_p(x)) + \phi(y))$ for $i \in P_2$

The next lemma follows immediately from the description of the composition of schemes.

Lemma 2.5.1. *For every finite field $\mathbb{K}$, the composition of two $\mathbb{K}$-vector space secret sharing schemes is a $\mathbb{K}$-vector space secret sharing scheme.*

If Γ_1 and Γ_2 are ideal and connected, then there exist some matroids $\mathcal{M}_1 = (Q_1, \mathcal{B}_1)$ and $\mathcal{M}_2 = (Q_2, \mathcal{B}_2)$ such that $\Gamma_1 = \Gamma_{D_1}(\mathcal{M}_1)$ and $\Gamma_2 = \Gamma_{D_2}(\mathcal{M}_2)$. The access structure $\Gamma = \Gamma_1[\Gamma_2; p]$ is also ideal and connected, and the associated matroid $\mathcal{M}$ coincides with $\mathcal{M}_1 \oplus_{(p,D_2)} \mathcal{M}_2$, the matroid on the base field $Q_1 \cup Q_2 \setminus \{p, D_2\}$ whose bases are the subsets $B \cup C$ with $B \subseteq Q_1 \setminus \{p\}$, $C \subseteq Q_2 \setminus \{D_2\}$ satisfying one of these properties

1. $B \in \mathcal{B}_1$ and $C \cup \{D_2\} \in \mathcal{B}_2$, or

2. $C \cup \{p\} \in \mathcal{B}_1$ and $B \in \mathcal{B}_2$.

Observe that $r(\mathcal{M}') = r(\mathcal{M}_1) + r(\mathcal{M}_2) - 1$.

Chapter 3

Ideal Multipartite Secret Sharing Schemes

3.1 Introduction

In this chapter we present new results on the characterization of the ideal multipartite access structures and on the construction of ideal multipartite secret sharing schemes. These results are based on a characterization of multipartite matroid ports in terms of integer polymatroids that is also presented in this chapter. By means of this characterization, we obtain a necessary condition for a multipartite access structure to be ideal and a necessary condition for a multipartite access structure to admit a vector space secret sharing scheme.

Our results provide a unified framework, which encloses most of the constructions of in the literature, to describe and analyze methods to construct ideal multipartite secret sharing schemes. Because of that, the open problems related to the efficiency of such constructions can be described in a clearer and simpler way. In Chapters 4 and 5 these results are used to study several families of access structures.

A *multipartite secret sharing scheme* is a scheme in which the set of participants is divided into several parts and all participants in the same part play an equivalent role in the scheme. Secret sharing schemes for multipartite access structures have received considerable attention. This is due to the fact that multipartite secret sharing schemes can be seen as a natural generalization of threshold secret sharing schemes. While in threshold secret sharing schemes all the participants are equivalent, in a multipartite secret sharing scheme the participants are distributed into different classes in which all the participants are equivalent. In addition, similarly to threshold access structures, multipartite access structures can be described in a very compact way, by means of a few conditions that are independent of the total number of participants.

Due to the difficulty (presumably, impossibility) of constructing an efficient secret sharing scheme for every given access structure, it is worthwhile to find families of access structures that admit ideal schemes and have useful properties for their applications. This line of research was initiated by Kothari [63], who posed the open problem of constructing ideal hierarchical secret sharing schemes, and by Simmons [96], who introduced the *multilevel* and *compartmented* secret sharing schemes. Multilevel secret sharing schemes are suitable

for hierarchical organizations, while compartmented secret sharing schemes can be used to initiate actions that require the agreement of different parties. By generalizing the geometric method by Blakley [14], Simmons [96] presented ideal secret sharing schemes for some particular examples of multilevel and compartmented access structures and provided ideas for more general constructions. By introducing the vector space secret sharing schemes, which were partially anticipated by Kothari [63], Brickell [19] was able to find ideal schemes for all multilevel and compartmented access structures. The vast majority of the constructions of ideal secret sharing schemes in the literature are vector space secret sharing schemes. This applies in particular to all the constructions of ideal multipartite secret sharing schemes that are discussed next.

Constructions of ideal secret sharing schemes for variants of the compartmented and multilevel access structures, and also for some tripartite access structures, have been given in [6,9,80,89,101,102]. All these constructions provide vector space secret sharing schemes, but some interesting new techniques are introduced in the ones by Tassa [101] and Tassa and Dyn [102]. Specifically, a random polynomial and some of its derivatives are evaluated in several points to obtain the shares in the scheme proposed in [101], and hence it is based on Birkhoff interpolation, while the constructions in [102] are based on bivariate polynomial interpolation.

Two efficiency questions appear in the construction of ideal multipartite secret sharing schemes. The first one deals with the computation needed to set up such a scheme. In most of the aformentioned constructions, a huge number of determinants, which can grow exponentially on the number of participants, have to be computed in order to check that a scheme with the required access structure is obtained. Brickell [19] proposed a method to avoid these checkings, but it requires that the base field of the scheme is very large. Another strategy has been proposed in [101,102]. Namely, one can estimate the probability that the required access structure is realized by randomly choosing the field elements involved in the construction. But a very large field is also needed in order to obtain a large enough value for that probability. The second question is to minimize the size of the base field among the multipartite vector space secret sharing schemes for a given access structure. It has been studied for particular families of multilevel access structures in [13, 49], and it appears to be a very difficult open problem.

Due to the difficulty of finding general results, the characterization of ideal access structures has been studied for several particular classes of access structures as, for instance, the access structures on sets of four [98] and five [60] participants, the ones defined by graphs [16, 20, 23], and those with three or four minimal qualified subsets [66]. This problem has been considered as well for some families of multipartite access structures. Partial results about weighted threshold access structures were given in [77, 85]. Subsequently, a complete characterization of the ideal access structures in this family was presented by Beimel, Tassa and Weinreb [6]. The ideal bipartite access structures were characterized in [85] and, independently, similar results were presented in [79, 81]. Partial results on the characterization of tripartite access structures have been presented in [6,28,89]. In addition, Herranz and Sáez [89] gave some necessary conditions for a multipartite access structure to be ideal.

In this chapter, we study the characterization of the ideal multipartite access structures. By considering as many parts as participants every access structure is multipartite, and

hence we are not dealing here with a particular family of structures, but with the general problem of characterizing the ideal access structures. We do not solve this open problem, but we present some new results by looking at it under a different point of view. Namely, we investigate the conditions given in Theorem 2.4.3 and Theorem 2.4.4 by taking into account that the set of participants can be divided into several parts formed by participants playing an equivalent role in the structure. We introduce the concept of *multipartite matroid*, which applies to the matroids that are defined from ideal multipartite secret sharing schemes. The study of multipartite matroids leads to *integer polymatroids*, which appear to be a very powerful tool to describe in a compact way multipartite matroids, and hence to characterize multipartite matroid ports. Even though our results can be applied to the general case, their most meaningful consequences are obtained when applied to access structures that are genuinely multipartite. That is, in the case that the number of parts is significantly smaller than the number of participants, or in situations in which the partition is derived from some special organization of the participants as, for instance, in hierarchical access structures.

We investigate how Theorem 2.4.3 can be applied to multipartite access structures. Consequently, we study the properties of multipartite matroid ports. The partition in the set of participants of a matroid port extends to the set of points of the corresponding matroid. We point out that every multipartite matroid with m parts defines a *integer polymatroid* on a set of m points. Integer polymatroids are a particular class of polymatroids. In the same way as matroids abstract some properties related to linear dependencies in collections of vectors in a vector space, integer polymatroids abstract similar properties in collections of subspaces of a vector space. Integer polymatroids have been thoroughly studied by researchers in combinatorial optimization, and the main results can be found in the books [47, 78, 90]. We use here the concise presentation of the basic facts about integer polymatroids by Herzog and Hibi [53], who applied these combinatorial objects to commutative algebra. We present in Theorem 3.3.2 a characterization of multipartite matroid ports, which implies a necessary condition for a multipartite access structure to be ideal. This result is based on the aforementioned connection between integer polymatroids and multipartite matroids, together with the geometric representation of multipartite access structures that was introduced in [85] for the bipartite case. We present some examples showing that this necessary condition is a useful tool to prove that a given multipartite structure is not ideal.

We also study the application of Theorem 2.4.4 to multipartite access structures. Therefore, we study the existence of linear representations for multipartite matroids, and we relate them to linear representations of integer polymatroids. In the same way as in a representation of a matroid a vector is assigned to each point in the ground set, a subspace is assigned to each point in a representation of an integer polymatroid. We prove in Theorem 3.4.1 that a multipartite matroid is representable if and only if the corresponding integer polymatroid is representable. This implies a sufficient condition for a multipartite access structure to be ideal. We think that Theorem 3.4.1 is interesting not only for its implications in secret sharing, but also as a result about representability of matroids. This result is specially useful if the number of parts is small. For instance, a tripartite matroid can have many points, but as a consequence of our result we only have to find three suitable subspaces of a vector space to prove that it is representable. In the following chapter we study the ideal tripartite access structures and we proceed in this way. However, Theorem 3.4.1 does

not provide an efficient algorithm to find a representation of a multipartite matroid from a representation of its associated integer polymatroid. It gives an upper bound on the minimum field size for such a representation, but this bound seems to be far from tight. Therefore, the aforementioned open questions about the search of efficient constructions of ideal multipartite secret sharing schemes are not solved here. Nevertheless, Theorems 3.3.2 and 3.4.1 provide a framework in which those open problems can be better described and studied.

3.2 Ideal Access Structures and Integer Polymatroids

3.2.1 Multipartite Access Structures and Multipartite Matroids

An *m-partition* $\Pi = (X_1, \ldots, X_m)$ of a set X is a disjoint family of m subsets of X with $X = X_1 \cup \cdots \cup X_m$. Let $\Lambda \subseteq \mathcal{P}(X)$ be a family of subsets of X. For a permutation σ on X, we define $\sigma(\Lambda) = \{\sigma(A) : A \in \Lambda\} \subseteq \mathcal{P}(X)$. A family of subsets $\Lambda \subseteq \mathcal{P}(X)$ is said to be Π-*partite* if $\sigma(\Lambda) = \Lambda$ for every permutation σ such that $\sigma(X_i) = X_i$ for every $X_i \in \Pi$. We say that Λ is *m-partite* if it is Π-partite for some m-partition Π.

An equivalent way to define multipartite structures is the following. A family Λ of subsets of X is Π-partite if and only if for all $1 \leq i \leq m$ and for any $p, q \in X_i$, the transposition τ_{pq} satisfies $\tau_{pq}(\Lambda) = \Lambda$. This transposition defines an equivalence relation $\sim$ among the elements in X. For any $p, q \in X$,

$$p \sim q \text{ if and only if } \tau_{pq}(\Lambda) = \Lambda.$$

These concepts can be applied to access structures, which are actually families of subsets of the set of participants, and they can be applied as well to the family of independent sets of a matroid. A matroid $\mathcal{M} = (Q, r)$ is Π-*partite* if its family of independent subsets $\mathcal{I} \subseteq \mathcal{P}(Q)$ is Π-partite.

In a multipartite access structure, the participants in each part play the same role. That is, in an authorized subset, each participant can be substituted by another participant from the same part. Trivially, the Shamir access structure is 1-partite, and every access structure with n participants can be seen as a n-partite access structure in which each part has a unique participant.

The partition Π' is a *refinement* of the partition Π if every set in Π' is a subset of some set in Π. Clearly, if $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite and Π' is a refinement of Π, then Λ is Π'-partite. Among all partitions Π for which a family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite, there exists a partition Π_Λ that is not a refinement of any other such partition. The partition Π_Λ is the one defined by the following equivalence relation: two elements $p, q \in P$ are said to be *equivalent according to* Λ if the transposition τ_{pq} satisfies $\tau_{pq}(\Lambda) = \Lambda$. It is not difficult to check that Λ is Π-partite if and only if Π is a refinement of Π_Λ. This argument, which was given in [89], proves that every family of subsets is multipartite, and moreover there is a *canonical partition* for every family of subsets.

The members of a Π-partite family of subsets are determined by the number of elements they have in each part. We formalize this in the following and we obtain a compact way to represent a multipartite family of subsets.

Let $\Pi = (X_1, \ldots, X_m)$ be a partition of a set X. For every $A \subseteq X$ and $i \in \{1, \ldots, m\}$, we define $\Pi_i(A) = |A \cap X_i|$. The partition Π defines a mapping $\Pi\colon \mathcal{P}(X) \to \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A), \ldots, \Pi_m(A))$. If a family $\Lambda \subseteq \mathcal{P}(X)$ of subsets is Π-partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda)$. That is, Λ is completely determined by the set of vectors $\Pi(\Lambda) \subset \mathbb{Z}_+^m$, and hence we can describe an m-partite family of subsets by using vectors in $\mathbb{Z}_+^m$. We write $\mathbf{p} = \Pi(P) = (|P_1|, \ldots, |P_m|)$ and

$$\mathbf{P} = \Pi(\mathcal{P}(P)) = \{u \in \mathbb{Z}_+^m \,:\, u \leq \mathbf{p}\}.$$

The *support of a vector* $u \in \mathbb{Z}_+^m$ is defined by $\mathrm{supp}(u) = \{i \in J_m \,:\, u_i \neq 0\} \subseteq J_m$, and the *support of a set* $\mathcal{S} \subseteq \mathbb{Z}_+^m$ *of vectors* by $\mathrm{supp}(\mathcal{S}) = \{\mathrm{supp}(u) \,:\, u \in \mathcal{S}\} \subseteq \mathcal{P}(J_m)$. For a partition $\Pi = (P_1, \ldots, P_m)$ of a set P, the *support of a subset* $A \subseteq P$ is $\mathrm{supp}(A) = \mathrm{supp}(\Pi(A))$, and the *support of a* Π*-partite family* $\Lambda \subseteq \mathcal{P}(P)$ is $\mathrm{supp}(\Lambda) = \mathrm{supp}(\Pi(\Lambda))$. If Γ is a Π-partite access structure, we notate $\Delta(\Gamma) = \mathrm{supp}(\Gamma)$. Of course, $\Delta(\Gamma)$ is an access structure on J_m.

3.2.2 Multipartite Matroids and Integer Polymatroids

We discuss in this section the connections between multipartite matroids and integer polymatroids, which are defined in Section 2.3.

Let $\mathcal{M} = (Q, r)$ be a Π-partite matroid, where $\Pi = (Q_1, \ldots, Q_m)$ is an m-partition of the ground set Q. Clearly, the mapping $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by

$$h(X) = r(\bigcup_{i \in X} Q_i)$$

is the rank function of an integer polymatroid $\mathcal{Z}(\mathcal{M}) = (J_m, h)$. It is clear that a Π-partite matroid $\mathcal{M}$ is univocally determined by the partition Π and the associated integer polymatroid $\mathcal{Z}(\mathcal{M})$. This connection between multipartite matroids and integer polymatroids is fundamental for our results. In the same way as matroids abstract some properties of collections of vectors, integral polymatroids do the same with collections of subspaces.

The following result shows the close connection between multipartite matroids and integer polymatroids, and derives from the basic properties of both objects.

Proposition 3.2.1. *Let $\Pi = (Q_1, \ldots, Q_m)$ be an m-partition of a set Q and let $\mathcal{I} \subseteq \mathcal{P}(Q)$ be a Π-partite family of subsets. Then $\mathcal{I}$ is the family of independent sets of a Π-partite matroid $\mathcal{M} = (Q, r)$ if and only if $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is the set of integer points of an integer polymatroid. In addition, if $\mathcal{M} = (Q, r)$ is a Π-partite matroid and $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ is the rank function of the integer polymatroid $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$, then $h(X) = r(\bigcup_{i \in X} Q_i)$ for every $X \subset J_m$.*

For a Π-partite matroid $\mathcal{M} = (Q, \mathcal{I})$, we say that $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is the set of integer points of the *discrete polymatroid associated with* $\mathcal{M}$. Clearly, a Π-partite matroid is univocally determined from its associated integer polymatroid and from the partition Π.

3.3 Multipartite Matroid Ports

By using the connection between multipartite matroids and integer polymatroids we discussed in the previous section, we present a characterization of multipartite matroid ports based on integer polymatroids. This characterization provides a necessary condition for a multipartite access structure to be ideal.

A matroid port is multipartite if and only if the corresponding matroid is multipartite for a similar partition. Specifically, we have the following result.

Lemma 3.3.1. *Let $\mathcal{M} = (Q, r)$ be a connected matroid and, for a point $p_0 \in Q$, consider the partitions $\Pi = (P_1, \ldots, P_m)$ and $\Pi_0 = (\{p_0\}, P_1, \ldots, P_m)$ of the sets $P = Q \setminus \{p_0\}$ and Q, respectively. Then the matroid port $\Gamma = \Gamma_{p_0}(\mathcal{M})$ is Π-partite if and only if the matroid $\mathcal{M}$ is Π_0-partite.*

Before presenting the characterization of multipartite matroid ports, given in the next theorem, it is convenient to define a particular kind of extensions of integer polymatroids, the completions.

For every integer $m \geq 1$, consider the set $J'_m = \{0, 1, \ldots, m\}$. An integer polymatroid $\mathcal{Z}' = (J'_m, h)$ with $h(\{0\}) = 1$ is called a *completion* of $\mathcal{Z} = \mathcal{Z}'(J_m)$. In this situation, we consider the family of subsets $\Delta(\mathcal{Z}') \subseteq \mathcal{P}(J_m)$ defined by

$$\Delta(\mathcal{Z}') = \{X \subseteq J_m \,:\, h(X \cup \{0\}) = h(X)\}.$$

Clearly, $\Delta(\mathcal{Z}')$ is monotone increasing, that is, $\Delta(\mathcal{Z}')$ is an access structure on the set J_m.

Theorem 3.3.2. *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set P and let Γ be a Π-partite access structure on P. Then Γ is a matroid port if and only if there exist an integer polymatroid $\mathcal{Z} = (J_m, h)$, with $h(\{i\}) \leq |P_i|$ for every $i \in J_m$, and a completion $\mathcal{Z}' = (J'_m, h)$ of $\mathcal{Z}$ such that*

$$\min \Gamma = \min \left\{ u \in \mathcal{B}(\mathcal{Z}, X) \,:\, X \in \Delta(\mathcal{Z}') \right\}.$$

Proof. Consider $\Pi = (P_1, \ldots, P_m)$, a partition of the set P, and the corresponding partition $\Pi_0 = (\{p_0\}, P_1, \ldots, P_m)$ of the set $Q = P \cup \{p_0\}$. Let $\mathcal{M} = (Q, r)$ be a connected Π_0-partite matroid and consider the Π-partite matroid port $\Gamma_{p_0}(\mathcal{M})$. Since $\mathcal{M}$ is connected, the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ associated with $\mathcal{M}$ is normalized. Finally, consider the integer polymatroid $\mathcal{Z} = \mathcal{Z}'(J_m)$ and the $\mathcal{Z}$-compatible family of subsets $\Delta = \Delta(\mathcal{Z}') \subseteq \mathcal{P}(J_m)$. We only have to prove that a subset $A \subseteq P$ is in $\Gamma_{p_0}(\mathcal{M})$ if and only if there exist a set $X \in \Delta$ and a vector $u \in \mathcal{B}(\mathcal{Z}, X)$ such that $\Pi(A) \geq u$.

Consider a vector $u = (u_1, \ldots, u_m) \in \mathbb{Z}_+^m$ such that $u \in \mathcal{B}(\mathcal{Z}, X)$ for some $X \in \Delta$, and a subset $A \subseteq P$ with $\Pi(A) \geq u$. We can suppose that $X = \{1, \ldots, r\}$, and hence $u = (u_1, \ldots, u_r, 0, \ldots, 0)$. Consider a subset $B \subseteq A$ with $\Pi(B) = u$. Since $\Pi_0(B) = \widetilde{u} = (0, u_1, \ldots, u_r, 0, \ldots, 0) \in \mathcal{Z}'$, we deduce that B is an independent set of the matroid $\mathcal{M}$. On the other hand, $\Pi_0(B \cup \{p_0\}) = (1, u_1, \ldots, u_r, 0, \ldots, 0) \notin \mathcal{Z}'$ because $\widetilde{u}(X)$ is a basis of $\mathcal{Z}'(X)$ and $h(X \cup \{0\}) = h(X)$. Therefore, $B \cup \{p_0\}$ is a dependent set of $\mathcal{M}$. This, together with the independence of B, implies that $B \in \Gamma_{p_0}(\mathcal{M})$, and hence $A \in \Gamma_{p_0}(\mathcal{M})$.

Let $A \subseteq P$ be a minimal qualified subset of $\Gamma_{p_0}(\mathcal{M})$ and let $X = \{i \in J_m \,:\, A \cap P_i \neq \emptyset\}$. We can suppose that $X = \{1, \ldots, r\}$. Consider $u = \Pi_0(A) = (0, u_1, \ldots, u_r, 0, \ldots, 0)$.

Observe that $u \in \mathcal{D}(\mathcal{Z}')$ because A is an independent set of $\mathcal{M}$. The proof is concluded by checking that $X \in \Delta(\mathcal{Z}')$ and that $u(X)$ is a basis of $\mathcal{Z}'(X)$. If, on the contrary, $u(X)$ is not a basis of $\mathcal{Z}'(X)$, we can suppose without loss of generality that $v = (0, u_1 + 1, u_2, \ldots, u_r, 0, \ldots, 0) \in \mathcal{D}(\mathcal{Z}')$. Since A is a minimal qualified subset of $\Gamma_{p_0}(\mathcal{M})$, the set $A \cup \{p_0\}$ is a circuit of $\mathcal{M}$, and hence $B = (A \cup \{p_0\}) \smallsetminus \{p_1\}$ is an independent set of $\mathcal{M}$ for every $p_1 \in A \cap P_1$. Therefore, $w = \Pi_0(B) = (1, u_1 - 1, u_2, \ldots, u_r, 0, \ldots, 0) \in \mathcal{D}(\mathcal{Z}')$. Since $|v| > |w|$, there exists $x \in \mathcal{D}(\mathcal{Z}')$ with $w < x \leq w \vee v$. This implies that $x = (1, u_1, u_2, \ldots, u_r, 0, \ldots, 0) = \Pi_0(A \cup \{p_0\}) \in \mathcal{D}(\mathcal{Z}')$, a contradiction. Therefore, $u(X)$ is a basis of $\mathcal{Z}'(X)$, and this implies $h(X \cup \{0\}) = h(X)$ because $(1, u_1, u_2, \ldots, u_r, 0, \ldots, 0) \notin \mathcal{D}(\mathcal{Z}')$. Hence, $X \in \Delta(\mathcal{Z}')$. □

For an integer polymatroid $\mathcal{Z} = (J_m, h)$, an access structure $\Delta \subseteq \mathcal{P}(J_m)$ is said to be *compatible with* $\mathcal{Z}$ or *$\mathcal{Z}$-compatible* if $\Delta = \Delta(\mathcal{Z}')$ for some completion $\mathcal{Z}'$ of $\mathcal{Z}$. Clearly, for every $\mathcal{Z}$-compatible access structure $\Delta \subseteq \mathcal{P}(J_m)$, there exists a unique completion $\mathcal{Z}'$ of $\mathcal{Z}$ with $\Delta = \Delta(\mathcal{Z}')$. A characterization of $\mathcal{Z}$-compatible access structures is given in Proposition 3.3.3. This result, which is a consequence of [35, Proposition 2.3], will be very useful in the characterization of ideal access structures, presented in Chapters 4 and 5.

Proposition 3.3.3. *An access structure Δ on J_m is compatible with a integer polymatroid $\mathcal{Z} = (J_m, h)$ if and only if the following conditions are satisfied.*

1. *If $X \subset Y \subseteq J_m$ and $X \notin \Delta$ while $Y \in \Delta$, then $h(X) \leq h(Y) - 1$.*
2. *If $X, Y \in \Delta$ and $X \cap Y \notin \Delta$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y) - 1$.*

The characterization of multipartite matroid ports given in Theorem 3.3.2 seems very involved and difficult to check. Nevertheless, the remainder of this section is devoted to demonstrate the utility of this result in determining whether a given multipartite access structure is a matroid port.

First, we present in Proposition 3.3.4, which is a corollary of Theorem 3.3.2, several efficiently checkable necessary conditions for a multipartite access structure to be a matroid port.

Proposition 3.3.4. *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set P and let Γ be a Π-partite matroid port on P. Let h be the rank function of the integer polymatroid $\mathcal{Z}(\Gamma)$. Then the following conditions are satisfied.*

1. *$\Delta(\Gamma) = \operatorname{supp}(\Gamma)$.*
2. *If $A \in \min \Gamma$, then $|A| = h(\operatorname{supp}(A))$.*
3. *All minimal qualified subsets having the same support have the same cardinality.*
4. *If $A, B \in \min \Gamma$ are such that $\operatorname{supp}(A) \subseteq \operatorname{supp}(B)$, then $|A| \leq |B|$.*
5. *If $A, B, C \in \min \Gamma$ are such that $\operatorname{supp}(C) = \operatorname{supp}(A) \cup \operatorname{supp}(B)$, then $|C| \leq |A| + |B| - 1$.*

Proof. For a set $X \subseteq J_m$, there exists a qualified subset $A \in \Gamma$ with $\operatorname{supp}(A) = X$ if and only if the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ that completes $\mathcal{Z}$ with $\Delta(\mathcal{Z}') = \Delta(\Gamma)$ satisfies $h(X \cup \{0\}) = h(X)$, that is, if and only if $X \in \Delta(\Gamma)$.

If $A \in \min\Gamma$ is a minimal qualified subset with $\operatorname{supp}(A) = X$, then $\Pi(A) \in \mathcal{B}(\mathcal{Z}, X)$ by Theorem 3.3.2, and hence $|A| = h(X)$. If $B \in \min\Gamma$ and $X \subseteq Y = \operatorname{supp}(B)$, then $|A| = h(X) \leq h(Y) = |B|$. If $C \subseteq \min\Gamma$ and $Z = \operatorname{supp}(C) = X \cup Y$ then, by submodularity of h,

$$h(Z \cup \{0\}) + h(X \cap Y \cup \{0\}) \leq h(X \cup \{0\}) + h(Y \cup \{0\}).$$

Since $X, Y, Z \in \Delta(\mathcal{Z})$ and $h(X \cap Y \cup \{0\}) \geq 1$, it follows that $h(Z) + 1 \leq h(X) + h(Y)$, which concludes the proof. □

Collins [28] proved that, in every ideal tripartite access structure, all minimal qualified subsets with maximum support (that is, equal to J_3) have the same cardinality, and he wondered whether this property can be generalized to all ideal multipartite access structures. Herranz and Sáez [89] conjectured an affirmative answer. Proposition 3.3.4 proves and generalizes this conjecture.

A possible strategy to determine whether a given multipartite access structure Γ is matroid-related is to check the necessary conditions given by Proposition 3.3.4 and, if they are satisfied, to assume that Γ is matroid-related and to try to determine $\mathcal{Z} = \mathcal{Z}(\Gamma)$. If this can be done and $\mathcal{Z}$ and $\Delta = \operatorname{supp}(\Gamma)$ are in the conditions of Theorem 3.3.2, then Γ is matroid-related. In some situations a contradiction is obtained, which implies that the structure is not matroid-related. We argue the usefulness of the method by presenting some examples.

Example 3.3.5. The following quadripartite access structures, which are described by their minimal vectors, are not matroid ports because they do not satisfy all the conditions in Proposition 3.3.4.

1. $\min\Pi(\Gamma_1) = \{(2,2,1,1), (1,3,1,2), (2,1,2,1), (1,1,2,2)\}$.
2. $\min\Pi(\Gamma_2) = \{(2,2,0,0), (1,1,1,0)\}$.
3. $\min\Pi(\Gamma_3) = \{(2,1,0,0), (0,0,1,2), (1,3,3,1)\}$.

Therefore, these access structures are not ideal. Moreover, by Theorem 2.4.5, in every secret sharing scheme for one of these access structures, the length of one of the shares must be at least 3/2 times the length of the secret.

We saw in Proposition 3.3.4 how to determine $\Delta(\Gamma)$, and the next result provides some tools to determine $\mathcal{Z}(\Gamma)$.

Proposition 3.3.6. *Let Γ be a Π-partite matroid port, and let h be the rank function of the integer polymatroid $\mathcal{Z}(\Gamma)$. Then the following statements hold for every $X \subseteq J_m$.*

1. *If there exists $A \in \min\Gamma$ with $\operatorname{supp}(A) = X$, then $h(X) = |A|$.*
2. *$h(X) \geq \max\{|u(X)| : u \in \Pi(\min\Gamma)\}$.*

Proof. Consider a subset $X \subseteq J_m$. The first statement is a consequence of Proposition 3.3.4. If $u \in \Pi(\min\Gamma)$, then $u \in \mathcal{D} = \mathcal{D}(\mathcal{Z}(\Gamma))$ by Theorem 3.3.2, and hence $|u(X)| \leq h(X)$. This proves the second statement. □

Corollary 3.3.7. *Let Γ be a connected m-partite matroid port and consider the integer polymatroid $\mathcal{Z} = \mathcal{Z}(\Gamma)$ and the $\mathcal{Z}$-compatible family $\Delta = \Delta(\Gamma)$. Let h be the rank function of $\mathcal{Z}$. For every $X \in \Delta$ and $A \subseteq \bigcup_{i\in X} P_i$, if $|A| = h(X)$ and $|A \cap (\bigcup_{i\in Y} P_i)| \leq h(Y)$ for all $Y \subseteq X$, then $A \in \Gamma$.*

Example 3.3.8. Let Γ be a quadripartite access structure such that

$$\min\Pi(\Gamma) = \{u \in \mathbb{Z}_+^4 \,:\, (1,1,1,1) \leq u \leq (3,4,4,4) \text{ and } |u| = 8\} \cup \{(4,0,0,0)\}.$$

This structure satisfies the necessary conditions in Proposition 3.3.4. Suppose that Γ is a matroid port and consider the integer polymatroid $\mathcal{Z}' = (J_4', h)$ associated to the corresponding 5-partite matroid. If $\Delta = \text{supp}(\Gamma) = \Delta_0(\mathcal{Z}')$, then $\min\Delta = \{\{1\}\}$. In addition, from Theorem 3.3.2, all vectors $u \in \Pi(\min\Gamma)$ with $\text{supp}(u) = J_4$ are in $\mathcal{B}$, the family of the bases of the integer polymatroid $\mathcal{Z} = \mathcal{Z}'(J_4)$. We affirm that

$$\mathcal{B} \subseteq \mathcal{A} = \{u \in \mathbb{Z}_+^4 \,:\, (1,1,1,1) \leq u \leq (4,4,4,4) \text{ and } |u| = 8\}.$$

Consider $u \in \mathcal{B}$. If $u \in \min\Pi(\Gamma)$, then $u \in \mathcal{A}$. If $u \notin \min\Pi(\Gamma)$, by Theorem 3.3.2 there exist $Y \subsetneq J_4$ and $v \in \mathcal{B}(\mathcal{Z}, Y)$ such that $v < u$ and $v \in \Pi(\min\Gamma)$. Clearly, this implies that $(4,0,0,0) < u$, and hence $u_i \leq 4$ if $2 \leq i \leq 4$ because $|u| = 8$. Suppose that $u \not\leq (4,4,4,4)$. This implies that $u_1 \geq 5$, but this is a contradiction with the fact that $h(\{1\}) = 4$ because $(4,0,0,0) \in \Pi(\min\Gamma)$. Suppose now that $(1,1,1,1) \not\leq u$. Without loss of generality we can assume that $u_2 = 0$. Take $v = (2,1,2,3) \in \mathcal{B}$. Since $v_2 > u_2$, there exists $j \in J_4$ with $v_j < u_j$ and $w = v - \mathbf{e}^2 + \mathbf{e}^j \in \mathcal{B}$, which implies that $w \in \Pi(\Gamma)$, but this is not possible because $w_1 < 4$ and $w_2 = 0$. Therefore, $(1,1,1,1) \leq u \leq (4,4,4,4)$ and our affirmation is proved. Since $h(X) = \max\{|u(X)| \,:\, u \in \mathcal{B}\}$ for every $X \subseteq J_4$, we obtain that $h(X) = 4$ if $|X| = 1$, and $h(X) = 6$ if $|X| = 2$, and $h(X) = 7$ if $|X| = 3$, and $h(J_4) = 8$. Then $(3,3,0,0) \in \mathcal{B}(\mathcal{Z}, \{1,2\})$ and, since $\{1,2\} \in \Delta$, this implies that $(3,3,0,0) \in \Pi(\Gamma)$, a contradiction. Therefore, Γ is not a matroid port.

Example 3.3.9. Consider now the quadripartite access structures Γ_1 and Γ_2 with

$$\begin{aligned}
\Pi(\min\Gamma_1) = \{&(2,0,0,0),(1,2,0,0),(1,0,2,0),\\
&(1,1,0,2),(1,0,1,2),(0,2,1,1),(0,1,2,1),(0,1,1,2),(1,1,1,1)\}\\
\Pi(\min\Gamma_2) = \{&(2,0,0,0),(1,2,0,0),(1,0,2,1),(1,1,2,0),\\
&(1,1,0,2),(1,0,1,2),(0,2,1,1),(0,1,2,1),(0,1,1,2),(1,1,1,1)\}.
\end{aligned}$$

These two access structures are matroid ports, and the corresponding integer polymatroids are the polymatroids $\mathcal{Z}_1 = (J_4', h_1)$ and $\mathcal{Z}_2 = (J_4', h_2)$ with $\Delta_1 = \Delta(J_4', h_1)$ and $\Delta_2 = \Delta(J_4', h_2)$ defined as follows. For $i = 1,2$, $\min\Delta_i = \{\{1\},\{2,3,4\}\}$, $h_i(\{j\}) = 2$ for all $j \in J_4$, and $h_i(X) = 4$ for all $X \subseteq J_4$ with $|X| > 2$. For all $\{j,k\} \subset J_4$, $h_i(\{j,k\}) = 3$ except for $h_1(\{1,4\}) = h_2(\{1,4\}) = h_2(\{1,3\}) = 4$.

3.4 Representable Multipartite Matroids

This section is dedicated to the proof of Theorem 3.4.1. This result relates the linear representations of multipartite matroids with the linear representations of its associated integer polymatroid. In particular, it provides a sufficient condition for a multipartite access structure to be vector space access structure that depends only on the minimal points of the structure and is independent from the number of players in every part. Moreover, given a multipartite access structure satisfying this sufficient condition, a method to construct vector space secret sharing schemes for it, which is discussed in Section 3.5, can be derived from Theorem 3.4.1.

Theorem 3.4.1. *Let $\mathcal{M} = (Q, r)$ be a Π-partite matroid such that $|Q| = n$ and $r(\mathcal{M}) = k$. Let $\mathcal{Z}$ be the integer polymatroid defined by $\mathcal{D}(\mathcal{Z}) = \Pi(\mathcal{I})$. If $\mathcal{M}$ is $\mathbb{K}$-linearly representable, then so is $\mathcal{Z}$. In addition, if $\mathcal{Z}$ is $\mathbb{K}$-representable, then $\mathcal{M}$ is $\mathbb{L}$-linearly representable for every field extension $\mathbb{L}$ of $\mathbb{K}$ such that $|\mathbb{L}| > \binom{n}{k}$.*

The first claim in the statement is not difficult to prove. Let $\Pi = (Q_1, \ldots, Q_r)$ be a partition of Q and let $\mathcal{M} = (Q, r)$ be a Π-partite matroid with $r(\mathcal{M}) = k$ and $|Q| = n$. Consider the integer polymatroid $\mathcal{Z}$ with $\mathcal{D}(\mathcal{Z}) = \Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ and its rank function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$. Suppose that $\mathcal{M}$ is represented over the field $\mathbb{K}$ by a matrix M. For every $i \in J_m$, consider the subspace V_i spanned by the columns of M corresponding to the points in Q_i. Then $h(X) = r(\cup_{i\in X} Q_i) = \dim(\sum_{i\in X} V_i)$ for every $X \subseteq J_m$. Therefore, the subspaces $V_1, \ldots, V_m$ are a $\mathbb{K}$-representation of the integer polymatroid $\mathcal{Z}$.

The proof for the second claim in the theorem is much more involved and needs several partial results. Clearly, it is enough to prove that, for every finite field with $|\mathbb{K}| > \binom{n}{k}$, the matroid $\mathcal{M}$ is $\mathbb{K}$-linearly representable if the integer polymatroid $\mathcal{Z}$ with $\mathcal{D}(\mathcal{Z}) = \Pi(\mathcal{I})$ is $\mathbb{K}$-linearly representable.

Assume that $|\mathbb{K}| > \binom{n}{k}$ and that $\mathcal{Z}$ is $\mathbb{K}$-linearly representable. Then there exists a $\mathbb{K}$-linear representation of $\mathcal{Z}$ consisting of subspaces $V_1, \ldots, V_m$ of the $\mathbb{K}$-vector space $E = \mathbb{K}^k$, where $k = h(J_m) = r(\mathcal{M})$. Consider the subset $\widetilde{\mathcal{D}} \subset \mathbb{Z}_+^m$ defined in the following way: an integer vector $u \in \mathbb{Z}_+^m$ is in $\widetilde{\mathcal{D}}$ if and only if there exists a sequence $(A_1, \ldots, A_m)$ of subsets of E such that

1. $A_i \subset V_i$ and $|A_i| = u_i$ for every $i \in J_m$,
2. $A_i \cap A_j = \emptyset$ if $i \neq j$, and
3. $A_1 \cup \cdots \cup A_m \subset E$ is an independent set of vectors.

Lemma 3.4.2. *In this situation, $\widetilde{\mathcal{D}} = \mathcal{D}(\mathcal{Z})$.*

Proof. If $(A_1, \ldots, A_m)$ is a sequence of subsets of E corresponding to an integer vector $u \in \widetilde{\mathcal{D}}$, then $|u(X)| = \sum_{j\in X} |A_j| \leq \dim(\sum_{j\in X} V_j) = h(X)$ for every $X \in J_m$ and, hence, $u \in \mathcal{D}(\mathcal{Z})$. Therefore, $\widetilde{\mathcal{D}} \subseteq \mathcal{D}(\mathcal{Z})$.

We prove now that the subset $\widetilde{\mathcal{D}} \subset \mathbb{Z}_+^m$ is the set of integer points of an integer polymatroid. Clearly, $\widetilde{\mathcal{D}} \neq \emptyset$ and, since $\widetilde{\mathcal{D}} \subseteq \mathcal{D}$, it is finite. Moreover, it is obvious that $v \in \widetilde{\mathcal{D}}$ if $v \leq u$ and $u \in \widetilde{\mathcal{D}}$. Consider $u, v \in \widetilde{\mathcal{D}}$ with $|u| < |v|$. Among all possible pairs of sequences $(A_1, \ldots, A_m)$ and $(B_1, \ldots, B_m)$ corresponding, respectively, to the integer vectors u and v,

we choose one maximizing $\sum_{j=1}^{m} |A_j \cap B_j|$. Let $A = A_1 \cup \cdots \cup A_m$ and $B = B_1 \cup \cdots \cup B_m$. Since $|B| > |A|$, there exists a vector $\mathbf{x} \in B \smallsetminus A$ such that $A \cup \{\mathbf{x}\}$ is an independent set. We claim that, if $\mathbf{x} \in B_i$, then $|B_i| > |A_i|$. If, on the contrary, $|B_i| \leq |A_i|$, there must exist $\mathbf{y} \in A_i \smallsetminus B_i$. Then $(A'_1, \ldots, A'_i, \ldots, A'_m)$, where $A'_i = (A_i \cup \{\mathbf{x}\}) \smallsetminus \{\mathbf{y}\}$ and $A'_j = A_j$ if $j \neq i$, is a sequence corresponding to u and such that $\sum_{j=1}^{m} |A'_j \cap B_j| > \sum_{j=1}^{m} |A_j \cap B_j|$, a contradiction. Therefore, by considering the sequence $(A_1, \ldots, A_i \cup \{\mathbf{x}\}, \ldots, A_m)$, we see that there exists $w \in \widetilde{\mathcal{D}}$ such that $u < w \leq u \vee v$. This proves that $\widetilde{\mathcal{D}}$ is the set of points of an integer polymatroid.

Consider the rank function $\widetilde{h} \colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $\widetilde{\mathcal{D}}$. Given a subset $X \subseteq J_m$, it is clear that

$$\widetilde{h}(X) = \max\{|u(X)| \,:\, u \in \widetilde{\mathcal{D}}\} \leq \dim\left(\sum_{j \in X} V_j\right) = h(X).$$

On the other hand, by considering a basis of the subspace $\sum_{j \in X} V_j$, we can find a vector $u \in \widetilde{\mathcal{D}}$ with $|u(X)| = \dim(\sum_{j \in X} V_j)$ and, hence, $\widetilde{h}(X) \geq h(X)$. Therefore, $\widetilde{\mathcal{D}} = \mathcal{D}(\mathcal{Z})$. □

Lemma 3.4.3. *For every basis u of $\mathcal{Z}$, there exists a basis $B = B_1 \cup \cdots \cup B_m$ of the vector space E such that $B_i \subset V_i$ and $|B_i| = u_i$ for every $i \in J_m$, and $B_i \cap B_j = \emptyset$ if $i \neq j$.*

Proof. A direct consequence Lemma 3.4.2. □

For every $i \in J_m$, take $k_i = \dim V_i$ and $n_i = |Q_i|$. Then $n = n_1 + \cdots + n_m$. Consider the space $\mathbf{M}$ of all $k \times n$ matrices over $\mathbb{K}$ of the form $(M_1|M_2|\cdots|M_m)$, where M_i is a $k \times n_i$ matrix whose columns are vectors in V_i. Observe that the columns of every matrix $M \in \mathbf{M}$ can be indexed by the elements in Q, corresponding the columns of M_i to the points in Q_i. The proof of Theorem 3.4.1 is concluded by proving that there exists a matrix $M \in \mathbf{M}$ whose columns are a $\mathbb{K}$-linear representation of the matroid $\mathcal{M}$.

Lemma 3.4.4. *If $A \subseteq Q$ is a dependent subset of the matroid $\mathcal{M}$, then, for every $M \in \mathbf{M}$, the columns of M corresponding to the elements in A are linearly dependent.*

Proof. Since $u = \Pi(A) \notin \mathcal{D}(\mathcal{Z})$, there exists $X \subseteq J_m$ such that $|u(X)| > h(X) = \dim(\sum_{j \in X} V_j)$. Then the columns of M corresponding to the elements in $A \cap (\cup_{j \in X} Q_j)$ must be linearly dependent. □

Therefore, Lemma 3.4.6 concludes the proof of Theorem 3.4.1. The following technical lemma is needed to prove it. Recall that, over a finite field $\mathbb{K}$, there exist nonzero polynomials $p \in \mathbb{K}[X_1, \ldots, X_N]$ on N variables such that $p(x_1, \ldots, x_N) = 0$ for every $(x_1, \ldots, x_N) \in \mathbb{K}^N$.

Lemma 3.4.5. *Let $p \in \mathbb{K}[X_1, \ldots, X_N]$ be a nonzero polynomial on N variables with degree at most $d < |\mathbb{K}|$ on each variable. Then, there exists a point $(x_1, \ldots, x_N)$ in $\mathbb{K}^N$ such that $p(x_1, \ldots, x_N) \neq 0$.*

Proof. The proof is by induction on N. The result is clear if $N = 1$, because in this case p has at most d roots. If $N > 1$, we can write

$$p = p_0 + p_1 X_N + p_2 X_N^2 + \cdots + p_t X_N^t,$$

where p_i are polynomials on the variables $X_1, \ldots, X_{N-1}$ and $p_t \neq 0$. By the induction hypothesis, there exists a point $(x_1, \ldots, x_{N-1}) \in \mathbb{K}^{N-1}$ with $p_t(x_1, \ldots, x_{N-1}) \neq 0$. By fixing these values for the $N-1$ first variables, we obtain a nonzero polynomial $p(x_1, \ldots, x_{N-1}, X_N)$ of degree $t \leq d$ on the variable X_N. Then there exists $x_N \in \mathbb{K}$ with $p(x_1, \ldots, x_{N-1}, x_N) \neq 0$. □

Now we present a construction of a matrix from the representation of the polymatroid. By fixing a basis of V_i for every $i \in J_m$, we obtain one-to-one mappings

$$\phi_i \colon \mathbb{K}^{k_i} \to V_i \subseteq \mathbb{K}^k.$$

Let $N = \sum_{i=1}^{m} k_i n_i$. By using the mappings ϕ_i, we can construct a one-to-one mapping

$$\Psi \colon \mathbb{K}^N = (\mathbb{K}^{k_1})^{n_1} \times \cdots \times (\mathbb{K}^{k_m})^{n_m} \to \mathbf{M}. \tag{3.1}$$

That is, by choosing an element in $\mathbb{K}^N$, we obtain n_i vectors in V_i for every $i \in J_m$.

Lemma 3.4.6. *There exists a matrix $M \in \mathbf{M}$ such that, for every basis $B \subseteq Q$ of the matroid $\mathcal{M}$, the corresponding columns of M are linearly independent.*

Proof. For every basis $B \subseteq Q$ of the matroid $\mathcal{M}$, we consider the mapping $f_B \colon \mathbb{K}^N \to \mathbb{K}$ defined by $f_B(\mathbf{x}) = \det(\Psi(\mathbf{x})_B)$, where Ψ is the functiondescribed in (3.1) and $\Psi(\mathbf{x})_B$ is the square submatrix of $\Psi(\mathbf{x})$ formed by the k columns corresponding to the elements in B. Clearly, f_B is a polynomial on at most N variables and with degree at most 1 on each variable, because every variable appears in at most one column of $\Psi(\mathbf{x})_B$, and every entry of this matrix is an homogeneous polynomial of degree 1. Let B be a basis of $\mathcal{M}$ and $u = \Pi(B) \in \mathbb{Z}_+^m$. From Lemma 3.4.3, there exists a basis of $\mathbb{K}^k$ of the form $\widetilde{B} = \widetilde{B_1} \cup \cdots \cup \widetilde{B_m}$ with $\widetilde{B_i} \subset V_i$ and $|\widetilde{B_i}| = u_i$ for every $i \in J_m$. By placing the vectors in $\widetilde{B}$ in the suitable positions in a matrix $M \in \mathbf{M}$, we can find a vector $\mathbf{x}_B \in \mathbb{K}^N$ such that $f_B(\mathbf{x}_B) \neq 0$, and hence the polynomial f_B is nonzero for every basis B of $\mathcal{M}$. Therefore, if $\mathcal{B}(\mathcal{M})$ is the family of bases of the matroid $\mathcal{M}$, the polynomial $\mathbf{f} = \prod_{B \in \mathcal{B}(\mathcal{M})} f_B$ is a nonzero polynomial on N variables with degree at most $\binom{n}{k} < |\mathbb{K}|$ on each variable, because $|\mathcal{B}(\mathcal{M})| \leq \binom{n}{k}$. From Lemma 3.4.5, there exists a point $\mathbf{x}_0 \in \mathbb{K}^N$ such that $\mathbf{f}(\mathbf{x}_0) \neq 0$, and hence $f_B(\mathbf{x}_0) \neq 0$ for every basis B of $\mathcal{M}$. Clearly, the matrix $\Psi(\mathbf{x}_0)$ is the one we are looking for. □

The following result is a corollary of Theorem 3.4.1 and deals with the application to integer polymatroids of the sufficient condition for representability in Theorem 2.3.4, the Ingleton inequality.

Theorem 3.4.7. *If an integer polymatorid $\mathcal{Z} = (J, h)$ is representable, then for every $A, B, C, D \subseteq J$,*

$$\begin{aligned} h(A) + h(B) + h(A \cup B \cup C) + h(A \cup B \cup D) + h(C \cup D) \leq \\ \leq h(A \cup B) + h(A \cup C) + h(A \cup D) + h(B \cup C) + h(B \cup D). \end{aligned}$$

3.5 Constructing Ideal Multipartite Secret Sharing Schemes

A sufficient condition for a multipartite access structure to be ideal is easily derived from Theorem 3.4.1. More precisely, a necessary and sufficient condition for a multipartite access structure to admit a vector space secret sharing scheme is obtained.

Corollary 3.5.1. *Let $\Gamma = \Gamma_{p_0}(\mathcal{M})$ be an m-partite matroid port, and let $\mathcal{Z}'$ be the integer polymatroid associated with the $(m+1)$-partite matroid $\mathcal{M}$. Then Γ is a vector space access structure if and only if the integer polymatroid $\mathcal{Z}'$ is representable. Moreover, if $\mathcal{Z}'$ is $\mathbb{K}$-representable, then Γ is a $\mathbb{L}$-vector space access structure for every field extension $\mathbb{L}$ of $\mathbb{K}$ with $|\mathbb{L}| \geq \binom{n+1}{k}$, where n is the number of participants and k is the rank of the matroid $\mathcal{M}$.*

In the following examples, we apply this condition to the multipartite matroid ports in the following example.

Example 3.5.2. Consider the quadripartite matroid ports in Example 3.3.9 and the associated integer polymatroids $\mathcal{Z}_1 = (J_4', h_1)$ and $\mathcal{Z}_2 = (J_4', h_2)$.

$$\begin{aligned}\Pi(\min\Gamma_1) = \{&(2,0,0,0),(1,2,0,0),(1,0,2,0),\\ &(1,1,0,2),(1,0,1,2),(0,2,1,1),(0,1,2,1),(0,1,1,2),(1,1,1,1)\}\\ \Pi(\min\Gamma_2) = \{&(2,0,0,0),(1,2,0,0),(1,0,2,1),(1,1,2,0),\\ &(1,1,0,2),(1,0,1,2),(0,2,1,1),(0,1,2,1),(0,1,1,2),(1,1,1,1)\}.\end{aligned}$$

The access structure Γ_1 does not admit any vector space secret sharing scheme because the rank function of the integer polymatroid $\mathcal{Z}_1(J_4)$ violates the Ingleton inequality (Theorem 3.4.7). This implies that the integer polymatroid $\mathcal{Z}_1$ associated is not representable. Moreover, it is easy to check that the Vamos matroid is a minor of $\mathcal{M}_1$. By taking into account that the ports of the Vamos matroid (Example 2.3.5) are not ideal [93] and the folklore results about minors of access structures that are discussed in [68], we have that the access structure Γ_1 is not ideal.

On the other hand, Γ_2 is a $\mathbb{K}$-vector space access structure for fields of all characteristics. Actually, if $\mathbb{K}$ is a finite field and $\{v_1, \ldots, v_4\}$ is a basis of $\mathbb{K}^4$, the subspaces $V_0 = \langle v_1 + v_2 + v_3 + v_4\rangle$, $V_1 = \langle v_2, v_1 + v_3 + v_4\rangle$, $V_2 = \langle v_1, v_2\rangle$, $V_3 = \langle v_1, v_3\rangle$, and $V_4 = \langle v_1, v_4\rangle$ are a representation of the integer polymatroid $\mathcal{Z}_2$.

As we said before, the existence of efficient methods to construct ideal multipartite access structures is an open problem. Even though the proof of Theorem 3.4.1 can be seen as constructive, it does not provide an efficient algorithm to obtain a representation of a multipartite matroid from a representation of its associated integer polymatroid. Because of that, we cannot derive from Theorem 3.4.1 and efficient method to construct a vector space secret sharing scheme for every given multipartite matroid port satisfying the condition in Corollary 3.5.1.

Another open problem is to determine the minimum size of the finite fields $\mathbb{K}$ for which the a matroid port in the conditions of Corollary 3.5.1 admits a $\mathbb{K}$-vector space secret sharing scheme. Upper and lower bounds on the field size were given by Beutelspacher and

Wettl [13] for some multilevel access structures with two levels. Upper bounds for the case of three levels have been presented recently by Giuletti and Vincenti [49]. Observe that a general upper bound can be derived from Corollary 3.5.1, which is exponential in the number of participants. Nevertheless, it is not known to which extent this general upper bound can be improved.

Nevertheless, our results make it possible to better mark the boundary of these open problems. In addition, while these open problems have been previously studied for particular families of multipartite access structures [6, 9, 13, 19, 49, 80, 85, 89, 101, 102], our approach makes it possible to state them in the most general possible way.

Open Problem 3.5.3. Determine the existence of efficient algorithms to find representations of multipartite matroids from representations of their associated polymatroids.

Open Problem 3.5.4. Given a representable multipartite matroid, determine the minimum size of the fields over which it admits a representation.

Of course, since every matroid is multipartite, Open Problem 3.5.4 is connected to extremely difficult open problems about matroid representation. Therefore, one can only expect to find lower and upper bounds for some special classes of multipartite matroids. A method to attack Open Problem 3.5.3 is derived from the proof of Theorem 3.4.1. Specifically, in order to find a representation of an m-partite matroid $\mathcal{M}$ whose associated polymatroid $\mathcal{Z}$ is representable, we have to search for a matrix of the form $(M_1|M_2|\cdots|M_m)$ over some finite field $\mathbb{K}$, in which the submatrices M_i are in one-to-one correspondence with the subspaces V_i representing the integer polymatroid $\mathcal{Z}$. The columns of every submatrix M_i are vectors in the corresponding subspace V_i. The existence of such a matrix representing the matroid $\mathcal{M}$ is guaranteed by Theorem 3.4.1. The constructions of ideal multipartite secret sharing schemes in [6,9,19,80,85,89,101,102] follow a common strategy. Namely, such a matrix M is constructed in some way and then one has to check that, for every basis of the matroid $\mathcal{M}$, the corresponding columns of M are linearly independent. Or, alternatively, the matrix M is constructed column by column and at every step one has to do the necessary checks for linearly independence. If the field $\mathbb{K}$ is large enough, the columns of M can be randomly chosen with high success probability. The aforementioned works differ in the method to construct the matrix M, and some of those proposals are less inefficient than the others, but most of them require a huge number of checks for linearly independence, which can grow exponentially with the number of participants. Brickell [19] proposed a method to avoid these checks, but it requires that the size of the base field is extremely large. The same happens in the random approach if a reasonable success probability is required.

In order to prove Theorem 3.5.6, we need the following lemma, called the Schwartz - Zippel Lemma [91].

Lemma 3.5.5. *Let $\mathbb{K}$ be a finite field of size q and $p \in \mathbb{K}[x_1, \ldots, x_t]$ a polynomial in which the degree of each variable is at most d. The number of zeros of p in $\mathbb{K}^t$ is at most td/q^{t-1}*

Theorem 3.5.6. *Let $\mathcal{M} = (Q, r)$ be a Π-partite matroid such that $|Q| = n$ and $r(\mathcal{M}) = k$. Let $\mathcal{Z}$ be the integer polymatroid defined by $\mathcal{D}(\mathcal{Z}) = \Pi(\mathcal{I})$, and $N = \sum_{i=1}^{m} k_i n_i$, where $k_i = \dim V_i$ and $n_i = |Q_i|$ for every $i \in J_m$. If $\mathcal{Z}$ is $\mathbb{K}$-representable and x is chosen*

uniformly at random from $\mathbb{K}^N$*, then the matrix* $\Psi(x)$ *described in (3.1) is a* $\mathbb{K}$*-representation of* $\mathcal{M}$ *with probability at least*

$$1 - \binom{n-1}{k-1} N q^{-1}.$$

Proof. Define, as in the proof of Theorem 3.4.1, $k_i = \dim V_i$ and $n_i = |Q_i|$ for every $i \in J_m$, and consider the space $\mathbf{M}$ of all $k \times n$ matrices over $\mathbb{K}$ of the form $(M_1|M_2|\cdots|M_m)$, where M_i is a $k \times n_i$ matrix whose columns are vectors in V_i. Let $x \in \mathbb{K}^N$. By Lemma 3.4.4, if $A \subseteq Q$ is a dependent subset of the matroid $\mathcal{M}$, then the columns of $\Psi(x)$ corresponding to the elements in A are linearly dependent. As in the proof of Lemma 3.4.6, consider for every basis $B \subseteq Q$ of $\mathcal{M}$ the mapping $f_B \colon \mathbb{K}^N \to \mathbb{K}$ defined by $f_B(\mathbf{x}) = \det(\Psi(\mathbf{x})_B)$, which is nonzero. Therefore, the polynomial $\mathbf{f} = \prod_{B \in \mathcal{B}(\mathcal{M})} f_B$, where $\mathcal{B}(\mathcal{M})$ is the family of bases of the matroid $\mathcal{M}$, is a nonzero polynomial on N variables with degree at most $\binom{n-1}{k-1}$. The proof is concluded by noting that, as consequence Lemma 3.5.5, the number of zeroes of $\mathbf{f}$ is at most $\binom{n-1}{k-1} N/q^{N-1}$. □

Chapter 4

Some Families of Ideal Multipartite Secret Sharing Schemes

4.1 Introduction

In the previous chapter, we present a new connection between integer polymatroids and ideal secret sharing schemes. On the basis of this connection, we study the ideal multipartite access structures and we provide a unified framework to describe and analyze methods to construct ideal multipartite secret sharing schemes.

In this chapter and in the following one we present applications of these results. We completely characterize the ideal hierarchical access structures, the ideal tripartite access structures, we analyze all the previous constructions of multipartite secret sharing schemes in terms of this connection, and we present a new family of ideal access structures that generalize multipartite access structures that were previously studied.

We consider a family of integer polymatroids that are very simple and that admit a simple representation, the boolean polymatroids, and we show that all the constructions of ideal multipartite secret sharing schemes found in the literature are related to polymatroids of this kind. This relation with boolean polymatroids provides a unified view of all these constructions and their access structures. We use this relation to find simpler constructions and to provide bounds on the size of the field.

The study of boolean polymatroids provides an interesting scope that we use to characterize the family of ideal tripartite access structures and the family of ideal hierarchical access structures, which were open problems, and to find other families of ideal multipartite access structures, as the family of compartmented access structures, which generalizes the ones in [19, 96, 102]. The study of hierarchical access structures is moved to the following chapter because it needs several specific combinatorial tools.

4.1.1 Compartmented Secret Sharing Schemes

We introduce a new family of ideal multipartite access structures, the *compartmented* access structures. These structures generalize the threshold ones regarding situations in which the participants are from different areas or compartments, and the presence of participants from each of these compartments in authorized subsets must be both guaranteed and limited.

That is, the authorized subsets of a compartmented access structure are those of size larger than a certain threshold in which the number of participants from each part is in a certain range. We show that every compartmented access structure is ideal by representing an ideal vector space secret sharing scheme for each one.

In 1988, Simmons [96] considered a set of participants divided into different parts and asked about the existence of schemes in which the secret can only be recovered by those subsets whose size is larger than a given threshold, and that contain at least a minimum number of participants from each part. Brickell [19] found a solution for this question, and presented a vector space secret sharing scheme for these access structures. Tassa and Dyn [102] found new ideal schemes that solved the question presented by Simmons by using bivariate Lagrange interpolation, a technique that was not previously used in secret sharing. They also designed ideal schemes in which the secret can only be recovered by subsets whose size is larger than a certain threshold, and that the number of participants in each part is limited. The access structures of these schemes were called compartmented access structures *with upper bounds* while the structures considered by Simmons were called compartmented *with lower bounds*.

The compartmented access structures defined herein allow to guarantee and, at the same time, to limit the presence of participants from the compartments in the authorized subsets. Therefore, our family contains all these structures studied previously in [19, 96, 102].

4.1.2 Bipartite And Tripartite Secret Sharing Schemes

In this chapter we present a complete characterization of the ideal bipartite and tripartite access structures and we show that all these structures admit a vector space secret sharing scheme.

The ideal bipartite access structures were completely characterized by Padró and Sáez [85], and similar results were presented independently in [79, 81]. Even though, we give a simpler proof of the characterization by using the connection with integer polymatroids. For multipartite access structures with more than two parts, there is not any similar result in the literature. In the case of tripartite access structures, there are only partial results [6, 28, 89] that present families of ideal tripartite access structures and also necessary conditions for a tripartite access structure to be ideal.

By using Theorem 3.3.2, we characterize the tripartite matroid ports, and by using Theorem 3.4.1 we prove that all matroids related to these structures are representable. Hence, we show that all tripartite matroid ports are vector space access structures. The result for bipartite and tripartite access structures cannot be extended to m-partite access structures with $m \geq 4$, because the Vamos matroid (Example 2.3.5) is quadripartite and is not entropic. Therefore there exist quadripartite matroid ports that are not ideal.

4.2 Families of Representable Integer Polymatroids

In this section we study different kinds of integer polymatroids that are interesting for the study of the ideal multipartite access structures considered in this chapter and in the following. All these polymatroids are obtained by operating on a particular kind of polymatroids,

the boolean ones, which admit a very simple description. The families of integer polymatroids presented herein include the polymatroids associated to most of the ideal multipartite access structures considered in the literature.

4.2.1 Boolean Polymatroids

Definition 4.2.1. An integer polymatroid $\mathcal{Z} = (J, h)$ is *boolean* if there exist a finite set B and a family $\{B_i\}_{i\in J}$ of subsets of B such that, for every $X \subseteq J$,

$$h(X) = \left|\bigcup_{i\in J} B_i\right|.$$

Boolean polymatroids are representable over every finite field. Let $\mathbb{K}$ be a finite field and assume that $B = \{1, \ldots, r\}$, where $r = h(J)$. Let $\{e_1, \ldots, e_r\}$ be a basis of $E = \mathbb{K}^r$, and for every $i = 1, \ldots m$ define V_i the vector subspace generated by the vectors in $\{e_j\}_{j\in B_i}$. Then a $\mathbb{K}$-linear representation of $\mathcal{Z}$ consists of the vector subspaces $(V_i)_{i\in J}$.

Definition 4.2.2. A polymatroid $\mathcal{Z} = (J, h)$ is *modular* if for every $X, Y \subseteq J$,

$$h(X \cup Y) + h(X \cap Y) = h(X) + h(Y).$$

Every modular integer polymatroid is boolean. A boolean polymatroid defined by a family of sets $\{B_i\}_{i\in J}$ is modular if these sets are pairwise disjoint. In this case, the polymatroid admits a linear representation that is even simpler than the described above. Let $\mathcal{Z} = (J, h)$ be a modular integer polymatroid and $\mathbb{K}$ a finite field. Define $a \in \mathbb{Z}_+^J$ by $a_i = h(\{i\})$ for all $i \in J$. For $i = 1, \ldots, r$ define $V_i = \mathbb{K}^{a_i}$, and E as the direct sum of $V_1, \ldots, V_r$. Then $V_1, \ldots, V_m$ form a $\mathbb{K}$-representation of $\mathcal{Z}$. Moreover, $\mathcal{Z}$ has only one basis, $\mathcal{B}(\mathcal{Z}) = \{a\}$.

4.2.2 Operations

Now we present two operations on integer polymatroids that are interesting for the construction of linearly representable polymatroids: the sum and the truncation. The sum is a common operation in the study of polymatroids, and the truncation is the composition of two very well known operations: it is a minor of an extension.

Proposition 4.2.3. *The sum of $\mathbb{K}$-representable integer polymatroids is $\mathbb{K}$-representable.*

Proof. Let $\mathcal{S}_1 = (Q, h_1)$ and $\mathcal{S}_2 = (Q, h_2)$ be two integer polymatroids on the same ground set. Consider two $\mathbb{K}$-vector spaces V and W and two families of subspaces, $(V_i)_{i\in Q}$ with $V_i \subseteq V$ and $(W_i)_{i\in Q}$ with $W_i \subseteq W$, that are $\mathbb{K}$-representations of the polymatroids $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively. Then the subspaces $V_i \oplus W_i \subseteq V \oplus W$ form a $\mathbb{K}$-representation of the integer polymatroid $\mathcal{S}_1 + \mathcal{S}_2$. □

Lemma 4.2.4. *Let $\mathcal{Z}_1 = (J, h_1)$, $\mathcal{Z}_2 = (J, h_2)$ and $\mathcal{Z}_3 = (J, h_3)$ be integer polymatroids. If $\mathcal{B}(\mathcal{Z}_3) = \mathcal{B}(\mathcal{Z}_1) + \mathcal{B}(\mathcal{Z}_2)$ then $\mathcal{Z}_3 = \mathcal{Z}_1 + \mathcal{Z}_2$.*

Proof. If $\mathcal{B}(\mathcal{Z}_3) = \mathcal{B}(\mathcal{Z}_1) + \mathcal{B}(\mathcal{Z}_2)$, then for every $X \subseteq J$

$$\begin{aligned} h_3(X) &= \max\{|u(X)| : u \in \mathcal{B}(\mathcal{Z}_3)\} \\ &= \max\{|u_1(X)| + |u_2(X)| : u_1 \in \mathcal{B}(\mathcal{Z}_1) \text{ and } u_2 \in \mathcal{B}(\mathcal{Z}_2)\} \\ &= \max\{|u_1(X)| : u_1 \in \mathcal{B}(\mathcal{Z}_1)\} + \max\{|u_2(X)| : u_2 \in \mathcal{B}(\mathcal{Z}_2)\} \\ &= h_1(X) + h_2(X), \end{aligned}$$

and so $\mathcal{Z}_3 = \mathcal{Z}_1 + \mathcal{Z}_2$. □

Definition 4.2.5. Let $\mathcal{Z} = (J, h)$ be an integer polymatroid and d a positive integer with $d < h(J)$. Then the map h' defined by

$$h'(X) = \min\{h(X), d\}$$

is the rank function of a polymatroid, the *d-truncation* of $\mathcal{Z}$.

The truncation of an integer polymatroid can be seen as a minor of an extension of the polymatroid. Let $\mathcal{Z} = (J, h)$ be an integer polymatroid. Define $t = h(J)$ and consider $d \in \mathbb{Z}_+$ with $d < t$. Define $J' = J \cup \{p\}$ for some $p \notin J$ and consider $\mathcal{Z}_1 = (J', h_1)$ the extension of $\mathcal{Z}$ such that

$$h_1(X \cup \{p\}) = \min\{h(X) + t - d, t\}$$

for every $X \subseteq J$. It is not difficult to see that $\mathcal{Z}_1$ is indeed an integer polymatroid. Now define $\mathcal{Z}_2 = (J, h_2) = \mathcal{Z}_1/\{p\}$. Observe that for every $X \subseteq J$, $h_2(X) = h_1(X \cup \{p\}) - h_1(\{p\}) = \min\{h(X) + t - d, t\} - (t - d) = \min\{h(X), d\}$.

4.2.3 Truncated Boolean Polymatroids

Proposition 4.2.6. *Let $\mathcal{Z} = (J, h)$ be a boolean polymatroid. All truncations of $\mathcal{Z}$ are $\mathbb{K}$-linearly representable for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq h(J)$.*

Proof. Let $\mathcal{Z}' = (J, h')$ be the truncation of $\mathcal{Z}$ with $h'(J) = t$. Define $r = |B|$. Let $\mathbb{K}$ be a finite field with $|\mathbb{K}| \geq r$ and assume that $B = \{1, \ldots, r\}$. Let $x_1, \ldots, x_r$ be different elements in $\mathbb{K}$ and let $\{e_1, \ldots, e_t\}$ be a basis of $E = \mathbb{K}^t$. Consider the function $v : \mathbb{K} \to E$ defined as

$$v(x) = e_1 + xe_2 + \ldots + x^{t-1}e_t.$$

The vector subspaces $V_1, \ldots, V_m$ defined as $V_i = \langle v(x_j) : j \in B_i \rangle$ form a $\mathbb{K}$-linear representation $\mathcal{Z}'$. □

Definition 4.2.7. An integer polymatroid is called *of Veronese type* if it is the truncation of a modular integer polymatroid.

The integer polymatroids of Veronese kind have been studied in [53, 54]. For every integer polymatroid of Veronese type $\mathcal{Z} = (J, h)$ there exists $a \in \mathbb{Z}_+^m$ and $d \in \mathbb{Z}_+$ for which for all $X \subseteq J$

$$h(X) = \min\left\{d, \sum_{i \in X} a_i\right\}.$$

Their integer points and bases are the following:

$$\mathcal{B}(\mathcal{Z}) = \{x \in \mathbb{Z}^J \,:\, 0 \leq x \leq a \text{ and } |x| = d\}$$

$$\mathcal{D}(\mathcal{Z}) = \{x \in \mathbb{Z}^J \,:\, 0 \leq x \leq a \text{ and } |x| \leq d\}$$

4.2.4 The Strong Exchange Property

The integer polymatroids with the strong exchange property are closely related to the compartmented access structures, which are studied in Section 4.3.2.

Herzog, Hibi, and Vladoiu [54] proved that integer polymatroids with the strong exchange property are, up to an affinity, of Veronese type. We use this result to show that all integer polymatroids with this property are linearly representable over every large enough field (Corollary 4.2.12). Moreover, some combinatorial properties of their bases are used in Section 4.3.2 to describe the compartmented access structures. First we define the strong exchange property for matroids and then for integer polymatroids.

Definition 4.2.8. A matroid $\mathcal{M} = (Q, \mathcal{B})$ has the strong exchange property if for every $B_1, B_2 \in \mathcal{B}$, both $B_1 \smallsetminus \{p\} \cup \{q\}$ and $B_2 \smallsetminus \{q\} \cup \{p\}$ are in $\mathcal{B}$ for all $p \in B_1 \smallsetminus B_2$ and $q \in B_2 \smallsetminus B_1$.

Definition 4.2.9. An integer polymatroid $\mathcal{Z} = (J, h)$ with $\mathcal{B} = \mathcal{B}(\mathcal{Z})$ has the *strong exchange property* if for all $u, v \in \mathcal{B}$ and $i, j \in J$ the following condition is satisfied.

$$\text{If } u_i > v_i \text{ and } u_j < v_j, \text{ then } u - \mathbf{e}_i + \mathbf{e}_j \text{ and } v + \mathbf{e}_i - \mathbf{e}_j \text{ are in } \mathcal{B}. \tag{4.1}$$

Every nonempty set $\mathcal{B} \subseteq \mathbb{Z}_+^m$ satisfying the condition 4.1 for every $u, v \in \mathcal{B}$, also satisfies the exchange condition (Proposition 2.3.7), and so $\mathcal{B}$ is the family of bases of an integer polymatroid. And every restriction of an integer polymatroid with the strong exchange property also has this property. Observe that a multipartite matroid possesses the strong exchange property if and only if its associated integer polymatroid does.

In order to simplify the description of the bases of integer polymatroids with the strong exchange property, we present Proposition 4.2.10, which appears in [54]. For every $u, v \in \mathbb{Z}_+^m$ with $|u| = |v| = d$, we notate

$$[u, v] = \left\{w \in \mathbb{Z}_+^m \,:\, |w| = d \text{ and } u \wedge v \leq w \leq u \vee v\right\}.$$

Proposition 4.2.10. *A set $\mathcal{B} \subseteq \mathbb{Z}_+^m$ is the set of bases of an integer polymatroid with the strong exchange property if and only if $\mathcal{B} = \cup_{u,v \in \mathcal{B}}[u, v]$.*

Theorem 4.2.11. *Every integer polymatroid with the strong exchange property is the sum of a polymatroid of Veronese type and a modular polymatroid.*

Proof. Herzog, Hibi, and Vladoiu proved in [54, Theorem 1.1] that an integer polymatroid $\mathcal{Z}$ with set of bases $\mathcal{B}$ has the strong exchange property if and only if $\mathcal{B}$ is isomorphic of $\mathcal{B}' = \{u \in \mathbb{Z}_+^m \,:\, |u| = t \text{ and } u \leq c\}$ for some $t \in \mathbb{Z}_+$ and $c \in \mathbb{Z}_+^m$. It is proved by showing that there exists $a \in \mathbb{Z}_+^m$ such that $\mathcal{B} = \{x + a \,:\, x \in \mathcal{B}'\}$. Since $\mathcal{B}'' = \{a\}$ is the set of bases of a modular polymatroid $\mathcal{Z}''$, $\mathcal{B} = \mathcal{B}' + \mathcal{B}''$ and so $\mathcal{Z} = \mathcal{Z}' + \mathcal{Z}''$. □

Corollary 4.2.12. *For every integer polymatroid with the strong exchange property $\mathcal{Z} = (J, h)$ there exists $a, b \in \mathbb{Z}_+^J$ and $d \in \mathbb{Z}_+$ with $a \leq b$ and $|a| \leq d \leq |b|$ such that*

1. $\mathcal{B} = \{x \in \mathbb{Z}_+^J : |x| = d \text{ and } a \leq x \leq b\}$, *and*
2. $h(A) = \min\{|b(X)|, d - |a| + |a(X)|\}$ *for all* $X \subseteq J$.

Moreover, it is $\mathbb{K}$-linearly representable for every finite field $\mathbb{K}$ with $|\mathbb{K}| > |b - a|$.

Proposition 4.2.13. *Every integer polymatroid $\mathcal{Z} = (J_m, h)$ with $m \leq 3$ satisfies the strong exchange property.*

Proof. The statement is obvious for $m = 1, 2$. Let $\mathcal{Z} = (J_3, h)$ be an integer polymatroid and consider two different bases $u, v \in \mathcal{B}$. Suppose, without loss of generality, that $u_1 > v_1$, and $u_2 < v_2$, and $u_3 \geq v_3$. Then it is clear that $u - \mathbf{e}_1 + \mathbf{e}_2 \in \mathcal{B}$. Suppose, for the sake of contradiction, that $v - \mathbf{e}_2 + \mathbf{e}_1 \notin \mathcal{B}$, which implies that $h(\{1\}) < v_1 + 1$ or $h(\{1, 3\}) < v_1 + v_3 + 1$. But $v_1 + 1 \leq u_1 \leq h(\{1\})$ and $v_1 + v_3 + 1 \leq u_1 + u_3 \leq h(\{1, 3\})$, a contradiction. □

As consequence of this proposition, we obtain the following corollaries, which are used in the characterization of bipartite and tripartite ideal access structures. Note that Corollary 4.2.14 was proved by Hammer, Romashchenko, Shen, and Vereshchagin [52] in an alternative way.

Corollary 4.2.14. *Every integer polymatroid with ground set J_m with $m \leq 3$ is representable over every large enough field.*

Corollary 4.2.15. *Every m-partite matroid with $m \leq 3$ is representable over every large enough field.*

Observe that the strong exchange property is not a necessary condition for an integer polymatroid to be representable, since for instance boolean polymatroids in general do not satisfy this property.

4.3 Some Families of Ideal Multipartite Access Structures

4.3.1 The Sum of Access Structures

In this section we analyze different tools to construct secret sharing schemes. The result presented in Proposition 4.3.2 is based on the construction in Corollary 3.5.1. Another tool used in this chapter is the composition of vector space secret sharing schemes, which is defined in 2.5.3.

Definition 4.3.1. Let Γ and Γ' be two access structures on P that are $(P_1, \ldots, P_m)$-partite. Then Γ'' is the *sum* of the access structures Γ and Γ' if it is $(P_1, \ldots, P_m)$-partite and

$$\Gamma'' = \{x \in \mathbf{P} : x = u + v, \text{ with } u \in \Gamma_1 \text{ and } v \in \Gamma_2\}$$

In this case we note $\Gamma'' = \Gamma + \Gamma'$.

Proposition 4.3.2. *Let Π be a partition of a set P of n participants, Γ_1 and Γ_2 two Π-partite $\mathbb{K}$-vector space access structures for some finite field $\mathbb{K}$, and $\mathcal{Z}_1 = (J'_m, h_1)$ and $\mathcal{Z}_2 = (J'_m, h_2)$ their associated integer polymatroids. Let $r_1 = h_1(J'_m)$ and $r_2 = h_2(J'_m)$. If*

$$\min \Gamma_1 = \mathcal{B}(\mathcal{Z}_1, J_m) \qquad \text{and} \qquad \min \Gamma_2 = \mathcal{B}(\mathcal{Z}_2, J_m),$$

then the access structure Γ_3 defined as $\Gamma_3 = \Gamma_1 + \Gamma_2$ admits a $\mathbb{L}$-vector space secret sharing scheme for any finite extension $\mathbb{L}$ of $\mathbb{K}$ with $\mathbb{L} > \binom{n+1}{r_1+r_2}$.

Proof. Let $V_0, V_1, \ldots, V_m \subseteq E$ and $W_0, W_1, \ldots, W_m \subseteq F$ be $\mathbb{K}$-representations of $\mathcal{Z}_1$ and $\mathcal{Z}_2$. Let $v \in V_0$ and $w \in W_0$ be non-zero vectors. Define G as the direct sum of E and F, $U_i = V_i \oplus W_i$ for every $i = 1, \ldots, m$, and $U_0 = \langle v + w \rangle$. Define $\mathcal{Z}_3 = (J'_m, h_3)$ as the integer polymatroid linearly represented by $U_0, U_1, \ldots, U_m \subseteq G$ and Γ_3 as the Π-partite access structure that is associated to $\mathcal{Z}_3$. Since $\Delta_3 = \Delta_1 \cap \Delta_2$,

$$\min \Gamma_3 = \min \left\{ \bigcup_{X \in \Delta_3} \mathcal{B}(\mathcal{Z}_3, X) \right\} = \min \left\{ \bigcup_{X \in \Delta_1 \cap \Delta_2} \mathcal{B}(\mathcal{Z}_1, X) + \mathcal{B}(\mathcal{Z}_2, X) \right\}.$$

By hypothesis, for $i = 1, 2$,

$$\min \left\{ \bigcup_{X \in \Delta_1 \cap \Delta_2} \mathcal{B}(\mathcal{Z}_i, X) \right\} = \mathcal{B}(\mathcal{Z}_i, J_m),$$

so it is easy to see that $\min \Gamma_3 = \mathcal{B}(\mathcal{Z}_1, J_m) + \mathcal{B}(\mathcal{Z}_2, J_m) = \min \Gamma_1 + \Gamma_2$. □

4.3.2 Compartmented Secret Sharing Schemes

The definition of compartmented access structures we give in this work is new and is the natural generalization of all the previous definitions [19, 96, 102]. Moreover, we show in Corollary 4.3.7 that all these new access structures are ideal.

Definition 4.3.3. Let P be a set of participants and $\Pi = (P_1, \ldots, P_m)$ a partition of P. A Π-partite access structure Γ is *compartmented* if there exists $a, b \in \mathbb{Z}_+^m$ with $a \leq b$, and $d \in \mathbb{Z}_+$ with $|a| \leq d \leq |b|$ such that

$$\min \Gamma = \{x \in \mathbb{Z}_+^m \,:\, |x| = d \text{ and } a \leq x \leq b\}.$$

The compartmented access structures *with upper bounds* and *with lower bounds* defined in [102] correspond to the compartmented access structures defined above with $a = (0, \ldots, 0)$ and with $b = (|P_1|, \ldots, |P_m|)$, respectively. Observe that if $a = (0, \ldots, 0)$ and $b = (|P_1|, \ldots, |P_m|)$, then it is a threshold access structure. Therefore this new notion of compartmented access structure include all the previous ones.

Compartmented access structures allows to combine upper and lower bounds on the number of participants in each compartment. An equivalent way to describe these access structures is the following.

$$\Gamma = \{x \in \mathbb{Z}_+^m \,:\, |x| \geq d \text{ and } a_i \leq x_i \leq b_i + (|x| - d) \text{ for all } 1 \leq i \leq m\}.$$

Example 4.3.4. Consider a set of participants P with three parts, P_1, P_2 and P_3, and an access structure in which the authorized subsets are those with more than 5 participants with at least 2, 0 and 1 participants in P_1, P_2 and P_3, respectively, satisfying that the minimal authorized subsets have at most 3, 2, and 2 participants in P_1, P_2 and P_3. This structure corresponds to the compartmented access structure determined by $a = (2, 0, 1)$, $b = (3, 2, 2)$ and $d = 5$. The minimal authorized subsets are those $A \subseteq P$ with $\Pi(A)$ equals to $(3, 0, 2)$, $(3, 1, 1)$, $(2, 1, 2)$, or $(2, 2, 1)$. If $\mathbf{P} > (3, 2, 2)$, this access structure does not belong to any previous family of compartmented structures.

For any $a, b \in \mathbb{Z}_+^m$ with $a \leq b$, and $d \in \mathbb{Z}_+$ with $|a| \leq d \leq |b|$, we obtain a compartmented access structure. However, in order to have a more accurate description of the structure, we will assume that these parameters satisfy some additional inequalities. We assume that

- $|P| \geq d$ and that
- $|P_i| \geq b_i$ for all $i = 1, \ldots, m$.

Moreover, in order to have a more clear definition of Γ, we assume that the vectors a and b are *tight* for Γ. That is, we assume that for all $i = 1, \ldots, m$ there exist some $x, y \in \min \Gamma$ with $x_i = a_i$ and $y_i = b_i$. It is equivalent to say that for all $i = 1, \ldots, m$,

$$d - \sum_{j \neq i} b_j \leq a_i \quad \text{and} \quad d - \sum_{j \neq i} a_j \geq b_i \tag{4.2}$$

Now we study two particular kinds of compartmented access structures. This Lemma is used in Theorem 4.3.6 to show that all compartmented access structures admit a vector space secret sharing scheme for every large enough finite field.

Lemma 4.3.5. *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of P, a set of n participants. Let $a \in \mathbb{Z}_+^m$ and $d \in \mathbb{Z}_+$ with $|a| \leq d$.*

1. *The access structure Γ_1 defined by $\min \Gamma_1 = \{a\}$ is ideal. Moreover the associated integer polymatroid is representable over every finite field.*
2. *The access structure Γ_2 defined by $\min \Gamma_2 = \{x \in \mathbf{P} : |x| \geq d \text{ and } x_i \leq a\}$ is ideal. Moreover the associated integer polymatroid is $\mathbb{K}$-representable for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq |a|$.*

Proof. Let $\mathbb{K}$ be a field. Consider the $\mathbb{K}$-representation $V_1, \ldots, V_m \subseteq E$ of $\mathcal{Z}_1 = (J_m, h_1)$, the modular polymatroid with $h(\{i\}) = a_i$. Now define $v = v_1 + \ldots + v_m$, where v_i is a vector in V_i that is nonzero if $F_i \neq \{0\}$. Observe that the integer polymatroid $\mathcal{Z}_1' = (J_m', h_1)$ represented by the vector subspaces $V_0 = \langle v \rangle, V_1, \ldots, V_m$ is the polymatroid associated to Γ_1.

Consider now a finite field $\mathbb{K}$ with $|\mathbb{K}| > |a|$ and a $\mathbb{K}$-representation $V_0, V_1, \ldots, V_m \subseteq E$ of $\mathcal{Z}_2 = (J_m', h_2)$, the d-truncation of a modular polymatroid with $h(\{i\}) = a_i$ for all $i = 1, \ldots, m$ and $h(\{0\}) = 1$. Observe that $\mathcal{Z}_2$ is the integer polymatroid associated to Γ_2. □

Theorem 4.3.6. *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of P, a set of n participants. If Γ is a Π-partite compartmented access structure that is determined by $a, b \in \mathbb{Z}_+^m$ and $d \in \mathbb{Z}_+$, then it admits a $\mathbb{K}$-vector space secret sharing scheme for every finite field $\mathbb{K}$ with $|\mathbb{K}| > \binom{n+1}{d}$.*

Proof. Let $\mathbb{K}$ be a field with $|\mathbb{K}| > \binom{n+1}{d}$. Let Π be a partition of P and Γ a Π-partite compartmented access structure determined by a, b, and d. Let Γ_1 and Γ_2 be two Π-partite access structures with

$$\min \Gamma_1 = \{x \in \mathbf{P} : |x| \geq d - |a| \text{ and } x_i \leq b - a\}, \text{ and}$$
$$\min \Gamma_2 = \{a\}.$$

By Lemma 4.3.5, these access structures are ideal. Moreover, if $\mathcal{Z}_1$ and $\mathcal{Z}_2$ are the respective associated integer polymatroids, it is easy to see that $\min \Gamma_1 = \mathcal{B}(\mathcal{Z}_1, J_m)$ and $\min \Gamma_2 = \mathcal{B}(\mathcal{Z}_2, J_m)$. Since $\Gamma = \Gamma_1 + \Gamma_2$, by Lemma 4.3.2 Γ admits a $\mathbb{K}$-vector space secret sharing scheme. □

Corollary 4.3.7. *All compartmented access structures are ideal and admit a vector space secret sharing scheme over every large enough field.*

The relation between integer polymatroids and compartmented access structures derives from Theorem 4.3.6. If $\mathcal{Z} = (J'_m, h)$ is the integer polymatroid associated to the compartmented access structure Γ, then $\mathcal{Z}(J_m)$ has the strong exchange property. Taking into account the results obtained in Proposition 4.2.10, we obtain a new description of the compartmented access structures.

Corollary 4.3.8. *An m-partite access structure Γ is compartmented if and only if for every $x, y \in \min \Gamma$ it follows $|x| = |y|$ and $[x, y] \subseteq \min \Gamma$.*

4.3.3 Dual Compartmented Access Structures

For every access structure Γ, the minimal qualified subsets of the dual access structure Γ^* determined by the set of maximal non-authorized subsets $\mathcal{A}$,

$$\min \Gamma^* = \{P \smallsetminus A : A \in \max \mathcal{A}\}.$$

Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set of participants P. If Γ is a Π-partite compartmented access structure defined by $a, b \in \mathbb{Z}_+^m$ and $d \in \mathbb{Z}$, then the maximal non authorized points are those $x \in \mathbb{Z}^m$ satisfying one of the following conditions:

1. $x_i = a_i - 1$ for some $i \in J_m$ and $x_j = |P_j|$ for all $j \neq i$.
2. $x_i = |P_i|$ and $\sum_{j \neq i} x_j = d - b_i - 1$.
3. $a_i \leq x_i \leq b_i - 1$ for all $i \in J_m$ and $|x| = d - 1$.

The minimal points of Γ^* are of the kind $\mathbf{P} \smallsetminus y$, with y a maximal non-authorized point of Γ. Therefore, the minimal points of Γ^* are those $x \in \mathbb{Z}_+^m$ that satisfy one of the following conditions:

- $x_i = |P_i| - a_i + 1$ for some $i \in J_m$ and $x_j = 0$ for all $j \neq i$.

- $x_i = 0$ for some i and $\sum_{j \neq i} x_j = \sum |P_j| - d + b_i + 1$.
- $|P_i| - b_i + 1 \leq x_i \leq |P_i| - a_i$ and $|x| = |P| - d + 1$.

Proposition 4.3.9. *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set P with n participants. Let $a, b \in \mathbb{Z}_+^m$ and $d \in \mathbb{Z}_+$ with $a \leq b$ and $|a| \leq d \leq |b|$. The access structure*

$$\Gamma = \left\{ x \in \mathbf{P} \,:\, |x| \geq t \text{ or there is } i \in J_m \text{ with } x_i \geq a_i \text{ or } \sum_{j \neq i} x_j \geq b_i \right\}$$

is ideal and admits a vector space secret sharing scheme over every finite field $\mathbb{K}$ with $\mathbb{K} > \binom{n+1}{d}$.

4.3.4 Ports of Matroids with the Strong Exchange Property

Let $\mathcal{Z} = (J_m, h)$ be an integer polymatroid with the strong exchange property that is determined by $a, b \in \mathbb{Z}_+^m$ and $d \in \mathbb{Z}_+$. Let $\Pi = (Q_1, \ldots, Q_m)$ be a partition of a set Q of size $n+1$ with $|Q_1| > a_1$. Every Π-partite matroid $\mathcal{M}$ is $\mathbb{K}$-representable for every finite field $\mathbb{K}$ with $\mathbb{K} > \binom{n+1}{d}$.

For every $p \in Q_1$, consider the matroid port $\Gamma = \Gamma_p(\mathcal{M})$ and $P = Q \setminus \{p\}$. A point $x \in \mathbf{P}$ is in Γ if and only if there exists $u \in \bigcup_{A \in \Delta} \Gamma_A$ with $x \geq u$, where

1. $\Gamma_A = \{x \in \mathbf{P} \,:\, |x(A)| = h(A) \text{ and } x_i = 0 \text{ for } i \notin A \text{ and } a_i \leq x_i \leq b_i \text{ for } i \in A\}$, and
2. $\Delta = \{A \subseteq J_m \,:\, h(A) = h(A \cup \{1\})\}$.

Example 4.3.10. Let $\mathcal{M} = (Q, r)$ be a 4-partite multipartite matroid with the strong exchange property whose associated integer polymatroid $\mathcal{Z}_{abd}$ is defined by $a = (1,1,1,1)$, $b = (2,2,2,2)$ and $d = 5$. If we choose $p_0 \in P_1$ and $|P_1| > 2$, then the minimal points of $\Gamma = \Gamma_{p_0}(\mathcal{M})$ are $\min \Gamma = \{(2,0,0,0), (1,2,0,0), (1,0,2,0), (1,0,0,2)\}$.

4.3.5 Other Ideal Multipartite Secret Sharing Schemes

Simmons [96] considered a family of multipartite access structures that he also called compartmented, but does not belong to the family presented above. They are multipartite access structures in which the authorized subsets must have a certain number of participants in some of the parts.

Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set P and $t, k_1, \ldots, k_m$ integers with $1 \leq t \leq m$ and $1 \leq k_i \leq |P_i|$ for all $i = 1, \ldots, m$. The access structure determined by these parameters is

$$\Gamma = \bigcup_{S \subseteq J_m,\, |S| = t} \{x \in \mathbf{P} \,:\, x_i \geq k_i \text{ for all } i \in S\}.$$

Observe that it is in fact the composition of threshold access structures, and so it is ideal. Hence, it admits a $\mathbb{K}$-vector space secret sharing scheme for every $\mathbb{K}$ with $|\mathbb{K}| \geq \{m, n_1, \ldots, n_m\}$.

Consider now a modification of these structures. We additionally require the authorized subsets to be greater than a certain threshold d. That is,

$$\Gamma = \bigcup_{S \subseteq J_m,\, |S|=t} \{x \in \mathbf{P} \,:\, |x| \geq d \text{ and } x_i \geq k_i \text{ for all } i \in S\}. \tag{4.3}$$

The resulting access structure is, in general, non-ideal. However, if $k_i = 1$ for all $i = 1, \ldots, m$, then the access structure is ideal. This case was studied by Herranz and Sáez in [89]. Let d be an integer with $0 < d \leq |P|$. The access structure presented in [89] is the following

$$\Gamma = \bigcup_{S \subseteq J_m,\, |S|=t} \{x \in \mathbf{P} \,:\, |x| \geq d \text{ and } x_i > 0 \text{ for all } i \in S\}.$$

This access structure is associated to the t-truncation of the boolean polymatroid defined by $B = \{0, \ldots, m\}$, $B_0 = \{0\}$ and $B_i = \{i\} \cup \{m+1, \ldots, r\}$ for $i = 1, \ldots, m$, where $r = m + t - d$. Hence, this integer polymatroid is $|\mathbb{K}|$-representable for every $|\mathbb{K}| > m$. Therefore, Γ admits a $\mathbb{K}$-vector space secret sharing scheme for every $\mathbb{K}$ with $|\mathbb{K}| > \binom{n+1}{t}$.

Now observe that, in general, the access structures defined in (4.3) are not ideal. We argue this fact by using the connection between ideal multipartite access structures and integer polymatroids. For instance, consider an access structure Γ with $m = 3$, $t = 2$, $d = 7$, and $k_i = 3$ for $i = 1, 2, 3$. Suppose that it is ideal, and let $\mathcal{Z}$ the integer polymatroid associated to Γ. Since $(3, 3, 1)$ and $(3, 1, 3)$ are in $\min \Gamma$, then they are also in $\mathcal{B}(\mathcal{Z})$ by Theorem 3.3.2. Hence $(3, 2, 2) \in \mathcal{B}(\mathcal{Z})$ by the exchange property, but $(3, 2, 2)$ is not in Γ, a contradiction. Therefore, Γ is not a matroid port and so it is non-ideal.

Another access structure related to the one in (4.3) is the access structure by Ng in [80]. This access structure is defined by

$$\Gamma = \{x \in \mathbf{P} \,:\, x_1 \geq k_1\} \cup \left(\bigcup_{S \subseteq \{2,\ldots,m\},\, |S|=t} \Gamma_S \right), \qquad \text{where}$$
$$\Gamma_S = \{x \in \mathbf{P} \,:\, x_i \geq k_i \text{ for all } i \in S \text{ and } x_1 \geq k_1 - 1\}.$$

Observe that this access structure is a threshold access structure composed with a Simmons' compartmented access structure. Namely, $\Gamma = \Gamma_1[p, \Gamma_2]$, where Γ_1 is a access structure of threshold k_1 on the set $P_1 \cup \{p\}$, with $p \notin P$, and Γ_2 is a $(P_2, \ldots, P_m)$-partite Simmons' compartmented access structure with thresholds $k_2, \ldots, k_m$. Since the Simmons' compartmented access structure admits a vector space secret sharing scheme for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq \max\{m-1, n_2, \ldots, n_m\}$, by Lemma 2.5.1 this access structure admits a vector space secret sharing for every finite field $|\mathbb{K}| \geq \max\{m-1, n_1, \ldots, n_m\}$.

4.4 Bipartite and Tripartite Access Structures

In this section, we apply our general results on ideal multipartite access structures to completely characterize the ideal bipartite and tripartite access structures. The characterization of ideal bipartite access structures was done previously in [85], but only partial results were known about the tripartite case [6, 28, 89].

We begin by characterizing the bipartite and tripartite matroid ports. This is done in Section 4.4.1 by applying Theorem 3.3.2 to the particular cases $m = 2$ and $m = 3$. In Section 4.4.2, we use Theorem 3.4.1 to prove that all matroids corresponding to those access structures are representable. Therefore, all matroid ports in these families are ideal and, by Theorem 2.4.5, in every secret sharing scheme for a non-ideal bipartite or tripartite access structure, the length of one of the shares must be at least 3/2 times the length of the secret.

We observe that this approach cannot provide a characterization of ideal multipartite access structures with more than three parts. This is due to the fact that the Vamos matroid is quadripartite and it is not ss-representable. Therefore, there exist quadripartite matroid ports that are not ideal.

4.4.1 Characterizing Bipartite and Tripartite Matroid Ports

Let Γ be a bipartite matroid port, that is, a Π-partite matroid port for some partition $\Pi = (P_1, P_2)$ of the set P of participants. The rank function of the integer polymatroid $\mathcal{Z} = (J_2, h)$ whose existence is given by Theorem 3.3.2 is completely determined by the values $r_i = h(\{i\}) \leq |P_i|$ for $i \in J_2$ and $s = h(\{1, 2\})$. Moreover, from the definition of polymatroid and Proposition 3.3.3, the integer values $r_1, r_2, s \in \mathbb{Z}$ are the values of the rank function of an integer polymatroid that is compatible with $\Delta = \mathrm{supp}(\Gamma)$ if and only if the following conditions are satisfied for every $i \in J_2$.

1. $0 \leq r_i \leq s \leq r_1 + r_2$.
2. $r_i > 0$ if $\{i\} \in \Delta$, and $s > r_i$ if $\{i\} \notin \Delta$.
3. $r_1 + r_2 > s$ if $\{\{1\}, \{2\}\} \subseteq \Delta$.

In addition, the sets $\mathcal{B}(\mathcal{Z}, X)$ can be easily described by

- $\mathcal{B}(\mathcal{Z}, J_2) = \{v \in \mathbb{Z}_+^2 \,:\, (s - r_2, s - r_1) \leq v \leq (r_1, r_2) \text{ and } |v| = s\}$, and
- $\mathcal{B}(\mathcal{Z}, \{1\}) = \{(r_1, 0)\}$, and $\mathcal{B}(\mathcal{Z}, \{2\}) = \{(0, r_2)\}$.

Therefore, a bipartite access structure is a matroid port if and only if it there exist integers r_1, r_2, s in the above conditions such that $\min \Pi(\Gamma) = \min\{u \in \mathcal{B}(\mathcal{Z}, X) \,:\, X \in \Delta\}$.

We proceed in a similar way to characterize the tripartite matroid ports. Consider now a tripartition $\Pi = (P_1, P_2, P_3)$ of a set P and a Π-partite matroid port Γ on P. The values of a rank function of the corresponding integer polymatroid $\mathcal{Z} = (J_3, h)$ will be denoted by $r_i = h(\{i\}) \leq |P_i|$, where $i \in J_3$, and $s_i = h(\{j, k\})$ if $\{i, j, k\} = J_3$, and $s = h(J_3)$. The integer values r_i, s_i, and s, where $i \in J_3$, univocally determine a discrete polymatroid $\mathcal{Z}$ with ground set J_3 that is compatible with $\Delta = \mathrm{supp}(\Gamma)$ if and only if the following conditions are satisfied for every i, j, k with $\{i, j, k\} = J_3$.

1. $0 \leq r_i \leq s_j \leq s$.
2. $s_i \leq r_j + r_k$, and $s \leq s_i + r_i$, and $s + r_i \leq s_j + s_k$.
3. $r_i > 0$ if $\{i\} \in \Delta$, and $r_i < s_j$ if $\{i\} \notin \Delta$ and $\{i, k\} \in \Delta$, and $s_i < s$ if $\{j, k\} \notin \Delta$.
4. $s_i < r_j + r_k$ if $\{\{j\}, \{k\}\} \subseteq \Delta$.

5. $s + r_i < s_j + s_k$ if $\{i\} \notin \Delta$ and $\{\{i,j\},\{i,k\}\} \subseteq \Delta$.

6. $s < s_i + r_i$ if $\{\{i\},\{j,k\}\} \subseteq \Delta$.

In this case the sets $\mathcal{B}(\mathcal{Z}, X)$ can be described by

- $\mathcal{B}(\mathcal{Z}, J_3) = \{v \in \mathbb{Z}_+^m : (s-s_1, s-s_2, s-s_3) \leq v \leq (r_1, r_2, r_3) \text{ and } |v| = s\}$,
- $\mathcal{B}(\mathcal{Z}, \{1,2\}) = \{v \in \mathbb{Z}_+^m : (s_3 - r_2, s_3 - r_1, 0) \leq v \leq (r_1, r_2, 0) \text{ and } |v| = s_3\}$, and
- $\mathcal{B}(\mathcal{Z}, \{1\}) = \{(r_1, 0, 0)\}$,

and we obtain by symmetry the descriptions for the other sets $\mathcal{B}(\mathcal{Z}, X)$. In conclusion, a tripartite access structure Γ is a matroid port if and only if there exist integers r_i, s_i, and s, where $i \in J_3$, satisfying the previous conditions such that $\min \Pi(\Gamma) = \min\{u \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}$.

4.4.2 All Bipartite and Tripartite Matroid Ports Are Ideal

Hammer, Romashchenko, Shen, and Vereshchagin [52] proved that every integer polymatroid with ground set J_m with $m \leq 3$ is representable, and we have presented an alternate proof of this result in Section 4.2.4. Therefore every tripartite matroid is representable. However, it is not enough to prove that every tripartite matroid port is ideal because tripartite access structures are related to quadripartite matroids. We need a more general result, which is presented in Proposition 4.4.1.

Let $\mathcal{Z}$ be an integer polymatroid with ground set J_3 that is represented over the field $\mathbb{K}$ by three subspaces V_1, V_2, V_3 of a vector space E. If r_i, s_i and s are the integer values of the rank function of $\mathcal{Z}$, then $r_i = \dim V_i$ for every $i \in J_3$, and $s_i = \dim(V_j + V_k)$ if $\{i,j,k\} = J_3$, and $s = \dim(V_1 + V_2 + V_3)$. If $\{i,j,k\} = J_3$, consider $t_i = r_j + r_k - s_i = \dim(V_j \cap V_k)$. Observe that $t = \dim(V_1 \cap V_2 \cap V_3)$ is not determined in general by $\mathcal{Z}$. That is, there can exist different representations of $\mathcal{Z}$ with different values of t. Nevertheless, there exist some restrictions on this value. Of course, $t \leq t_i$ for every $i \in J_3$. In addition, since $(V_1 \cap V_3) + (V_2 \cap V_3) \subseteq (V_1 + V_2) \cap V_3$, we have that $\dim((V_1 + V_2) \cap V_3) - \dim((V_1 \cap V_3) + (V_2 \cap V_3)) = \sum s_i - \sum r_i - (s-t) \geq 0$. Therefore, $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$.

Proposition 4.4.1. *Let $\mathcal{Z}$ be an integer polymatroid with ground set J_3. Consider an integer t with $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$ and $\ell = \sum s_i - \sum r_i - (s-t)$. Let $\mathbb{K}$ be a field with $|\mathbb{K}| \geq s_3 + \ell$. Then there exists a $\mathbb{K}$-representation of $\mathcal{Z}$ given by subspaces $V_1, V_2, V_3 \subseteq E = \mathbb{K}^s$ with $\dim(V_1 \cap V_2 \cap V_3) = t$.*

Proof. Consider two subspaces $V, W \subseteq E$ such that $\dim V = s_3$ and $E = V \oplus W$. Given a basis $\{v_1, \ldots, v_{s_3}\}$ of V, consider the mapping $\mathbf{v}\colon \mathbb{K} \to V$ defined by $\mathbf{v}(x) = \sum_{i=1}^{s_3} x^{i-1} v_i$. Observe that the vectors $\mathbf{v}(x)$ have Vandermonde coordinates with respect to the given basis of V. This implies that every set of at most s_3 vectors of the form $\mathbf{v}(x)$ is independent.

Consider three disjoint sets $T_3, R_1, R_2 \subseteq \{\mathbf{v}(x) : x \in \mathbb{K}\} \subseteq V$ with $|T_3| = t_3$, $|R_1| = r_1 - t_3$, and $|R_2| = r_2 - t_3$. The subspaces $V_1 \subseteq V$ and $V_2 \subseteq V$, spanned, respectively, by $T_3 \cup R_1$ and $T_3 \cup R_2$, are such that $V_1 + V_2 = V$ and have dimensions $\dim V_1 = r_1$ and $\dim V_2 = r_2$.

At this point, we have to find a suitable subspace $V_3 \subseteq E$ to complete the representation of $\mathcal{Z}$. Consider sets $T \subseteq T_3$ with $|T| = t$, and $A_1 \subseteq R_1$ and $A_2 \subseteq R_2$ with $|A_1| = t_2 - t$ and $|A_2| = t_1 - t$, and $B \subseteq \{\mathbf{v}(x) : x \in \mathbb{K}\}$ with $|B| = \ell$ and $B \cap (T_3 \cup R_1 \cup R_2) = \emptyset$. Finally, take $V_3 = U \oplus W$, where $U \subseteq V$ is the subspace spanned by $T \cup A_1 \cup A_2 \cup B$.

Since $|T \cup A_1 \cup A_2 \cup B| = s_3 + r_3 - s \leq s_3$, this is an independent set of vectors and, hence, it is a basis of U. Therefore, $\dim V_3 = r_3$. We assert that $\dim(V_3 \cap V_1) = t_2$. Effectively, it is clear that $\dim(V_3 \cap V_1) = \dim(U \cap V_1)$. The sets $T_3 \cup R_1$ and $T \cup A_1 \cup A_2 \cup B$ are bases of V_1 and U, respectively. The intersection of these two sets is $T \cup A_1$, which has cardinality t_2, and their union is $T_3 \cup R_1 \cup A_2 \cup B$, which is an independent set because its cardinality is $s_3 - (s - s_2) \leq s_3$. This proves our assertion. Analogously, $\dim(V_3 \cap V_1) = t_1$. Therefore, $\dim(V_1 + V_3) = s_2$ and $\dim(V_2 + V_3) = s_1$. A similar argument as before proves that $\dim(V_1 \cap V_2 \cap V_3) = t$. □

Observe that Corollary 4.2.14 and Corollary 4.2.15 are also a consequence of Proposition 4.4.1.

Corollary 4.4.2. *Every bipartite matroid port is ideal. More specifically, every bipartite matroid port is a vector space access structure over every large enough field.*

Proof. If $\Gamma_{p_0}(\mathcal{M})$ is a bipartite matroid port, then the matroid $\mathcal{M}$ is tripartite and, from Corollary 4.2.15, it is representable over every large enough field. □

The next lemma is a well known result of linear algebra. It will be used in the proof of Theorem 4.4.4.

Lemma 4.4.3. *Let $\mathbb{K}$ be a field with $|\mathbb{K}| > n$ and let V and $W_1, \ldots, W_n$ be subspaces of a $\mathbb{K}$-vector space E such that $V \not\subseteq W_i$ for every $i = 1, \ldots, n$. Then $V \not\subseteq \bigcup_{i=1}^{n} W_i$.*

Theorem 4.4.4. *Every tripartite matroid port is ideal. More specifically, every tripartite matroid port is a vector space access structure over every large enough field.*

Proof. Let $\Gamma = \Gamma_{p_0}(\mathcal{M})$ be a tripartite matroid port. By Theorem 3.4.1, we only have to prove that the integer polymatroid $\mathcal{Z}' = (J_3', h)$ associated to $\mathcal{M}$ is representable over every large enough field. Consider $\Delta = \mathrm{supp}(\Gamma)$ and the values r_i, s_i, s, where $i = 1, 2, 3$, of the rank function of the integer polymatroid $\mathcal{Z} = \mathcal{Z}'(J_3) = (J_3, h)$. Take $t_i = r_j + r_k - s_i$ for $\{i, j, k\} = J_3$. From Proposition 4.4.1, for every integer t such that $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$ and for every large enough field $\mathbb{K}$, there exists a $\mathbb{K}$-representation of $\mathcal{Z}$ formed by subspaces $V_1, V_2, V_3 \subseteq E = \mathbb{K}^s$ with $\dim(V_1 \cap V_2 \cap V_3) = t$. The proof is concluded by finding a vector $x_0 \in E$ such that the subspace $V_0 = \langle x_0 \rangle$ together with the subspaces V_1, V_2, V_3 form a $\mathbb{K}$-representation of $\mathcal{Z}'$. We distinguish several cases, depending on the access structure Δ. Remember that the values r_i, s_i, s must satisfy the conditions in Section 4.4.1.

1. $\min \Delta = \{\{1\}\}$. In this case, we have to choose a vector $x_0 \in V_1$ such that $x_0 \notin V_2 + V_3$. Such a vector exists because $\{2, 3\} \notin \Delta$ and hence $s_1 < s$.

2. $\min \Delta = \{\{1\}, \{2\}\}$. Then $s_3 < r_1 + r_2$ and $s + r_3 < s_1 + s_2$. In particular, $t_3 = r_1 + r_2 - s_3 > \max\{0, s - \sum s_i + \sum r_i\}$. Therefore, we can take $t < t_3$, and hence there exists a representation of $\mathcal{Z}$ such that $V_1 \cap V_2 \not\subseteq V_3$. Now, we only have to take a vector $x_0 \in V_1 \cap V_2$ such that $x_0 \notin V_3$.

3. $\min\Delta = \{\{1\},\{2\},\{3\}\}$. In this situation, $s_i < r_j + r_k$ whenever $\{i,j,k\} = J_3$. Therefore, $\min\{t_1,t_2,t_3\} > 0$ and there exists a representation of $\mathcal{Z}$ with $V_1 \cap V_2 \cap V_3 \neq \{0\}$.

4. $\min\Delta = \{\{1\},\{2,3\}\}$. Then $s < r_1 + s_1$. In addition, $s + r_2 < s_1 + s_3$ and $s + r_3 < s_1 + s_2$. Observe that $\dim(V_1 \cap (V_2 + V_3)) = r_1 + s_1 - s > 0$. Moreover, we assert that $V_1 \cap (V_2 + V_3) \not\subseteq V_i$ if $i \neq 1$. Suppose that, for instance, $V_1 \cap (V_2 + V_3) \subseteq V_2$. This implies that $V_1 \cap (V_2 + V_3) = V_1 \cap V_2$ and, by considering the dimensions of these subspaces, $r_1 + s_1 - s = r_1 + r_2 - s_3$. Since $s + r_2 < s_1 + s_3$, we have obtained a contradiction that proves our assertion. Finally, we take a vector $x_0 \in V_1 \cap (V_2 + V_3)$ such that $x_0 \notin V_2$ and $x_0 \notin V_3$.

5. $\min\Delta = \{\{1,2\}\}$. For $i \in \{1,2\}$, we have $s_i < s$ and, hence, $V_1 + V_2 \not\subseteq V_i + V_3$. Then there exists a vector $x_0 \in V_1 + V_2$ such that $x_0 \notin V_2 + V_3$ and $x_0 \notin V_1 + V_3$.

6. $\min\Delta = \{\{1,2\},\{2,3\}\}$. Consider $V = (V_1 + V_2) \cap (V_2 + V_3)$. Observe that $\dim V = s_3 + s_1 - s > r_2 = \dim V_2$. Therefore, $V \not\subseteq V_2$. In addition, since $V' = V_2 + (V_1 \cap V_3) \subseteq V$,
$$E = (V_1 + V_3) + V' \subseteq (V_1 + V_3) + V \subseteq E, \tag{4.4}$$
and $V_1 + V_3 \neq E$ because $s_2 < s$. Therefore, there exists a vector $x_0 \in V$ such that $x_0 \notin V_1 + V_3$ and $x_0 \notin V_2$.

7. $\min\Delta = \{\{1,2\},\{2,3\},\{3,1\}\}$. Consider $W = (V_1 + V_2) \cap (V_2 + V_3) \cap (V_3 + V_1)$. Because of Equation (4.4), $\dim W = \sum s_i - 2s$. Clearly, if $\{i,j,k\} = J_3$, then $W \cap V_i = V_i \cap (V_j + V_k)$ and, hence, $\dim(W \cap V_i) = r_i + s_i - s$. Since $\dim W - \dim(W \cap V_i) = s_j + s_k - s - r_i > 0$, we have proved that $W \not\subseteq V_i$ for every $i \in J_3$. Therefore, there exists a vector $x_0 \in W$ such that $x_0 \notin V_i$ for every $i \in J_3$.

8. $\min\Delta = \{\{1,2,3\}\}$. In this case $s_i < s$ for every $i \in J_3$ and there exists a vector $x_0 \in E$ such that $x_0 \notin V_j + V_k$ for every $\{j,k\} \subseteq J_3$.

Clearly, the cases that are not considered here are solved by symmetry. □

Chapter 5

Ideal Hierarchichal Secret Sharing Schemes

This chapter is dedicated to the hierarchical secret sharing schemes, that are the ones in which there is a hierarchy among the set of participants. As in the previous chapter, we apply the new results on ideal multipartite access structures presented in Chapter 3 to characterize the ideal access structures in certain families. We characterize the ideal hierarchical access structures and the ideal weighted threshold access structures. These results are obtained by means of some new specific combinatorial techniques that are presented herein.

The first contribution on non-threshold access structures was done by Shamir [94] by considering a kind of hierarchical access structures. He proposed a construction based on the threshold scheme. Namely, every participant receives as its share a certain number of shares from a threshold scheme, according to its position in the hierarchy. In this way a scheme for a *weighted threshold access structure* is obtained. That is, every participant has a weight (a positive integer) and a set is qualified if and only if its weight sum is at least a given threshold. This new hierarchical scheme is not ideal because the shares are in general larger than the secret. Simmons [96] proposed two families of access structures, the *multilevel* and the compartmented (studied in the last chapter), and conjectured them to admit ideal secret sharing schemes. In this way, he initiated a new line of work in secret sharing, the constructing ideal secret sharing schemes for families of access structures with interesting properties.

The multilevel access structures are multipartite, and in these structures the participants are hierarchically ordered, being the participants in higher levels more powerful than the ones in lower levels. Multipartite and, in particular, hierarchical secret sharing are the most natural generalization of threshold secret sharing. Brickell [19] constructed ideal linear schemes for multilevel and compartmented access structures, proving the conjecture by Simmons. By using different kinds of polynomial interpolation, Tassa [101], and Tassa and Dyn [102] proposed constructions of ideal secret sharing schemes for several families of multipartite access structures, some of them with hierarchical properties.

Among hierarchical access structures, the family of weighted threshold access structures is, among hierarchical access structures, one of the most studied. Beimel, Tassa and Weinreb [6] presented a characterization of the ideal weighted threshold access structures that

generalizes the partial results in [77,85]. Another important result about weighted threshold access structures have been obtained recently by Beimel and Weinreb [8]. They prove that all such access structures admit secret sharing schemes in which the size of the shares is quasi-polynomial in the number of users.

This chapter deals with the two lines of work in secret sharing that have been discussed previously: first, the construction of ideal secret sharing schemes for useful classes of access structures, in particular the ones with hierarchical properties, and second, the characterization of ideal access structures. In this chapter we solve a question that is important for these two lines of research. Namely, what hierarchical access structures admit an ideal secret sharing scheme?

First of all, we formalize the concept of *hierarchical access structure* by introducing in Section 5.1 a natural definition for it. Basically, if a participant in a qualified subset is substituted by a *hierarchically superior* participant, the new subset must be still qualified. An access structure is *hierarchical* if, for any two given participants, one of them is hierarchically superior to the other. According to this definition, the family of the hierarchical access structures contains the multilevel access structures [19, 96], the hierarchical threshold access structures studied by Tassa [101] and by Tassa and Dyn [102], and also the weighted threshold access structures that were first considered by Shamir [94] and studied in [6, 8, 77, 85]. Morevoer, similarly to multipartite and weighted threshold access structures, the family of the hierarchical access structures is closed by duality and minors. This is proved in Section 5.2.1.

The main result in this chapter is Theorem 5.5.2, which provides a complete characterization of the ideal hierarchical access structures. In particular, we prove that all hierarchical matroid ports are ports of representable matroids.

Theorem 5.0.5. *Let Γ be a hierarchical access structure. The following properties are equivalent:*

1. *Γ admits a vector space secret sharing scheme over every large enough finite field.*
2. *Γ is ideal.*
3. *Γ admits a secret sharing scheme in which the length of every share is less than $3/2$ times the length of the secret value.*
4. *Γ is a matroid port.*

This generalizes the analogous statement that holds for weighted threshold access structures as a consequence of the results in [6,68]. Actually, as an application of our results, we present in Section 5.6 a new proof of the characterization of the ideal weighted threshold access structures that simplifies the proof given by Beimel, Tassa and Weinreb [6].

Our starting point is the observation that every hierarchical access structures is determined by its *hierarchically minimal sets*, which are the minimal qualified sets such that the participants are in the lowest possible levels in the hierarchy. The integer polymatroids related to ideal hierarchical access structures are also boolean, as the access structures studied in the last chapter.

An important technique to describe the hierarchical access structures is to use the stabilizers. The *stabilizer* of an access structure is a set of vectors that preserve the access

structure. That is, the points of the access structures plus the vectors of the stabilizer are in the access structure. By using the stabilizers, we define the *hierarchically minimal points*, which represent the hierarchically minimal sets and provides a compact description of the access structure.

Our characterization of the ideal hierarchical access structures is given in terms of some properties of the hierarchically minimal points that can be efficiently checked. By using our results, given a hierarchical access structure that is described by its hierarchically minimal points, one can efficiently determine whether it is ideal or not. If the access structure is described by its minimal qualified subsets, it is easy to determine the hierarchically minimal points. If the access structure is described in another way, one has to find the hierarchically minimal points, but this can be done efficiently most of the times. This is the case, for instance, of weighted threshold access structures that are determined by the weights and the threshold. Moreover, by using the general results on ideal multipartite secret sharing schemes presented in the previous chapters, a method to construct an ideal linear secret sharing scheme for every given ideal hierarchical access structure can be obtained.

5.1 Hierarchical Access Structures

We present here a natural definition for the family of the *hierarchical access structures*, which embraces all possible situations in which there is a hierarchy on the set of participants. For instance, the weighted threshold access structures and the hierarchical threshold access structures [101] are contained in this new family. Hierarchical access structures are in particular multipartite. Therefore, we can take advantage of the results and techniques in Chapter 3 about the characterization of ideal multipartite access structures.

Let Γ be an access structure on a set of participants P. We say that the participant $p \in P$ is *hierarchically superior* to the participant $q \in P$, and we write $q \preceq p$, if $A \cup \{p\} \in \Gamma$ for every subset $A \subseteq P \setminus \{p, q\}$ with $A \cup \{q\} \in \Gamma$. An access structure is said to be *hierarchical* if all participants are hierarchically related, that is, for every pair of participants $p, q \in P$, either $q \preceq p$ or $p \preceq q$. If $p \preceq q$ and $q \preceq p$, we say that these two participants are *hierarchically equivalent*, and we write $p \sim q$. Clearly, this is an equivalence relation. If $\Pi = (P_1, \ldots, P_m)$ is the corresponding partition of P into equivalence classes, the hierarchical relation $\preceq$ is an order on Π. Observe that an access structure is hierarchical if and only if this is a total order.

Let $\Pi = (P_1, \ldots, P_m)$ be a partition of P. An access structure Γ is said to be Π-*partite* if every pair of participants in the same part P_i are hierarchically equivalent. A different but equivalent definition for this concept is given in Section 3.2.1. A Π-partite access structure is said to be Π-*hierarchical* if $q \preceq p$ for every pair of participants $p \in P_i$ and $q \in P_j$ with $i < j$. That is, the participants in the first level are hierarchically superior to those in the second level and so on. Obviously, an access structure is hierarchical if and only if it is Π-hierarchical for some partition Π of the set of participants.

5.2 A Geometric Representation of Hierarchical Access Structures

In this section we recall the geometric representation for multipartite access structures that was introduced in Chapter 3 and we adapt it to hierarchical access structures by introducing the new concept of *stabilizers* of multipartite access structures. The concept of stabilizer generalizes properties of multipartite access structures as monotonicity, hierarchy, and the weighted threshold description.

Let $\Pi = (P_1, \ldots, P_m)$ be a partition of P. A set $V \subseteq \mathbb{Z}^m$ is called a *stabilizer* if V is closed by sums, and $\mathbb{Z}_+^m \subseteq V$, and $V \cap (\mathbb{Z}_-^*)^m = \{0\}$. For a stabilizer $V \subseteq \mathbb{Z}^m$, we define the binary relation $\leq_V$ in $\mathbb{Z}^m$ by $u \leq_V v$ if and only if $v - u \in V$. Since $0 \in V$ and V is closed by sums, this binary relation is reflexive and transitive. It is an order if and only if $V \cap (-V) = \{0\}$.

For a stabilizer $V \subseteq \mathbb{Z}^m$ and an Π-partite access structure $\Gamma \subseteq \mathbf{P} \subset \mathbb{Z}_+^m$, we say that Γ is *V-stable* if $(\Gamma + V) \cap \mathbf{P} = \Gamma$. If $\leq_V$ is an order, that is, if $V \cap (-V) = \{0\}$, we can consider the minimal points in Γ according to the order $\leq_V$, which are called the *V-minimal points of* Γ. Clearly, if $V \cap (-V) = \{0\}$, a V-stable multipartite access structure is completely determined by its V-minimal points.

Obviously, every m-partite access structure is $\mathbb{Z}_+^m$-stable. For $i = 1, \ldots, m$, we notate $\mathbf{e}^i$ for the i-th vector of the canonical basis of $\mathbb{R}^m$, and, for $i = 1, \ldots, m-1$, we take $\mathbf{v}^i = \mathbf{e}^i - \mathbf{e}^{i+1}$. Consider

$$H_0 = \left\{ \sum_{i=1}^{m-1} \lambda_i \mathbf{v}^i \,:\, \lambda_i \in \mathbb{Z}_+ \text{ for every } i = 1, \ldots, m-1 \right\} \subset \mathbb{Z}^m$$

and $H = H_0 + \mathbb{Z}_+^m$. Clearly, H is a stabilizer and $H \cap (-H) = \{0\}$. In addition, a Π-partite access structure is Π-hierarchical if and only if it is H-stable. Consequently, every hierarchical access structure is determined by its family of H-minimal points, that we call $\min_H \Gamma$.

The next lemma shows a characterization of the vectors in H. This result and the one in Lemma 5.2.2 will be very useful in our study of hierarchical access structures and will be used in the following sections.

Lemma 5.2.1. *A vector $v \in \mathbb{Z}^m$ is in H if and only if $\sum_{j=1}^{i} v_j \geq 0$ for all $i = 1, \ldots, m$.*

Proof. For every $i = 1, \ldots, m$, consider the vector $\mathbf{w}^i = \sum_{j=1}^{i} \mathbf{e}^j$. Observe that $\mathbf{w}^i \cdot v = \sum_{j=1}^{i} v_j$ for every $v \in \mathbb{Z}^m$ and $i = 1, \ldots, m$. Therefore, $\mathbf{w}^i \cdot \mathbf{v}^i = 1$ while $\mathbf{w}^i \cdot \mathbf{v}^j = 0$ if $i \neq j$. If $v \in H$, there exist integers $\lambda_i \geq 0$ and a vector $u \in \mathbb{Z}_+^m$ such that $v = \sum_{j=1}^{m-1} \lambda_j \mathbf{v}^j + u$. Then $\mathbf{w}^i \cdot v = \lambda_i + \mathbf{w}^i \cdot u \geq 0$ if $1 \leq i \leq m-1$ and $\mathbf{w}^m \cdot v = \mathbf{w}^m \cdot u \geq 0$. The converse is proved by taking into account that $\{\mathbf{v}^1, \ldots, \mathbf{v}^{m-1}, \mathbf{e}^m\}$ is a basis of $\mathbb{R}^m$ and

$$v = \sum_{i=1}^{m-1} (\mathbf{w}^i \cdot v)\mathbf{v}^i + (\mathbf{w}^m \cdot v)\mathbf{e}^m$$

for every $v \in \mathbb{Z}^m$. □

Lemma 5.2.2. *If $x, y \in \mathbb{Z}_+^m$ are such that $y - x \in H$, then there exist $v \in H_0$ and $u \in \mathbb{Z}_+^m$ such that*

$$y = x + v + u \text{ and } x + v \geq 0.$$

In particular, if Γ is a Π-hierarchical access structure and $y \in \min \Gamma$, then there exists $x \in \min_H \Gamma$ such that $y - x \in H_0$.

Proof. The proof is by induction on m. The result is trivial for $m = 1$. Assume that $m > 1$. For a vector $x \in \mathbb{Z}^m$, we notate $x = (\widetilde{x}, x_m)$ with $\widetilde{x} \in \mathbb{Z}^{m-1}$. If $x, y \in \mathbb{Z}_+^m$ are such that $y - x \in H$, then it is clear from Lemma 5.2.1 that $\widetilde{y} - \widetilde{x} \in H$. By the induction hypothesis, $\widetilde{y} = \widetilde{x} + \widetilde{v} + \widetilde{u}$, where $\widetilde{v} \in H_0$, and $\widetilde{u} \in \mathbb{Z}_+^{m-1}$, and $\widetilde{x} + \widetilde{v} \geq 0$. If $x_m \leq y_m$, then

$$y = (\widetilde{y}, y_m) = (\widetilde{x}, x_m) + (\widetilde{v}, 0) + (\widetilde{u}, y_m - x_m).$$

So, we can take $v = (\widetilde{v}, 0)$ and $u = (\widetilde{u}, y_m - x_m)$. If $x_m > y_m$, then there exists $w = (\widetilde{w}, y_m - x_m) \in H_0$ such that $\widetilde{w} \geq 0$, and $x' = x + w \geq 0$, and $y - x' \in H$. Since $x'_m = y_m$, we have that $y = x' + v' + u'$ with $v' \in H_0$, and $u' \in \mathbb{Z}_+^m$, and $x' + v' \geq 0$. In this case we can take $v = v' + w$ and $u = u'$.

If Γ is a Π-hierarchical access structure and $y \in \min \Gamma$, there exists an H-minimal point $x \in \min_H \Gamma$ such that $x \leq_H y$. Then $y = x + v + u$, where $v \in H_0$, and $u \in \mathbb{Z}_+^m$, and $x + v \in \mathbf{P}$. Since $x + v \in \Gamma$ and y is a minimal point of Γ, we have that $u = 0$. □

Stabilizers are also convenient for the study of weighted theshold access structures. For a vector $w \in \mathbb{R}_+^m \setminus \{0\}$, consider the stabilizer $W(w) = \{u \in \mathbb{Z}^m : w \cdot u \geq 0\}$. Then Γ is a weighted threshold access structure if and only if Γ is $W(w)$-stable for some vector $w \in \mathbb{R}_+^m \setminus \{0\}$. Since $\leq_{W(w)}$ is not an order, we cannot consider here the $W(w)$-minimal points. Instead, we can consider the points in Γ with minimum weight, that is, those $u \in \Gamma$ that minimize $w \cdot u$.

Example 5.2.3. Brickell [19] showed how to construct ideal secret sharing schemes for the multilevel structures proposed by Simmons [96]. These structures are of the form

$$\Gamma = \{A \subseteq P : |A \cap (\cup_{j=1}^{i} P_j)| \geq t_i \text{ for every } i = 1, \ldots, m\}$$

for some monotone increasing sequence of integers $0 < t_1 < \ldots < t_m$. Clearly, if the number of participants in every level is large enough, Γ is a Π-hierarchical access structure with only one H-minimal point: $(t_1, t_2 - t_1, \ldots, t_m - t_{m-1})$.

Example 5.2.4. Another hierarchical threshold access structure was proposed by Tassa [101]. Given integers $0 < t_1 < \ldots < t_m$, the access structure is defined as

$$\Gamma = \{A \subseteq P : |A \cap (\cup_{j=1}^{i} P_j)| \geq t_i \text{ for some } i = 1, \ldots, m\}.$$

In this case, if the number of participants in each level is large enough, the access structure Γ is Π-hierarchical and its family of H-minimal points is $\min_H \Gamma = \{t_1 \mathbf{e}^1, \ldots, t_m \mathbf{e}^m\}$.

5.2.1 Minors and Composition

Recall that the dual of an access structure Γ on a set P is the access structure on the same set defined by $\Gamma^* = \{A \subset P : P \smallsetminus A \notin \Gamma\}$. It is not difficult to prove that Γ is Π-partite if and only if Γ^* is so. For a subset $B \subset P$, $\Gamma\backslash B$ and Γ/B on the set $P \smallsetminus B$ by $\Gamma\backslash B = \{A \subset P \smallsetminus B : A \in \Gamma\}$ and $\Gamma/B = \{A \subset P \smallsetminus B : A \cup B \in \Gamma\}$. If $\Pi = (P_1, \ldots, P_m)$ is a partition of P and Γ is a Π-partite access structure, then the minors $\Gamma\backslash B$ and Γ/B are $(\Pi\backslash B)$-partite access structures, where $\Pi\backslash B = (P_1 \smallsetminus B, \ldots, P_m \smallsetminus B)$, a partition of $P \smallsetminus B$. If $\Pi(B) = b$, then the geometric representations of these access structures are $\Gamma\backslash B = \{x \leq \mathbf{p} - b : x \in \Gamma\}$ and $\Gamma/B = \{x \leq \mathbf{p} - b : x + b \in \Gamma\}$.

Proposition 5.2.5. *Let $V \subset \mathbb{Z}^m$ be a stabilizer. Then the dual of a V-stable m-partite access structure is V-stable and all its minors are V-stable as well. In particular, this holds for hierarchical and weighted threshold access structures.*

Proof. Let Γ be a V-stable access structure. Consider a point $u \in \mathbf{P}$ with $u \in \Gamma^*$ and a vector $v \in V$ such that $u + v \in \mathbf{P}$. Then $\mathbf{p} - u \notin \Gamma$, and hence $\mathbf{p} - u - v = \mathbf{p} - (u + v) \notin \Gamma$ because Γ is V-stable. This implies that $u + v \in \Gamma^*$.

Consider now the minors $\Gamma\backslash B$ and Γ/B for some $B \subset P$, and take $b = \Pi(B)$. Consider vectors $0 \leq u \leq \mathbf{p} - b$ and $v \in V$ such that $0 \leq u + v \leq \mathbf{p} - b$. If $u \in \Gamma\backslash B$, then $u \in \Gamma$. This implies that $u + v \in \Gamma$ and hence $u + v \in \Gamma\backslash B$. If $u \in \Gamma/B$, then $u + b \in \Gamma$ and hence $u + v + b \in \Gamma$. Therefore, $u + v \in \Gamma/B$. □

Let Γ' be an access structure on $P = P_1 \cup \ldots \cup P_r$, and Γ'' an access structure $P' = P_{r+1}, \ldots, P_{r+s}$ with $P \cap P' = \emptyset$. Suppose that Γ' is $(P_1, \ldots, P_r)$-partite and Γ'' is $(P_{r+1}, \ldots, P_{r+s})$-partite, and take $p \in P_r$. Then the composition $\Gamma = \Gamma'[\Gamma''; p]$ is $(P'_1, \ldots, P'_{r+s})$-partite, where $P'_r = P_r \smallsetminus \{p\}$ and $P'_i = P_i$ for $i \neq r$.

In general, the composition of access structures does not have such good properties with respect stabilizers. However, some particular compositions of hierarchical access structures does. Namely, if Γ' and Γ'' are hierarchical and $p \in P_r$ then $\Gamma'[\Gamma''; p]$ is also hierarchical. Observe that the composition is made over a participant in the lowest level of Γ', and if it made over a participant from another part the resulting scheme is not always hierarchical. If $P_r = \{p\}$, then P'_r is empty and so Γ is $(r + s - 1)$-partite.

5.3 Hierarchical Matroid Ports

In this section we use the connection between integer polymatroids and multipartite matroid ports that is discussed in Chapter 3 to find necessary conditions for hierarchical access structures to be matroid ports. First we prove some technical lemmas that apply to every integer polymatroid. Specific results on integer polymatroids associated to hierarchical matroid ports are given afterwards.

Lemma 5.3.1. *Consider an integer polymatroid $\mathcal{Z} = (J_m, h)$, a subset $A \subseteq J_m$, and a point $y \in \mathbb{Z}_+^m$ that is H-minimal in $\mathcal{B}(\mathcal{Z}, A)$. Then y is the H-minimum point of $\mathcal{B}(\mathcal{Z}, A)$, that is, $y \leq_H x$ for every $x \in \mathcal{B}(\mathcal{Z}, A)$.*

Proof. We prove that $\mathcal{B}(\mathcal{Z}, A) \subset y + H$. Suppose that, on the contrary, $R = \mathcal{B}(\mathcal{Z}, A) \setminus (y + H) \neq \emptyset$ and consider a point $x \in R$ that is H-minimal in R. Let $i \in A$ be the smallest index with $x_i \neq y_i$. If $x_i < y_i$, there exists $j \in A$ with $j > i$ such that $x_j > y_j$ and $z = y + \mathbf{e}^j - \mathbf{e}^i \in \mathcal{B}(\mathcal{Z}, A)$. Observe that $y - z \in H_0 \setminus \{0\}$, a contradiction with the fact that y is H-minimal in $\mathcal{B}(\mathcal{Z}, A)$. If $x_i > y_i$, there exists $j \in A$ with $j > i$ such that $x_j < y_j$ and $u = x + \mathbf{e}^j - \mathbf{e}^i \in \mathcal{B}(\mathcal{Z}, A)$. Then $u \notin R$ because x is H-minimal in R, and hence $u \in y + H_0$. This implies that $x - y = (x - u) + (u - y) \in H_0$, a contradiction. □

For every $i, j \in \mathbb{Z}$ we notate $[i, j] = \{i, i+1, \ldots, j\}$ if $i < j$, while $[i, i] = \{i\}$ and $[i, j] = \emptyset$ if $i > j$. Let $\mathcal{Z} = (J_m, h)$ be a integer polymatroid. For every $i \in J_m$, consider the point $y^i = y^i(\mathcal{Z}) \in \mathbb{Z}_+^m$ defined by

$$y^i_j = h([j, i]) - h([j + 1, i]).$$

Observe that these points are vertices of the polytope defined by $\mathcal{Z}$ (see Section 2.3) and that $\sum_{j=k}^{i} y^i_j = h([k, i])$ for every $k \in [1, i]$. Hence, y^i is in $\mathcal{B}(\mathcal{Z}, [1, i])$ for every $i = 1, \ldots, m$.

Lemma 5.3.2. *For every $i = 1, \ldots, m$, the point $y^i(\mathcal{Z})$ is the H-minimum of $\mathcal{B}(\mathcal{Z}, [1, i])$.*

Proof. Taking into account Lemma 5.3.1 and the fact that $y^i(\mathcal{Z})$ is an H-minimal point of $\mathcal{B}(\mathcal{Z}, [1, i])$ for all $i = 1, \ldots, m$, it is enough to prove that y^i is H-minimal in $\mathcal{B}(\mathcal{Z}, [1, i])$. If not, there exists $v \in H_0 \setminus \{0\}$ such that $u = y^i - v \in \mathcal{B}(\mathcal{Z}, [1, i])$. Observe that $v_j = 0$ or all $j > i$. By Lemma 5.2.1, there exists $s \in [1, i]$ for which $\sum_{j=1}^{s-1} v_j > 0$, and hence $\sum_{j=s}^{i} v_j < 0$. Then

$$|u([s, i])| = \sum_{j=s}^{i} u_j > \sum_{j=s}^{i} y^i_j = h([s, i]),$$

a contradiction with the assumption that $u \in \mathcal{B}(\mathcal{Z}, [1, i])$. □

Lemma 5.3.3. *If $1 \leq j \leq i < m$, then $y^i_j \geq y^{i+1}_j$.*

Proof. Since h is submodular,

$$y^{i+1}_j = h([j, i + 1]) - h([j + 1, i + 1]) \leq h([j, i]) - h([j + 1, i]) = y^i_j.$$

□

For the remaining of this section, we assume that Γ is a Π-hierarchical matroid port, where $\Pi = (P_1, \ldots, P_m)$ is an m-partition of the set of participants P. Recall that we notate $\mathbf{p} = \Pi(P)$ and $\mathbf{P} = \Pi(\mathcal{P}(P)) \subset \mathbb{Z}_+^m$. In addition, we assume that the access structure Γ is *connected*, that is, that every participant is in a minimal qualified subset or, equivalently, for every $i \in J_m$, there is a minimal point $x \in \min \Gamma$ such that $x_i > 0$. Consider the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $\Gamma = \Gamma_0(\mathcal{Z}')$, and the integer polymatroid $\mathcal{Z} = \mathcal{Z}'(J_m) = (J_m, h)$. Since Γ is connected, $h(\{i\}) > 0$ for all $i \in J_m$, and hence $y^i_i > 0$. Recall that for every $x \in \mathbb{Z}_+^m$, we notate $\operatorname{supp}(x) = \{i \in J_m : x_i \neq 0\} \subseteq J_m$. We define $s(x) = \max(\operatorname{supp}(x))$. Moreover, recall that $\Delta(\Gamma) = \{\operatorname{supp}(x) : x \in \Gamma\} \subseteq \mathcal{P}(J_m)$ and $\Delta(\Gamma) = \{A \subseteq J_m : h(A \cup \{0\}) = h(A)\}$ by Proposition 2.3.

Lemma 5.3.4. *If $x \in \mathbf{P}$ is a minimal point of Γ, then $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$.*

Proof. From Theorem 3.3.2, $x \in \mathcal{B}(\mathcal{Z}, A)$ for some $A \subseteq [1, s(x)]$. We are going to prove that $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$ by checking that $h(A) = h([1, s(x)])$. Specifically, we show that $h(A \cup \{j\}) = h(A)$ for every $j \in [1, s(x)] \smallsetminus A$. Consider $j \in [1, s(x)] \smallsetminus A$ and the point $x' = x + \mathbf{e}^j - \mathbf{e}^{s(x)} \in \mathbf{P}$. Observe that $x' \in \Gamma$ because $x' - x \in H$. Applying Theorem 3.3.2 again, there exist $C \subseteq A \cup \{j\}$ with $C \in \Delta(\Gamma)$ and a point $u \in \mathcal{B}(\mathcal{Z}, C)$ such that $x' \geq u$. If $u_j = 0$, then $u < x$, but this is not possible because $x \in \min \Gamma$. Thus, $u_j = 1$ and $j \in C$. Since h is submodular,

$$h(A \cup \{j\}) + h(C \smallsetminus \{j\}) \leq h(A) + h(C).$$

Therefore, $h(A \cup \{j\}) = h(A)$ if $h(C) = h(C \smallsetminus \{j\})$. Suppose now that $h(C \smallsetminus \{j\}) \leq h(C) - 1$. Observe that

$$h(C \smallsetminus \{j\}) \geq |u(C \smallsetminus \{j\})| = |u(C)| - 1 = h(C) - 1$$

because $u \in \mathcal{B}(\mathcal{Z}, C)$. Hence, $h(C \smallsetminus \{j\}) = h(C) - 1$ and $u - \mathbf{e}^j \in \mathcal{B}(\mathcal{Z}, C \smallsetminus \{j\})$. Moreover $u - \mathbf{e}^j \notin \Gamma$ because $u - \mathbf{e}^j < x$ and $x \in \min \Gamma$. Thus, $C \smallsetminus \{j\} \notin \Delta(\Gamma)$ and

$$h((C \smallsetminus \{j\}) \cup \{0\}) = h(C \smallsetminus \{j\}) + 1 = h(C).$$

The submodularity of h implies that

$$\begin{aligned} h(A \cup \{j, 0\}) + h(C) &= h(A \cup \{j, 0\}) + h((C \smallsetminus \{j\}) \cup \{0\}) \leq h(A \cup \{0\}) + h(C \cup \{0\}) \\ &= h(A) + h(C). \end{aligned}$$

Therefore, $h(A \cup \{j\}) = h(A)$. □

Lemma 5.3.5. *If $x \in \mathbf{P}$ is an H-minimal point of Γ, then $x = y^{s(x)}(\mathcal{Z})$.*

Proof. From Lemma 5.3.4, $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$ and, since $\mathcal{B}(\mathcal{Z}, [1, s(x)]) \subseteq \Gamma$ by Theorem 3.3.2, x is H-minimal in $\mathcal{B}(\mathcal{Z}, [1, s(x)])$. By Lemmas 5.3.1 and 5.3.2, this implies that $x = y^{s(x)}(\mathcal{Z})$. □

Lemma 5.3.6. *If $x, y \in \mathbf{P}$ are two different H-minimal points of Γ, then $s(x) \neq s(y)$. Moreover, if $s(x) < s(y)$, then $|x| < |y|$.*

Proof. It is obvious from Lemma 5.3.5 that $s(x) \neq s(y)$ if $x \neq y$. Observe that $|x| = h([1, s(x)])$ and $|y| = h([1, s(y)])$, and hence $|x| \leq |y|$ if $s(x) < s(y)$. If $|x| = |y|$, then $x \in \mathcal{B}(\mathcal{Z}, [1, s(y)]) \subseteq y + H$ and $x - y \in H$, a contradiction. □

Lemma 5.3.7. *If $x, y \in \min_H \Gamma$ are such that $s(x) < s(y)$, then $x_i \geq y_i$ for all $i = 1, \ldots, s(x)$.*

Proof. A direct consequence of Lemmas 5.3.3 and 5.3.5. □

Lemma 5.3.8. *Let $x, y \in \mathbf{P}$ be two different H-minimal points of Γ with $s(x) < s(y)$ such that there is not any H-minimal point z with $s(x) < s(z) < s(y)$. If $x_i > y_i$ for some $i \in [1, s(x) - 1]$, then $|P_j| = x_j$ for all $j \in [i + 1, s(x)]$.*

Proof. Suppose that $x_i > y_i$ and $x_j < |P_j|$ for some i, j with $1 \leq i < j \leq s(x)$. Since $y_k \leq x_k$ for all $k = 1, \ldots, s(x)$ and $|y| > |x|$, there exists a point $y' \in (y + H_0) \cap \mathbf{P}$ such that

- $y'_k = y_k$ for all $1 \leq k < j$, and
- $y'_j = x_j + 1$, and
- $y'_k = x_k$ for all $j < k \leq s(x)$.

The point y' is in Γ but it is not in $\min \Gamma$, because $|y([j, s(x)])| > |x([j, s(x)])| = h([j, s(x)])$ and so $y' \notin \mathcal{D}(\mathcal{Z})$. Therefore, there exists $z' \in \min \Gamma$ such that $z' < y'$, and by Lemma 5.2.2 there exists $z \in \min_H \Gamma$ such that $z' - z \in H_0$. By Lemma 5.3.6, $s(z) < s(y)$ because $|z| = |z'| < |y'| = |y|$. Clearly, $s(z) \geq i$ because $z < y$ if $s(z) < i$. If $s(z) \leq s(x)$, then $z_k \geq x_k$ for all $k = 1, \ldots, s(z)$ by Lemma 5.3.7, a contradiction with $z_i \leq y'_i = y_i < x_i$. Therefore, there exists an H-minimal point z such that $s(x) < s(z) < s(y)$. □

5.4 A Family of Ideal Hierarchical Access Structures

Lemmas 5.3.6, 5.3.7, and 5.3.8 in the previous section provide necessary conditions for a Π-hierarchical access structure to be a matroid port, and hence to be ideal, in terms of the properties of its H-minimal points. A sufficient condition is given in this section by constructing a new family of hierarchical vector space secret sharing schemes. Specifically, we present a family of linearly representable integer polymatroids that are boolean and we prove that the multipartite access structures that are obtained from them are actually hierarchical. In addition, they are vector space access structures by Theorem 3.5.1.

Given a finite field $\mathbb{K}$ and a pair of integer vectors $\mathbf{a} = (a_0, \ldots, a_m) \in \mathbb{Z}_+^{m+1}$ and $\mathbf{b} = (b_0, \ldots, b_m) \in \mathbb{Z}_+^{m+1}$ such that

1. $a_0 = a_1 = b_0 = 1$, and
2. $a_i \leq a_{i+1} \leq b_i \leq b_{i+1}$ for every $i = 0, \ldots m - 1$,

take $d = b_m$ and consider a basis $\{e^1, \ldots, e^d\}$ of $\mathbb{K}^d$ and, for every $i = 1, \ldots, m$, consider the subspace $V_i = \langle e^{a_i}, \ldots, e^{b_i} \rangle \subseteq \mathbb{K}^d$. Let $\mathcal{Z}' = \mathcal{Z}'(\mathbf{a}, \mathbf{b}) = (J'_m, h)$ be the integer polymatroid that is linearly represented by the subspaces $V_0, V_1, \ldots, V_m$. This polymatroid is boolean, and so the rank function h of $\mathcal{Z}'$ is such that

$$h(A) = |\cup_{i \in A} [a_i, b_i]|$$

for all $A \subseteq J'_m$. In particular, $h([j, i]) = |[a_j, b_i]| = b_i - a_j + 1$ whenever $0 \leq j \leq i \leq m$, and hence $h(\{0\}) = 1$. Therefore, for every set of players P and for every m-partition $\Pi = (P_1, \ldots, P_m)$ of P such that $|P_i| \geq h(\{i\}) = b_i - a_i + 1$, we can consider the Π-partite matroid port $\Gamma = \Gamma_0(\mathcal{Z}')$ that is determined as in Theorem 3.3.2. Since $\mathcal{Z}'$ is $\mathbb{K}$-linearly representable for every finite field $\mathbb{K}$, we have from Theorem 3.5.1 that Γ is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. We prove in the following that Γ is actually a Π-hierarchical access structure.

Consider the integer polymatroid $\mathcal{Z} = \mathcal{Z}(\mathbf{a}, \mathbf{b}) = \mathcal{Z}'(J_m) = (J_m, h)$ and, for $i = 1, \ldots, m$, the points $y^i = y^i(\mathcal{Z}) \in \mathbb{Z}_+^m$. Observe that $y^i_j = h([j, i]) - h([j+1, i]) = a_{j+1} - a_j$ if $j < i$ while $y^i_i = b_i - a_i + 1$. Therefore,

$$y^i = (a_2 - a_1, \ldots, a_i - a_{i-1}, b_i - a_i + 1, 0, \ldots, 0).$$

In the following lemma, we present a characterization of the families of points $(y^i(\mathcal{Z}))_{1 \leq i \leq m}$ corresponding to integer polymatroids of the form $\mathcal{Z} = \mathcal{Z}(\mathbf{a}, \mathbf{b})$.

Lemma 5.4.1. *The points $y^1, \ldots, y^m \in \mathbb{Z}_+^m$ are of the form $y^i = y^i(\mathcal{Z}(\mathbf{a}, \mathbf{b}))$ for some $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_+^{m+1}$ in the above conditions if and only if*

1. *$s(y^i) = i$ for every $i = 1, \ldots, m$, and*
2. *$|y^i| \leq |y^{i+1}|$ and $y^i_i > y^{i+1}_i$ for every $i = 1, \ldots, m-1$, and*
3. *$y^i_j = y^{i+1}_j$ if $1 \leq j < i \leq m-1$.*

Proof. Clearly, the points of the form $y^i = y^i(\mathcal{Z}(\mathbf{a}, \mathbf{b}))$ satisfy the required conditions. We prove now the converse. Given points $y^1, \ldots, y^m \in \mathbb{Z}_+^m$ satisfying the conditions in the statement, consider $\mathbf{a} = (a_0, \ldots, a_m)$ and $\mathbf{b} = (b_0, \ldots, b_m)$ defined as follows:

- $a_0 = a_1 = b_0 = 1$,
- $a_i = \sum_{j=1}^{i-1} y^i_j + 1$ for all $i = 1, \ldots, m$,
- $b_i = \sum_{j=1}^{i} y^i_j$ for all $i = 1, \ldots, m$.

Clearly $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_+^{m+1}$, and $a_{i+1} - a_i = y^{i+1}_i \geq 0$ and $b_i = |y^i| \leq |y^{i+1}| = b_{i+1}$. In addition, $b_i - a_{i+1} = y^i_i - y^{i+1}_i - 1 \geq 0$. Finally observe that $y^i = (a_2 - a_1, \ldots, a_i - a_{i-1}, b_i - a_i + 1, 0, \ldots, 0)$ for all $i = 1, \ldots, m$. □

Lemma 5.4.2. *If $h(A) < h([\min(A), \max(A)])$, then there exists $t \in [\min(A), \max(A)] \smallsetminus A$ such that*

$$h(A) = h(A \cap [1, t]) + h(A \cap [t+1, m]).$$

Proof. Consider $t \in [\min(A), \max(A)] \smallsetminus A$ such that $h(A \cup \{s\}) > h(A)$ and define $A_1 = A \cap [1, t]$, and $A_2 = A \cap [t+1, m]$, and $B = \cup_{i \in A}[a_i, b_i]$. There exists $t' \in [a_t, b_t]$ such that $t' \notin B$, and hence

$$h(A) = |B \cap [1, t'-1]| + |B \cap [t'+1, m]| = h(A_1) + h(A_2).$$

□

Lemma 5.4.3. *If $x \in \min \Gamma$, then $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$.*

Proof. Take $A = \operatorname{supp}(x)$. Clearly, $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$ if $h(A) = h([1, s(x)])$. Suppose that $h(A) < h([1, s(x)])$. Observe that $h(A \cup \{0\}) = h(A)$ because $A \in \Delta(\Gamma)$, and hence $a_{\min(A)} = 1$. Then the subset $A' = A \cup [1, \min(A)]$ is such that $h(A') = h(A)$. By applying Lemma 5.4.2 to A', there exists $t \in [1, s(x)] \smallsetminus A'$ such that

$$h(A') = h(A' \cap [1, t]) + h(A' \cap [t+1, m]).$$

Consider $A_1 = A' \cap [1,t]$. Since $|x(B)| \leq h(B)$ for all $B \subseteq J_m$ and $|x| = h(A) = h(A')$, we have that $|x(A_1)| = h(A_1)$, and hence $x' = \sum_{i \in A_1} x_i \mathbf{e}^i \in \mathcal{B}(\mathcal{Z}, A_1)$. Then $x' \in \Gamma$ because $A_1 \in \Delta(\Gamma)$, a contradiction with $x \in \min \Gamma$. □

Lemma 5.4.4. *The access structure Γ is Π-hierarchical.*

Proof. It is enough to prove that $x + \mathbf{v}^i \in \Gamma$ if $x \in \Gamma$ and $x + \mathbf{v}^i \in \mathbf{P}$ (recall that, for $i = 1, \ldots, m-1$, we notate $\mathbf{v}^i = \mathbf{e}^i - \mathbf{e}^{i+1} \in H_0$). First, we argue that we can assume $x \in \min \Gamma$. Consider $z \in \min \Gamma$ with $z \leq x$. If $z_{i+1} = 0$ and $x + \mathbf{v}^i \in \mathbf{P}$, then $z \leq x + \mathbf{v}^i$, and hence $x + \mathbf{v}^i \in \Gamma$. If $z_{i+1} > 0$, then $z + \mathbf{v}^i \in \mathbf{P}$, and $x + \mathbf{v}^i \in \Gamma$ if $z + \mathbf{v}^i \in \Gamma$ because $z + \mathbf{v}^i \leq x + \mathbf{v}^i$.

Let $x \in \min \Gamma$ be such that $y = x + \mathbf{v}^i \in \mathbf{P}$. Then $k = s(x) > i$ and $x \in \mathcal{B}(\mathcal{Z}, [1,k])$. Clearly, $y \in \Gamma$ if $y \in \mathcal{B}(\mathcal{Z}, [1,k])$. Suppose that $y \notin \mathcal{B}(\mathcal{Z}, [1,k])$. We assert that, in this situation, there exists $t \in [1,i]$ such that $\sum_{j=t}^{i} y_j > h([t,i])$. Since $y \notin \mathcal{B}(\mathcal{Z}, [1, s(x)])$, there exists $A \subseteq [1,k]$ such that $|y(A)| > h(A)$ and that is minimal with this property. It is clear that $i \in A$ and $i+1 \notin A$. Take $t = \min(A)$ and $t' = \max(A)$. If $h(A) < h([t,t'])$, there exists by Lemma 5.4.2 a value $\ell \in [t,t'] \smallsetminus A$ such that $h(A) = h(A_1) + h(A_2)$, where $A_1 = A \cap [t,\ell]$ and $A_2 = A \cap [\ell+1, t']$. Then, $|y(A_j)| > h(A_j)$ if $i \in A_j$, a contradiction with the election of A. Therefore, $h(A) = h([t,t'])$ and $t' = i$ because $|y([t,t'])| > h([t,t'])$. This proves our assertion.

Observe that

$$h([1,i]) = \sum_{j=1}^{i} y_j^i = \sum_{j=1}^{t-1} y_j^i + h([t,i]) = \sum_{j=1}^{t-1} y_j^k + h([t,i]).$$

In addition, $\sum_{j=1}^{t-1}(x_j - y_j^k) \geq 0$ because $x \in \mathcal{B}(\mathcal{Z}, [1,k]) \subset y^k + H_0$. Therefore,

$$h([1,i]) \leq \sum_{j=1}^{t-1} x_j + h([t,i]) < \sum_{j=1}^{t-1} y_j + \sum_{j=t}^{i} y_j = |y([1,i])|.$$

Clearly, this implies that $|y([1,i])| = h([1,i]) + 1$. Then $|x([1,i])| = |y([1,i])| - 1 = h([1,i])$, and hence $x' = \sum_{j=1}^{i} x_j \mathbf{e}^j \in \mathcal{B}(\mathcal{Z}, [1,i])$ and $x' \in \Gamma$. But this is a contradiction with the fact that $x \in \min \Gamma$. Therefore, $y \in \mathcal{B}(\mathcal{Z}, [1,k])$ and $y \in \Gamma$. □

Lemma 5.4.5. *A point $x \in \mathbf{P}$ is H-minimal in Γ if and only if $x = y^i$ with $i = m$ or $i < m$ and $|y^i| < |y^{i+1}|$.*

Proof. From Lemma 5.3.5, $\min_H \Gamma \subseteq \{y^1, \ldots, y^m\}$, and hence $\min_H \Gamma = \min_H \{y^1, \ldots, y^m\}$. Take $i, j \in J_m$ with $i < j$ and define $v = y^i - y^j$. Then $v_k = \sum_{\ell=1}^{k}(y_\ell^i - y_\ell^j) = 0$ if $1 \leq k < i$, while $v_i = y_i^i - y_i^j > 0$, and $v_k \geq |y^i| - |y^j| = v_m$ if $i+1 \leq k \leq m$. Therefore, by Lemma 5.2.1, $y^j - y^i \notin H$ while $y^i - y^j \in H$ if and only if $|y^i| = |y^j|$. □

The next proposition summarizes the results in this section.

Proposition 5.4.6. *Let $\Pi = (P_1, \ldots, P_m)$ be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P. Let $x^1, \ldots, x^r \in \mathbb{Z}_+^m$ be the H-minimal points of Γ and define $m_i = \max(\mathrm{supp}(x^i))$. Suppose that the following properties are satisfied.*

1. *If $i < j$, then $m_i < m_j$ and $x^i_k = x^j_k$ for all $k = 1, \ldots, m_i - 1$.*

2. *If $m_{j-1} < i \leq m_j$, then $|P_i| \geq \sum_{\ell=i}^{m_j} x^j_\ell$.*

Then Γ is ideal and, moreover, admits a $\mathbb{K}$-vector space secret sharing scheme for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq \binom{n+1}{|x^r|}$.

Proof. Consider the points $y^1, \ldots, y^m \in \mathbf{P}$ defined as follows: if $m_{j-1} < i \leq m_j$, then

- $y^i_k = x^j_k$ for every $k = 1, \ldots, i$, and
- $y^i_i = \sum_{\ell=i}^{m_j} x^j_\ell$, and
- $y^i_k = 0$ for every $k = i+1, \ldots, m$.

Observe that $x^j_{m_j} > x^{j+1}_{m_j}$ because $x^j \leq x^{j+1}$ otherwise. With that in mind, it is not difficult to check that the points $y^1, \ldots, y^m \in \mathbb{Z}^m_+$ satisfy the conditions in Lemma 5.4.1, and hence there exists an integer polymatroid of the form $\mathcal{Z} = \mathcal{Z}(\mathbf{a}, \mathbf{b})$ such that $y^i = y^i(\mathcal{Z})$ for every $i = 1, \ldots, m$. In addition, from the previous results, $\Gamma_0(\mathcal{Z})$ is a Π-hierarchical access structure with $\min_H \Gamma_0(\mathcal{Z}) = \min_H\{y^1, \ldots, y^m\} = \{x^1, \ldots, x^r\}$. Therefore, $\Gamma = \Gamma_0(\mathcal{Z})$. Since $\mathcal{Z}$ is linearly representable over every finite field, Γ is a $\mathbb{K}$-vector space access structure for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq \binom{n+1}{h(J_m)}$ by Theorem 3.5.1, and $h(J_m) = |x^r|$. □

5.5 A Characterization of Ideal Hierarchical Access Structures

By using the results in Sections 5.3 and 5.4, we present here a complete characterization of ideal hierarchical access structures. Moreover, we prove that every ideal hierarchical access structure is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. The next result is a consequence of Proposition 5.4.6 and the necessary conditions for a hierarchical access structure to be ideal given in Section 5.3. It provides a characterization of hierarchical access structures in which the number of participants in every hierarchical level is large enough in relation to the H-minimal points.

Theorem 5.5.1. *Let $\Pi = (P_1, \ldots, P_m)$ be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P with $\min_H \Gamma = \{x^1, \ldots, x^r\}$. For $j = 1, \ldots, r$, consider $m_j = \max(\mathrm{supp}(x^j))$ and suppose that $|P_{m_j}| > x^j_{m_j}$. Then Γ is ideal if and only if*

1. *$m_i \neq m_j$ if $i \neq j$, and*

2. *if $m_i < m_j$, then $x^i_k = x^j_k$ for all $k = 1, \ldots, m_i - 1$.*

Moreover, in this situation Γ is a $\mathbb{K}$-vector space access structure for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq \binom{n+1}{|x^r|}$.

Proof. The conditions are necessary because of the results in Section 5.3. We prove now that they are also sufficient. Assume that the H-minimal points of Γ are ordered in such a way that $m_i < m_j$ if $i < j$. Consider a set $\widehat{P} \supseteq P$ and an m-partition $\widehat{\Pi} = (\widehat{P}_1, \ldots, \widehat{P}_m)$ of

$\widehat{P}$ such that $\widehat{P}_i \supseteq P_i$ for all $i = 1, \ldots, m$ and $|\widehat{P}_i| \geq \sum_{\ell=i}^{m_j} x_\ell^j$ if $m_{j-1} < i \leq m_j$. Let $\widehat{\Gamma}$ be the $\widehat{\Pi}$-hierarchical access structure with $\min_H \widehat{\Gamma} = \{x^1, \ldots, x^r\}$. By Proposition 5.4.6, $\widehat{\Gamma}$ is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$. Observe that $((x^j+H)\cap\widehat{\mathbf{P}})\cap\mathbf{P} = (x^j + H) \cap \mathbf{P}$ for every $j = 1, \ldots, r$. This implies that the access structure Γ is a minor of $\widehat{\Gamma}$. Specifically, $\Gamma = \widehat{\Gamma}\backslash(\widehat{P} \smallsetminus P)$. □

Finally, we present our complete characterization of ideal hierarchical access structures in terms of the properties of the H-minimal points. Actually, we prove that a hierarchical access structure is ideal if and only if it is a minor of an access structure in the family that is presented in Section 5.4. Therefore every ideal hierarchical access structure is a $\mathbb{K}$-vector access structure for all large enough finite fields $\mathbb{K}$.

Theorem 5.5.2. *Let $\Pi = (P_1, \ldots, P_m)$ be an m-partition of a set P of n participants and let Γ be a Π-hierarchical access structure on P with $\min_H \Gamma = \{x^1, \ldots, x^r\}$. Consider $m_j = \max(\mathrm{supp}(x^j))$ and suppose that the H-minimal points are ordered in such a way that $m_j \leq m_{j+1}$. Then Γ is ideal if and only if*

1. *$m_j < m_{j+1}$ and $|x^j| < |x^{j+1}|$ for all $j = 1, \ldots, r-1$, and*
2. *$x_i^j \geq x_i^{j+1}$ if $1 \leq j \leq r$ and $1 \leq i \leq m_j$, and*
3. *if $x_i^j > x_i^r$ for some $1 \leq j < r$ and $1 \leq i < m_j$, then $|P_k| = x_k^j$ for all $k = i+1, \ldots, m_j$.*

Moreover, in this situation Γ is a $\mathbb{K}$-vector space access structure for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq \binom{n+1}{|x^r|}$.

Proof. As before, the results in Section 5.3 imply that the given conditions are necessary. Suppose that the conditions are satisfied. Take $\widehat{x}^r = x^r$, and for $j = 1, \ldots, r-1$ consider the point $\widehat{x}^j \in \mathbb{Z}_+^m$ defined by

- $\widehat{x}_i^j = x_i^r$ if $1 \leq i \leq m_j - 1$, and
- $\widehat{x}_{m_j}^j = x_{m_j}^j + \sum_{k=1}^{m_j-1}(x_k^j - x_k^r)$, and
- $\widehat{x}_i^j = 0$ if $m_j + 1 \leq i \leq m$.

As we did in the proof of Theorem 5.5.1, we extend the set P of participants to a larger one. Consider a set $\widehat{P} \supseteq P$ and an m-partition $\widehat{\Pi} = (\widehat{P}_1, \ldots, \widehat{P}_m)$ of $\widehat{P}$ such that $\widehat{P}_i \supseteq P_i$ for all $i = 1, \ldots, m$ and $|P_i| \geq \sum_{\ell=i}^{m_j} \widehat{x}_\ell^j$ if $m_{j-1} < i \leq m_j$. Let $\widehat{\Gamma}$ be the $\widehat{\Pi}$-hierarchical access structure on $\widehat{P}$ with $\min_H \widehat{\Gamma} = \{\widehat{x}^1, \ldots, \widehat{x}^r\}$. It is not difficult to check that $\widehat{\Gamma}$ satisfies the conditions in Proposition 5.4.6, and hence it is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$. Consider the integer polymatroid $\widehat{\mathcal{Z}}' = (J'_m, \widehat{h})$ associated to $\widehat{\Gamma}$ and take $\widehat{\mathcal{Z}} = \widehat{\mathcal{Z}}'(J_m) = (J_m, \widehat{h})$.

The proof is concluded by checking that Γ is a minor of $\widehat{\Gamma}$. Specifically, we prove that

$$\Gamma = (\{x^1, \ldots, x^r\} + H) \cap \mathbf{P} = (\{\widehat{x}^1, \ldots, \widehat{x}^r\} + H) \cap \mathbf{P} = \widehat{\Gamma} \cap \mathbf{P},$$

which implies that $\Gamma = \widehat{\Gamma}\backslash(\widehat{P} \smallsetminus P)$. Observe that $x^j - \widehat{x}^j \in H_0$, and hence $\Gamma \subseteq \widehat{\Gamma} \cap \mathbf{P}$. For $j = 1, \ldots, r$, consider $A_j = (\widehat{x}^j + H_0) \cap \mathbf{P}$. Clearly, it is enough to prove that $A_j \subseteq \Gamma$ for

all $j = 1, \ldots, r$. Suppose that, on the contrary, there exists $j = 1, \ldots, r$ such that $A_j \not\subseteq \Gamma$ while $A_k \subseteq \Gamma$ for all $k = 1, \ldots, j-1$.

Suppose that $x^j \notin \mathcal{B}(\widehat{\mathcal{Z}}, [1, m_j])$. Then $x^j \notin \min \widehat{\Gamma}$ and, since $x^j \in \widehat{\Gamma}$, there exists $z \in \min \widehat{\Gamma}$ with $z < x^j$. By Lemma 5.2.2, there exists an H-minimal point x of $\widehat{\Gamma}$ such that $z - x \in H_0$, and hence $|x| = |z| < |x^j|$. This is impossible if $j = 1$. If $j > 1$, then $x = \widehat{x}^k$ for some $k < j$, and hence $z \in A_k \subseteq \Gamma$. Clearly, $z \in \min \Gamma$ and, by applying Lemma 5.2.2 again, $z - x^k \in H_0$. This implies that $x^j - x^k = (x^j - z) + (z - x^k) \in H$, a contradiction. Therefore, $x^j \in \mathcal{B}(\widehat{\mathcal{Z}}, [1, m_j])$.

Consider $R = A_j \setminus \Gamma$ and consider a point $y \in R$ that is H-minimal in R. We assert that $y \in \mathcal{B}(\widehat{\mathcal{Z}}, [1, m_j])$. If not, $y \in \widehat{\Gamma}$ but $y \notin \min \widehat{\Gamma}$. By repeating the previous argument, $j > 1$ and $y - x^k \in H$ for some $k < j$. Since $y \notin \Gamma$, we reached a contradiction that proves our assertion.

Let $i \in J_m$ be the smallest value such that $y_i \neq x_i^j$. If $y_i < x_i^j$, there exists ℓ with $i + 1 \leq \ell \leq m_j$ such that $y_\ell > x_\ell^j$. Since $y - \widehat{x}^j \in H_0$, it follows that

$$|\widehat{x}^j([1, i])| \leq |y([1, i])| < |x^j([1, i])|,$$

and hence $x_s^r = \widehat{x}_s^j < x_s^j$ for some s with $1 \leq s \leq i$. This implies that $x_\ell^j = |P_\ell|$ and $y_\ell \leq x_\ell^j$ because $y \in \mathbf{P}$, a contradiction. If $y_i > x_i^j$, then $y_\ell < x_\ell^j$ and $y' = y - \mathbf{e}^i + \mathbf{e}^\ell \in \mathcal{B}(\widehat{\mathcal{Z}}, [1, m_j]) \cap \mathbf{P}$ for some ℓ with $i + 1 \leq \ell \leq m_j$. Since $y - y' \in H_0$ and and y is an H-minimal point in R, it follows that $y' \notin R$, and hence $y' \in \Gamma$, a contradiction with $y \notin \Gamma$. □

By combining Theorem 5.5.2 with the results in previous sections and the ones in [68], the results in this chapter can be summarized in the following corollary. In Corollary 5.5.4 we show a general bound on the complexity of non-ideal hierarhical access structures.

Corollary 5.5.3. *Let Γ be a hierarchical access structure. The following properties are equivalent:*

1. *Γ admits a vector space secret sharing scheme over every large enough finite field.*
2. *Γ is ideal.*
3. *Γ admits a secret sharing scheme in which the length of every share is less than $3/2$ times the length of the secret value.*
4. *Γ is a matroid port.*

Corollary 5.5.4. *Let Γ be a hierarchical access structure in which the number of H-minimal points is r. Then*

$$\lambda(\Gamma) \leq r.$$

Example 5.5.5. Let Γ be the weighted theshold access structure defined by the vector of weights $w = (7, 5, 4, 3)$ and the threshold $T = 13$ on the set of participants $P = P_1 \cup P_2 \cup P_3 \cup P_4$ with $|P_i| = 4$ for all $i = 1, \ldots, 4$. The H-minimal points of Γ are $x^1 = (2, 0, 0, 0)$, $x^2 = (0, 1, 2, 0)$, and $x^3 = (0, 0, 1, 3)$. Since $x_2^2 > x_2^3$ and $|P_3| > x_3^2$, it follows from Theorem 5.5.2 that Γ is not ideal.

Example 5.5.6. Let $P = P_1 \cup P_2 \cup P_3 \cup P_4$ be a set of participants and $t_1 < t_2 < t_3 < t_4$ some positive integers. Consider a 4-partite hierarchical scheme on P with access structure Γ in which all authorized subsets must have at least one participant from P_1, and also must have t_1 participants in P_1, or t_2 in $P_1 \cup P_2$, or t_3 in $P_1 \cup P_2 \cup P_3$, or t_4 in P. The access structure of this scheme, Γ, is a minor of Γ', the access structure whose H-minimal points are $(1,0,0,t_4)$, $(1,0,t_3,0)$, $(1,t_2,0,0)$ and $(t_1,0,0,0)$. Since Γ' is ideal by Proposition 5.4.6, Γ is ideal.

The access structures described in Example 5.2.3 with and Example 5.2.4 are ideal. If Γ is a hierarchical access structure with just one H-minimal point $(t_1, t_2 - t_1, \ldots, t_m - t_{m-1})$, it is ideal by Proposition 5.4.6. The vector subspaces $V_0, \ldots, V_m$ that represent the polymatroid associated to Γ satisfy $V_m \subset \ldots \subset V_1$, $V_0 \subset V_1$, and $V_0 \nsubseteq V_i$ for $i \neq 1$. If Γ is a hierarchical access structure with $\min_H \Gamma = \{t_1\mathbf{e}^1, \ldots, t_m\mathbf{e}^m\}$, then Γ is also ideal and the vector subspaces $V_0, \ldots, V_m$ satisfy $V_0 \subset V_1 \subset \ldots \subset V_m$.

Tassa in [101] proposed an open problem on hierarchical access structures that can be solved by using our results. For a set of participants $P = P_1 \cup \cdots \cup P_m$, he asked for which sequence of integers $0 < k_1 < \cdots < k_m$ and for which $\ell \in \{1, \ldots, m\}$, the access structure defined as follows is ideal

$$\Gamma_\ell = \bigcup_{A \in \{1,\ldots,m\},\, |A|=\ell} \left\{ x \in \mathbf{P} : \sum_{j=1}^{i} x_j \geq k_i \text{ for all } i \in A \right\}$$

We assume that the access structure is strictly m-partite. In particular, we assume that $\sum_{j=1}^{i} |P_i| \geq k_i$ for all $i = 1, \ldots, m$.

Corollary 5.5.7. *The access structure Γ_ℓ is ideal if and only if $\ell = 1$ or $\ell = m$.*

Proof. Let $\Pi = (P'_1, \ldots, P'_m)$ be a partition of a set $P' \supset P$ with $P'_i \supset P_i$ and $|P'_i| > k_i$ for all $i = 1, \ldots, m$. For every subset $A = \{i_1, \ldots, i_\ell\} \subset [1, m]$ with $i_j < i_{j+1}$ for $j = 1, \ldots, \ell - 1$, consider the vector v^A defined as

- $v^A_{i_1} = k_{i_1}$
- $v^A_{i_j} = k_{i_j} - k_{i_{j-1}}$ for $j = 2, \ldots, \ell$
- $v^A_j = 0$ for all $j \notin A$

Define w^A as the H-minimal point of $(v^A + H) \cap \mathbf{P}$, which is not empty by hypothesis, that satisfies $m(w^A) = i_\ell$. Let Γ'_ℓ be the Π-partite access structure whose set of H-minimal points is $\{v^A : A \subset [1, m] \text{ and } |A| = \ell\}$. Observe that $\Gamma_\ell = \Gamma'_\ell \cap \mathbf{P} = (\{w^A : A \subset [1, m] \text{ and } |A| = \ell\} + H) \cap \mathbf{P}$. By Theorem 5.5.1, if $\ell = 1$ or $\ell = m$ then Γ'_ℓ is ideal and hence Γ_ℓ is so.

Suppose that $\ell \neq 1, m$. If there exist two subsets A, A' of size ℓ with $w^A \neq w^{A'}$ but $m(w^A) = m(w^{A'})$, then Γ_ℓ is not ideal by Theorem 5.5.2. If not, then we claim that Γ is not strictly m-partite. Define $\tilde{w}^t = w^{[m-\ell-t+1, m-t]}$ for every $t = 0, \ldots, m - \ell$. Taking into account that for every $1 \leq i \leq m-\ell-t$, $\tilde{w}^t = w^A$ for $A = [m-\ell-t+1, m-t] \cup \{i\} \setminus \{m-t-1\}$, it follows $\sum_{j=1}^{i} \tilde{w}^t_j = k_i$ for $t = 0, \ldots, m - \ell$ and $i = 1, \ldots, m - t$. Hence $\tilde{w}^t = v^{[1,\ldots,m-t]}$. Since $\tilde{w}^t \geq \tilde{w}^{t-1}$ for $t = 1, \ldots, m - \ell$, then $\min_H \Gamma = \{\tilde{w}^{m-\ell+1}\}$, and so the participants in the parts $m - \ell + 2, \ldots, m$ are not relevant in the structure. ∎

5.6 Ideal Weighted Threshold Access Structures

By using our characterization of ideal hierarchical access structures, we present in this section a characterization of ideal weighted threshold access structures that is more precise than the one given by Beimel, Tassa and Weinreb [6]. As was noticed in [6], such an ideal structure can be the composition smaller ideal weighted threshold access structures. Because of that, we focus on the indecomposable structures in this family.

First, we describe several families of ideal weighted threshold access structures, and then we prove in Theorem 5.6.1 that every indecomposable ideal weighted threshold access structure must be in one of these families.

The (t, n)-threshold access structures form the first of those families. Of course, they are ideal weighted threshold access structures. We consider as well three families of ideal bipartite hierarchical access structures, that is, ideal Π-hierarchical access structures for some partition $\Pi = (P_1, P_2)$ of the set of participants.

$\mathbf{B}_1$ This family consists of the access structures with $\min_H \Gamma = \{(x_1, x_2)\}$, where $0 < x_1 < |P_1|$ and $0 < x_2 = |P_2| - 1$. We affirm that every member of $\mathbf{B}_1$ is a weighted threshold access structure with weight vector

$$w = (w_1, w_2) = \left(1 + \frac{1}{x_1 + x_2}, 1 - \frac{x_1}{x_2(x_1 + x_2)}\right)$$

and threshold $T = x_1 + x_2$. Observe that the H-maximal non-authorized points of $\Gamma \in \mathbf{B}$ are $u = (x_1 - 1, x_2 + 1)$ and $u' = (t, x_2 + x_1 - 1 - t)$, where $t = \min\{|P_1|, x_2 + x_1 - 1\}$. Our affirmation is proved by checking that $(x_1, x_2) \cdot w \geq T$ while $u \cdot w < T$ and $u' \cdot w < T$.

$\mathbf{B}_2$ The family $\mathbf{B}_2$ is formed by the access structures with $\min_H(\Gamma) = \{(x_1, 0), (0, x_1 + 1)\}$ for some integer $x_1 > 1$. Those structures are defined by the weights $w = (w_1, w_2) = (1, 1 - 1/(x_1 + 1))$ and the threshold $T = x_1$, because $u = (x_1 - 1, 1)$ is the only H-maximal non-authorized point of Γ, and $x \cdot w \geq T$ for every $x \in \min_H \Gamma$ while $u \cdot w < T$

$\mathbf{B}_3$ This is the family of the access structures with $\min_H \Gamma = \{(y_1 + y_2 - 1, 0), (y_1, y_2)\}$, where $y_1 > 0$, $y_2 > 2$, and $|P_2| \leq y_2 \leq |P_2| + 1$. In this case we have weighted threshold access structures with $w = (w_1, w_2) = (1, 1 - 1/y_2)$ and $T = y_1 + y_2 - 1$. This is proved as before by taking into account the H-maximal non-authorized points of Γ are $u = (y_1 + y_2 - 2, 1)$ and $u' = (y_1 - 1, y_2 + 1)$ (the second point only if $|P_2| = y_2 + 1$).

In addition we consider three families of ideal tripartite hierarchical access structures.

$\mathbf{T}_1$ This family consists of the structures with $\min_H \Gamma = \{(x_1, 0, 0), (0, y_2, y_3)\}$, where $0 < y_2 < |P_2|$ and $1 < y_3 = |P_3| - 1$, and $x_1 = y_2 + y_3 - 1$. By taking into account that the H-maximal non-authorized points of Γ are $u = (x_1 - 1, 1, 0)$ and $u' = (y_2 - 1, 0, y_3 + 1)$, one can prove that every $\Gamma \in \mathbf{T}_1$ is a weighted threshold access structure with

$$w = \left(1, 1 - \frac{1}{(y_3 + 1)(y_2 + y_3)}, 1 - \frac{1}{y_3} + \frac{y_2}{y_3(y_3 + 1)(y_2 + y_3)}\right)$$

and $T = x_1$.

$\mathbf{T}_2$ We consider in this case the structures such that $\min_H \Gamma = \{(x_1, 0, 0), (y_1, y_2, y_3)\}$ with $0 < y_2 = |P_2|$ and $1 < y_3 = |P_3| - 1$, and $x_1 = y_1 + y_2 + y_3 - 1$. The H-maximal non-qualified points of those access structures are $u = (x_1 - 1, 1, 0)$ and $u' = (y_1 + y_2 - 1, 0, y_3 + 1)$. As before, we can check that the weights

$$w = \left(1, 1 - \frac{1}{(y_3+1)(y_1+y_2+y_3)}, 1 - \frac{1}{y_3} + \frac{y_1+y_2}{y_3(y_3+1)(y_1+y_2+y_3)}\right)$$

and the threshold $T = x_1$ determine Γ.

$\mathbf{T}_3$ Finally, the family $\mathbf{T}_3$ contains the structures with $\min_H \Gamma = \{(x_1, x_2, 0), (y_1, y_2, y_3)\}$, where $0 < y_1 < x_1$, and $1 < y_3 = |P_3|$, and $0 < x_2 = y_2 + 1 = |P_2|$, and $x_1 + x_2 = y_1 + y_2 + y_3 - 1$. In this case we can consider the threshold $T = x_1 + x_2$ and the weight vector

$$w = \left(1 + \frac{1}{(x_1+x_2)^2}, 1 - \frac{x_1}{x_2(x_1+x_2)^2}, 1 - \frac{1}{x_1 - y_1 + 2}\left(1 + \frac{x_2 y_1 - x_1(x_2-1)}{x_2(x_1+x_2)^2}\right)\right).$$

Observe that the H-maximal non-authorized points of Γ are $u = (x_1 + x_2 - 1, 0, 1)$ and $u' = (y_1 - 1, x_2, x_1 - y_1 + 2)$.

At this point, we can state the result that provides our characterization of the ideal weighted threshold access structures.

Theorem 5.6.1. *A weighted threshold access structure is ideal if and only if*

1. *it is a threshold access structure, or*
2. *it is a bipartite access structure in one of the families $\mathbf{B}_1$, $\mathbf{B}_2$ or $\mathbf{B}_3$, or*
3. *it is a tripartite access structure in one of the families $\mathbf{T}_1$, $\mathbf{T}_2$ or $\mathbf{T}_3$, or*
4. *it is a composition of smaller ideal weighted threshold access structures.*

The rest of this section is devoted to the proof this theorem, which is divided into several partial results. We assume that Γ is an ideal Π-hierarchical access structure for some partition $\Pi = (P_1, \ldots, P_m)$ of the set P of participants. Consider the set $\min_H \Gamma = \{x^1, \ldots, x^r\}$ of the H-minimal points of Γ. As before, we assume that $m_j < m_{j+1}$, where $m_j = \max(\mathrm{supp}(x^j))$. We begin by proving some technical lemmas.

Lemma 5.6.2. *If there exists $i \in J_m$ such that $x_i^j = 0$ for all $j = 1, \ldots, r$, then Γ is not strictly m-partite.*

Proof. If $i = m$, it is clear that the participants in P_m are redundant. If $i < m$ it is enough to prove that the participants in P_i are equivalent to the ones in P_{i+1}. Consider $x \in \min \Gamma$ such that $x' = x - \mathbf{e}^i + \mathbf{e}^{i+1} = x - \mathbf{v}^i \in \mathbf{P}$. Consider an H-minimal point y with $u = x - y \in G$. Then $\hat{u}_i - \hat{u}_{i-1} = u_i = x_i - y_i = x_i > 0$, and hence $\hat{u}_i > 0$. Therefore, $u - \mathbf{v}^i \in H$ and $x' = y + u - \mathbf{v}^i \in \Gamma$. ∎

Lemma 5.6.3. *If there exist $j \in \{2,\dots,r\}$ and $i \in J_m$ such that $m_{j-1}+1 < i \le m_j$ and $x_i^k = |P_i|$ for all $k = i,\dots,r$, then Γ is not strictly m-partite.*

Proof. We claim that, in this situation, the participants in P_{i-1} and those in P_i are hierarchically equivalent. Consider $x \in \min\Gamma$ such that $x' = x - \mathbf{e}^{i-1} + \mathbf{e}^i = x - \mathbf{v}^{i-1} \in \mathbf{P}$. This implies that $x_i < |P_i|$ Consider an H-minimal point y with $u = x - y \in G$. Observe that $s(y) \ge i$ because $m_{j-1} < i-1$. Then $\hat{u}_i - \hat{u}_{i-1} = u_i = x_i - y_i = x_i - |P_i| < 0$, and hence $\hat{u}_{i-1} > 0$. Therefore, $u - \mathbf{v}^{i-1} \in H$ and $x' = y + u - \mathbf{v}^{i-1} \in \Gamma$. □

Lemma 5.6.4. *If $r \ge 2$ and there exist $j \in \{1,\dots,r-1\}$ and $i \in [1, m_j]$ such that $x^j([1,m_j]) = x^k([1,m_j]) + \mathbf{e}^i$ for all $k = j+1,\dots,r$, then Γ is decomposable.*

Proof. Suppose first that $i = m_j$. Consider $p \notin P$ and define $P_i' = P_i \cup \{p\}$. Consider as well the points $y^j = x^j([1,m_j]) + \mathbf{e}^i$, and $y^k = x^k([1,m_j])$ for $1 \le k < j$, and $z^k = x^k([m_j+1, m])$ for $j < k \le r$. Let Γ_1 be the $(P_1,\dots,P_{i-1},P_i')$-hierarchical access structure with $\min_H \Gamma_1 = \{y^1,\dots,y^j\}$, and let Γ_2 be the $(P_{i+1},\dots,P_m)$-hierarchical access structure with $\min_H \Gamma_2 = \{z^{j+1},\dots,z^r\}$. It is easy to check that $\Gamma = \Gamma_1[\Gamma_2; p]$.

Suppose now that $i < m_j$. In this case, $x_k^j = |P_k|$ for all $k = i+1,\dots,m_j$ by Theorem 5.5.2. Consider the point $y^j = x^j([1,m_j]) + \mathbf{e}^{m_j} - \mathbf{e}^i$, and the points $y^k = x^k([1,m_j])$ for all $1 \le k < j$ and $z^k = x^k([m_j+1,m])$ for all $j < k \le r$. Consider Γ_1 and Γ_2 defined as in the previous case and observe that $\Gamma = \Gamma_1[\Gamma_2; p]$. □

Lemma 5.6.5. *If $m \ge 2$ and $x_1^j = |P_1|$ for all $j = 1,\dots,r$, then Γ is decomposable.*

Proof. Consider $p \notin P$ and $P_1' = P_1 \cup \{p\}$, and the points $z^j = x^j([2,m])$ for all $j = 1,\dots,r$. Let Γ_1 be the (x_1^1+1, x_1^1+1)-threshold access structure on P_1' and let Γ_2 be the $(P_2,\dots,P_m)$-hierarchical access structure with $\min_H \Gamma_2 = \{z^1,\dots,z^r\}$. Then $\Gamma = \Gamma_1[\Gamma_2; p]$. □

Lemma 5.6.6. *If $m \ge 2$ and Γ is indecomposable, then $x_m^r > 1$*

Proof. Suppose that $m_{r-1} < m-1$ and $x_m^r = 1$. Consider $p \notin P$ and define $P_{m-1}' = P_{m-1} \cup \{p\}$, and the points $y^j = x^j([1,m-1])$ for $1 \le j \le m$. Let Γ_1 be the $(P_1,\dots,P_{m-2},P_{m-1}')$-hierarchical access structure with $\min_H \Gamma_1 = \{y^1,\dots,y^r\}$ and let Γ_2 the $(1,|P_m|)$-threshold access structure on P_m. One can check that $\Gamma = \Gamma_1[\Gamma_2; p]$. If $m_{r-1} = m-1$, then $x_m^r > 1$ by Theorem 5.5.2. □

We can now proceed to prove Theorem 5.6.1 by considering several cases depending on the number m of levels in the structure. Recall that a weighted threshold access structure with weight vector $w = (w_1,\dots,w_m) \in \mathbb{R}_+^m$, where $w_1 > \cdots > w_m > 0$, is W-stable for $W = W(w) = \{v \in \mathbb{Z}^m : v \cdot w \ge 0\}$. The fact that $W \cup (-W) = \mathbb{Z}^m$ will be very useful in our discussion.

The case $m = 1$ clearly corresponds to the threshold access structures. We discuss in Proposition 5.6.7 the case $m = 2$, that is, the characterization of ideal weighted threshold access structures with two weights. Actually, this was previously solved in [85, 86], but we are only interested in the indecomposable ones. The case $m \ge 3$ is analyzed in Propositions 5.6.8, 5.6.10 and 5.6.12.

Proposition 5.6.7. *Every ideal indecomposable weighted threshold access structure that is strictly bipartite is in one of the families $\mathbf{B}_1$, $\mathbf{B}_2$ or $\mathbf{B}_3$.*

Proof. Let Γ be an ideal indecomposable weighted threshold access structure with weight vector $w = (w_1, w_2) \in \mathbb{R}^2$. Suppose that $\min_H \Gamma = \{(x_1, x_2)\}$. Taking into account Lemmas 5.6.2, 5.6.3 and 5.6.5, it is clear that $0 < x_1 < |P_1|$ and $1 < x_2 < |P_2|$. If $|P_2| \geq x_2 + 2$, then $(x_1, x_2) + (-1, 2) \in \mathbf{P} \smallsetminus \Gamma$, which implies that $(-1, 2) \notin W$, and hence $(1, -2) \in W$. But $(x_1, x_2) + (1, -2) \in \mathbf{P} \smallsetminus \Gamma$, a contradiction implying that $|P_2| = x_2 + 1$. Then $\Gamma \in \mathbf{B}_1$ in this case. Suppose now that $\min_H \Gamma = \{(x_1, 0), (y_1, y_2)\}$. Since $y_2 \geq 2$ by Lemma 5.6.6 and $x_1 - y_1 \geq 2$ by Lemma 5.6.4, $(y_1, y_2) + (1, -2) \in \mathbf{P} \smallsetminus \Gamma$, so $(1, -2) \notin W$ and $w_1 < 2w_2$. In addition, $w_1 > (y_2 + y_1 - x_1)w_2$ because $(x_1, x_2) + (-1, y_2 + y_1 - x_1) \in \mathbf{P} \smallsetminus \Gamma$. This implies that $x_1 = y_2 + y_1 - 1$. If $y_1 = 0$ then $y_2 = x_1 + 1$, and hence $\Gamma \in \mathbf{B}_2$. Suppose that $y_1 > 0$. If $|P_2| \geq y_2 + 2$, then $(y_1, y_2) + (-1, 2) \in \mathbf{P} \smallsetminus \Gamma$, which implies that $(-1, 2) \notin W$, and hence $(1, -2) \in W$. But $(y_1, y_2) + (1, -2) \in \mathbf{P} \smallsetminus \Gamma$, a contradiction implying that $|P_2| \leq y_2 + 1$. Then $\Gamma \in \mathbf{B}_3$. This concludes the proof because, by Theorem 5.5.2, all possible cases for ideal hierarchical bipartite access structures have been analyzed. □

Proposition 5.6.8. *Let Γ be an ideal indecomposable weighted threshold access structure. If Γ is strictly m-partite with $m \geq 3$, then $r = |\min_H(\Gamma)| = 2$.*

Proof. Let Γ be an ideal indecomposable weighted threshold access structure with weight vector $w \in \mathbb{R}^m_+$. Suppose that $r = 1$. From Lemmas 5.6.2, 5.6.3 and 5.6.5, $0 < x^1_i < |P_i|$ for all $i = 1, \ldots, m$. This implies that the points $x^1 + (\mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^m)$ and $x^1 - (\mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^m)$ are in $\mathbf{P} \smallsetminus \Gamma$, and hence the vector $\mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^m$ is not in W nor in $-W$, a contradiction.

Suppose that $r \geq 3$. Define $x = x^{r-2}$, $y = x^{r-1}$, $z = x^r$, $i = m_{r-2}$, and $j = m_{r-1}$. By Theorem 5.5.2, $x' = x - \mathbf{e}^i + \mathbf{e}^j + \mathbf{e}^m \in \mathbf{P} \smallsetminus \Gamma$ because $|x'([1, m_k])| < |x^k|$ for all $k = 1, \ldots, r$. Thus $-\mathbf{e}^i + \mathbf{e}^j + \mathbf{e}^m \notin W$ and so $w_i > w_j + w_m$.

Suppose that $z_i < |P_i|$ and define the point $z' = z + \mathbf{e}^i - 2\mathbf{e}^m$, which is in $\mathbf{P}$ by Lemma 5.6.5. We claim that $z' \notin \Gamma$. Observe that $z' - x^k \notin H$ for all $k = 1, \ldots, r-2$ because $z'([1, m_k]) = z([1, m_k]) < x^k([1, m_k])$. Moreover, $z' - z \notin H$ because $|z'| < |z|$. Suppose now that $z' - x \in H$. In this case it is clear that $|z'([1, i])| \geq |x([1, i])|$. By Theorem 5.5.2, $|x([1, i])| = |z([1, i])| + 1 = |z'([1, i])|$. Since $z_i < |P_i|$, by applying Theorem 5.5.2 again it follows $x([1, i]) = z([1, i]) + \mathbf{e}^i$. Observe that $y([1, i]) = z([1, i])$ because $x([1, i]) > y([1, i])$. By Lemma 5.6.4, this is a contradiction. Therefore, $z' - x \notin H$. We prove now that $z' - y \notin H$. On the contrary, $|z'([1, j])| = |y([1, j])|$. If $y_j > z_j$, then $y([1, j]) = z([1, j]) + \mathbf{e}^j$, a contradiction by Lemma 5.6.4. If $y_j = z_j$ then there exists by Theorem 5.5.2 a value $k \in \{1, \ldots, j-1\}$ for which $y_k = z_k + 1$, $y_\ell = z_\ell = |P_\ell|$ for all $\ell = k+1, \ldots, j$, and $y_\ell = z_\ell$ for all $\ell = 1, \ldots, k-1$, a contradiction by Lemma 5.6.4. Therefore $z' \in \mathbf{P} \smallsetminus \Gamma$, and hence $w_i < 2w_m$, a contradiction.

Suppose that $z_i = |P_i|$. By Theorem 5.5.2 there exists $k \in \{1, \ldots, i-1\}$ for which $x_k > z_k$ and $|P_\ell| = z_\ell = x_\ell$ for all $\ell = k+1, \ldots, i$. Define $z' = z + \mathbf{e}^k - 2\mathbf{e}^m$. Analogously to the previous case, $z' \in \mathbf{P} \smallsetminus \Gamma$. Therefore, $w_k < 2w_m$, a contradiction. □

Lemma 5.6.9. *Let Γ be an ideal weighted threshold access structure that is strictly m-partite and indecomposable. If $r = 2$ and $m_1 > 1$, then $x^2_1 > 0$.*

Proof. Suppose that $x^2_1 = 0$. By Lemma 5.6.2, $x^1_1 > 0$ and, as consequence of Theorem 5.5.2, $x^1_\ell = |P_\ell|$ for all $\ell = 2, \ldots, m_1$. Then observe that participants in P_1 and P_2 are hierarchically equivalent, and hence Γ is $(P_1 \cup P_2, P_3, \ldots, P_m)$-partite with H-minimal points $(x^i_1 + x^i_2, x^i_3, \ldots, x^i_m)$ for $i = 1, 2$. □

Proposition 5.6.10. *Every ideal indecomposable weighted threshold access structure that is strictly tripartite is in one of the families* $\mathbf{T}_1$, $\mathbf{T}_2$ *or* $\mathbf{T}_3$.

Proof. Let Γ be an ideal indecomposable weighted threshold access structure with vector of weights $w \in \mathbb{R}^3_+$. Assume that Γ is strictly tripartite. By Proposition 5.6.8, Γ has exactly two minimal points.

Suppose that $\min_H \Gamma = \{x, y\} = \{(x_1, 0, 0), (y_1, y_2, y_3)\}$. Taking into account Lemmas 5.6.2, 5.6.3, and 5.6.5, it is clear that $0 < y_2$ and $1 < y_3 < |P_3|$. By Lemma 5.6.4, $x_1 > y_1 + 1$, which implies that $y + (1, -1, -1) \in \mathbf{P} \setminus \Gamma$. Hence $(1, -1, -1) \notin W$ and so $w_1 < w_2 + w_3$. Suppose that $y_2 = |P_2|$. If $|P_3| > y_3 + 1$, then $y + (0, -1, 2) \in \mathbf{P} \setminus \Gamma$ and so $w_2 > 2w_3$. But $w_1 < 2w_3$ because $y + (1, 0, -2) \in \mathbf{P} \setminus \Gamma$, a contradiction. Therefore, $|P_3| = y_3 + 1$ and Γ is in $\mathbf{T}_2$. Now suppose that $y_2 < |P_2|$. In this case $y + (0, 1, -2) \in \mathbf{P} \setminus \Gamma$. If $|P_3| > y_3 + 1$, then $y + (0, -1, 2) \in \mathbf{P} \setminus \Gamma$, a contradiction implying that $|P_3| = y_3 + 1$. If $y_1 > 0$, then $y + (-1, 1, 1) \in \mathbf{P} \setminus \Gamma$, a contradiction. Consequently, $y_1 = 0$ and Γ is in $\mathbf{T}_1$.

Suppose that $\min_H \Gamma = \{x, y\} = \{(x_1, x_2, 0), (y_1, y_2, y_3)\}$ with $x_2 > 0$. Observe that $y_3 \geq 2$ by Lemma 5.6.6. Suppose, for the sake of contradiction, that $x_1 = y_1$. Taking into account Lemmas 5.6.4 and 5.6.5, it is clear that $x_2 \geq y_2 + 2$ and $x_1 < |P_1|$. In this case, both $y + (1, 0, -2)$ and $y + (-1, 2, 0)$ are in $\mathbf{P} \setminus \Gamma$, a contradiction. Hence $x_1 > y_1$. As a consequence of Theorem 5.5.2, $x_2 = |P_2|$ and so $x_2 > y_2$ by Lemma 5.6.3. Note that $y_1 > 0$ by Lemma 5.6.9. Since $y + (1, 0, -2) \in \mathbf{P} \setminus \Gamma$, $w_1 < 2w_3$. If $|x| < |y| - 1$, then $x + (-1, 0, 2) \in \mathbf{P} \setminus \Gamma$ and so $w_1 > 2w_3$, a contradiction. Hence $|x| = |y| - 1$. If $y_3 < |P_3|$ then $y + (-1, 1, 1) \in \mathbf{P} \setminus \Gamma$ and so $w_1 > w_2 + w_3$, a contradiction implying $y_3 = |P_3|$. Observe that $x_2 = y_2 + 1$, because if $x_2 > y_2 + 1$ then $y + (-1, 2, 0) \in \mathbf{P} \setminus \Gamma$ and hence $w_1 > 2w_2$, a contradiction. Therefore, Γ is in $\mathbf{T}_3$.

This concludes the proof because, by Theorem 5.5.2, all possible tripartite hierarchical ideal access structures have been analyzed. □

Lemma 5.6.11. *Let* Γ *be an ideal weighted threshold access structure that is strictly* m*-partite and indecomposable. If* $r = 2$*, then* $|x^1([1, m_1])| > |x^2([1, m_1])| + 1$.

Proof. From Theorem 5.5.2, $x^1([1, m_1]) > x^2([1, m_1])$, and if $|x^1([1, m_1])| = |x^2([1, m_1])| + 1$, then there exists $1 \leq i \leq m_1$ for which $x^1([1, m_1]) = x^2([1, m_1]) + \mathbf{e}^i$, which contradicts Lemma 5.6.4. □

Proposition 5.6.12. *If an ideal weighted threshold access structure is strictly* m*-partite with* $m > 3$*, then it is decomposable.*

Proof. Let Γ be an ideal weighted threshold access structure that is strictly m-partite with $m > 3$. By Proposition 5.6.8, it has exactly two H-minimal points, that we call x and y, with $s(x) < s(y)$. Define $i = s(x)$ and observe that $s(y) = m$.

Suppose that $m - i = 1$ and $x_1 = y_1$. Since $i \geq 3$, by Lemmas 5.6.2, 5.6.3, and 5.6.5 we obtain that $x_j > 0$ and $y_j < |P_j|$ for all $j = 1, 2, 3$. Thus both $x + \mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^3$ and $y - \mathbf{e}^1 + \mathbf{e}^2 + \mathbf{e}^3$ are in $\mathbf{P} \setminus \Gamma$, a contradiction. Now suppose that $m - i = 1$ and $x_1 > y_1$. By Theorem 5.5.2, $x_j = |P_j|$ for all $j = 2, \ldots, i$, and by Lemma 5.6.3, $y_2 < |P_2|$ and $y_3 < |P_3|$. As a consequence of Lemma 5.6.9 we obtain that $y_1 > 0$, and by following an analogous reasoning, we obtain that $y_2 > 0$. Hence both $y - \mathbf{e}^1 + \mathbf{e}^2 + \mathbf{e}^3$ and $y + \mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^m$ are in $\mathbf{P} \setminus \Gamma$, which implies that $w_3 < w_m$, a contradiction. Therefore $m - i > 1$.

Now suppose that $m - i \geq 2$ and $i > 1$. By Lemmas 5.6.3 and 5.6.5, $y_2 < |P_2|$ and $1 < y_m < |P_m|$. Suppose that $x_1 = y_1$. It is clear that $y_1 > 0$ by Lemma 5.6.2, so taking into account Lemmas 5.6.11 and 5.6.5 we obtain that both $y + \mathbf{e}^1 - 2\mathbf{e}^m$ and $y - \mathbf{e}^1 + \mathbf{e}^2 + \mathbf{e}^m$ are in $\mathbf{P} \setminus \Gamma$, a contradiction. Now suppose that $x_1 > y_1$. In this case, $y_1 > 0$ by Lemma 5.6.9, and $x_j = |P_j|$ for all $j = 2, \ldots, i$ by Theorem 5.5.2. As a consequence of Lemma 5.6.11, both $y + \mathbf{e}^1 - \mathbf{e}^{m-1} - \mathbf{e}^m$ and $y - \mathbf{e}^1 + \mathbf{e}^{m-1} + \mathbf{e}^m$ are in $\mathbf{P} \setminus \Gamma$, a contradiction.

Finally, suppose that $i = 1$. By Lemmas 5.6.2, 5.6.3, and 5.6.4 we obtain that $x_1 - y_1 \geq 2$, $y_{m-j} > 0$ for $j = 0, 1, 2$, and $y_{m-j} < |P_{m-j}|$ for $j = 0, 1$. Both $y + \mathbf{e}^1 - \mathbf{e}^{m-1} - \mathbf{e}^m$ and $y - \mathbf{e}^{m-2} + \mathbf{e}^{m-1} + \mathbf{e}^m$ are in $\mathbf{P} \setminus \Gamma$, a contradiction. □

Chapter 6

Optimization of Bipartite Secret Sharing Schemes

6.1 Introduction

The previous chapters are dedicated to the study of ideal multipartite access structures, and this chapter is dedicated to the optimization of secret sharing schemes for non-ideal bipartite access structures. We study the parameters κ, σ, and λ for this family of access structures, we present a new family of optimal bipartite secret sharing schemes, and a method to compute κ for bipartite access structures, and for multipartite access structures in general.

Determining the optimal complexity for general access structures has appeared to be an extremely difficult open problem. The asymptotic behavior of this parameter is unknown and there is a huge gap between the best known general lower [35] and upper [12] bounds. Due to its difficulty, this open problem has been studied for several particular families of access structures. For instance, it has been almost solved for access structures on at most five participants [60, 98]. The access structures that can be represented by graphs, that is, those whose minimal qualified subsets have two participants, have received a lot of attention in [16, 36] and other works. In particular, the optimal complexities of almost all structures defined by graphs with order six have been found [104], and the problem has been solved recently for the ones defined by trees [100]. The access structures with at most four minimal qualified subsets have been considered in [66, 70].

For multipartite access structures, the only results on the optimization of secret sharing are for bipartite access structures and weighted threshold access structures. Padró and Sáez [85] studied the bipartite access structures, characterized the ideal ones, and gave bounds on the optimal complexity of those that are not ideal. The asymptotic behavior of the optimal complexity of weighted threshold access structures have been studied by Beimel and Weinreb [8].

Constructions of secret sharing schemes for a given access structure Γ provide upper bounds on $\sigma(\Gamma)$. Several methods to construct secret sharing schemes with low complexity have been presented in [18,21,60,99,105] and other works. In most cases, these constructions provide linear schemes, and hence, upper bounds on $\lambda(\Gamma)$. On the other hand, lower bounds

on the optimal complexity have been obtained in [16, 17, 23, 60] by deriving inequalities on the Shannon entropies of the random variables involved in a secret sharing scheme.

Csirmaz [35] pointed out that those lower bounds on the optimal complexity can be derived from the fact that every secret sharing scheme for a given access structure defines a polymatroid. The parameter $\kappa(\Gamma)$ was introduced in [68] to denote the best lower bound on $\sigma(\Gamma)$ that can be obtained by this combinatorial method.

Therefore, most of the known lower and upper bounds on $\sigma(\Gamma)$ are, respectively, lower bounds on $\kappa(\Gamma)$ and upper bounds on $\lambda(\Gamma)$. Even though our knowledge on the behavior of the parameters κ and λ can still be improved, it is clear that new techniques are needed in the research on the open problem that is considered here. For instance, Csirmaz proved that $\kappa(\Gamma) \leq n$ for every access structure Γ on n participants, while $\lambda(\Gamma)$ grows much faster [2, 7, 48]. In addition, by using non-Shannon information inequalities [110], a separation result between the parameters κ and σ was presented in [4]. The power of these inequalities is studied in [5]. A slightly larger gap was proved in [75]. A stronger separation result between the parameters σ and λ was given in [7]. Csirmaz [35] proved that for any set of n participants there exists an access structure whose optimal complexity is at least about $n/\log n$.

In this chapter we present new results on the parameters κ, λ and σ for bipartite access structures that improve our knowledge on them. We show new bounds on the optimal complexity by using polymatroids, we determine the value of this parameter for some non-ideal bipartite access structures, and we present some results on the polymatroids related to bipartite access structures.

In Section 6.5 we present a method to find the value of κ for bipartite access structures. This method is based on the fact that the verification of Shannon-type inequalities can be formulated as a linear programming problem [108]. A general lower bound on κ for bipartite access structures is presented in Section 6.4. This lower bound is derived from the independent sequence method and improves the existing bounds for these access structures [85]. In addition, we present new optimal linear constructions for non-ideal bipartite access structures. Some of these access structures were previously considered by Mecalf-Burton [76]. By taking into account the bounds obtained on κ, we show that for these access structures, σ, λ and κ coincide.

The polymatroids related to bipartite access structures are studied in Section 6.6. In particular, we show that there exist bipartite polymatroids that are non-entropic, and linearly representable bipartite polymatroids that are not a sum of matroids.

6.2 Multipartite Polymatroids

In this section we study the parameter κ for multipartite access structures and we show that it can be determined by considering only a special class of polymatroids that is introduced here, the so-called *multipartite polymatroids*.

Let $\Pi = (Q_1, \ldots, Q_m)$ be a partition of Q. A permutation τ on Q is said to be a Π-*permutation* if $\tau(Q_i) = Q_i$ for every $i = 1, \ldots, m$. Taking into account the definition of multipartite matroids given in Chapter 3 it is clear a matroid $\mathcal{M} = (Q, r)$ is Π-partite if for every $r(A) = r(\sigma(B))$ for every Π-*permutation* τ. Analogously, a polymatroid $\mathcal{S} = (Q, h)$

with ground set Q is Π-*partite* if $h(A) = h(\tau(A))$ for every $A \subseteq Q$ and for every Π-permutation τ on Q.

This geometric representation can be also applied to multipartite polymatroids. If $\mathcal{S} = (X, h)$ is a Π-partite polymatroid, then $h(A) = h(B)$ if $\Pi(A) = \Pi(B)$. Therefore, the polymatroid $\mathcal{S}$ is univocally determined by the mapping $\widehat{h}\colon \mathbf{X} \to \mathbb{R}$ defined by $\widehat{h}(\mathbf{x}) = h(A)$, where $A \subseteq X$ is such that $\Pi(A) = \mathbf{x}$.

For every m-partition $\Pi = (P_1, \ldots, P_m)$ of P, we consider the $(m+1)$-partition $\Pi_0 = (P_1, \ldots, P_m, \{p_0\})$ of $Q = P \cup \{p_0\}$. We prove in the following that, for every Π-partite access structure $\Gamma \subseteq \mathcal{P}(P)$, the value of $\kappa(\Gamma)$ can be determined by considering only the Γ-polymatroids that are Π_0-partite.

Proposition 6.2.1. *Let $\Pi = (X_1, \ldots, X_m)$ be an m-partition of a set P and let Π_0 be the corresponding $(m+1)$-partition of $Q = P \cup \{p_0\}$. Let Γ be a Π-partite access structure on P. Then*

- $\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \mathcal{S}$ *is a* Π_0*-partite* Γ*-polymatroid*$\}$.
- $\lambda(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \mathcal{S}$ *is a linearly entropic* Π_0*-partite* Γ*-polymatroid*$\}$.

Proof. Let Ψ be the set of the Π_0-permutations on Q. Let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid, and consider the mapping $\widetilde{h}\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by

$$\widetilde{h}(X) = \frac{1}{|\Psi|} \sum_{\tau \in \Psi} h(\tau(X))$$

for every $X \subseteq Q$. It is not difficult to check that $\widetilde{\mathcal{S}} = (Q, \widetilde{h})$ is a Π_0-partite Γ-polymatroid with $\sigma(\widetilde{\mathcal{S}}) \leq \sigma(\mathcal{S})$. Suppose now that $\mathcal{S}$ is $\mathbb{K}$-linearly entropic for some finite field $\mathbb{K}$. Then there exists a real number $b > 0$ such that $\mathcal{S}' = (Q, bh)$ is a $\mathbb{K}$-representable integer polymatroid. For a permutation τ on Q, consider the integer polymatroid $\tau\mathcal{S}' = (Q, b(h\tau))$, where $(h\tau)(X) = h(\tau(X))$ for every $X \subseteq Q$. Clearly, $\tau\mathcal{S}'$ is $\mathbb{K}$-representable. Then the integer polymatroid $\widetilde{\mathcal{S}}' = \sum_{\tau \in \Psi} \tau\mathcal{S}'$ is $\mathbb{K}$-representable by Proposition 4.2.3, and hence $\widetilde{\mathcal{S}} = 1/(b|\Psi|)\widetilde{\mathcal{S}}'$ is linearly entropic. □

Corollary 6.2.2. *If Γ is a Π-partite access structure, then*

$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Pi\text{-partite polymatroid compatible with } \Gamma\}.$$

For every bipartite access structure, the points in $\Pi(\min\Gamma) = \{(x_1, y_1), \ldots, (x_r, y_r)\}$ can be ordered in such a way that $0 \leq x_1 < x_2 < \cdots < x_r$ and, in this situation, $y_1 > y_2 > \cdots > y_r \geq 0$. We are going to assume always that the points in $\min\Pi(\Gamma)$ are ordered in this way.

Consider the tripartition $\Pi_0 = (X, Y, \{p_0\})$ of the set $Q = P \cup \{p_0\}$. As before, for every $A \subseteq Q$, we consider $\Pi_0(A) = (|A \cap X|, |A \cap Y|, |A \cap \{p_0\}|) \in \mathbf{P} \times \{0, 1\} \subseteq \mathbb{Z}_+^3$. If $\mathcal{S} = (Q, h)$ is a Π_0-partite polymatroid, then $h(A) = h(B)$ if $\Pi_0(A) = \Pi_0(B)$. Therefore, the polymatroid $\mathcal{S}$ is univocally determined by the map $\widehat{h}\colon \mathbf{P} \times \{0, 1\} \to \mathbb{R}$ defined by $\widehat{h}(x, y, z) = h(A)$, where $A \subseteq Q$ is such that $\Pi(A) = (x, y, z)$.

6.3 Duality and Minors

If Γ is Π-partite for some partition $\Pi = (P_1, \ldots, P_m)$ of the set P, then the dual access structure Γ^* is Π-partite as well. If $B \subseteq P$, the minors $\Gamma\backslash B$ and Γ/B are $(\Pi\backslash B)$-partite access structures, where $\Pi\backslash B = (P_1 \smallsetminus B, \ldots, P_m \smallsetminus B)$.

The next proposition, whose proof is straightforward, describes a useful connection between these operations on access structures.

Proposition 6.3.1. *Let Γ be and access structure on a set P. Then $(\Gamma/B)^* = \Gamma^* \setminus B$ for every subset $B \subseteq P$.*

For a polymatroid $\mathcal{S} = (Q, h)$ and a subset $B \subseteq Q$, we consider the polymatroids $\mathcal{S}\setminus B = (Q \smallsetminus B, h_{\setminus B})$ and $\mathcal{S}/B = (Q \smallsetminus B, h_{/B})$ with $h_{\setminus B}(X) = h(X)$ and $h_{/B}(X) = h(X \cup B) - h(B)$ for every $X \subseteq Q \smallsetminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by a sequence of such operations is a *minor* of $\mathcal{S}$. If $\mathcal{S}$ is a Γ-polymatroid, then $\mathcal{S} \setminus B$ is a $(\Gamma \setminus B)$-polymatroid and $\mathcal{S}/B$ is a (Γ/B)-polymatroid. Because of that, $\kappa(\Gamma') \leq \kappa(\Gamma)$ if Γ' is a minor of Γ. In addition, the aforementioned connection between minors and secret sharing implies that $\sigma(\Gamma') \leq \sigma(\Gamma)$ and $\lambda(\Gamma') \leq \lambda(\Gamma)$. The parameters λ and κ are invariant by duality, as it was proved, respectively, in [59] and [68]. The relation between $\sigma(\Gamma)$ and $\sigma(\Gamma^*)$ is an open problem.

Proposition 6.3.2 ([59,68])**.** *For every access structure, $\lambda(\Gamma) = \lambda(\Gamma^*)$ and $\kappa(\Gamma) = \kappa(\Gamma^*)$.*

We prove in the next theorem that the value of $\kappa(\Gamma)$ for a multipartite access structure depends only on the minimal points, and it does not depend on the number of participants in every part.

Theorem 6.3.3. *Let Γ be a Π-partite access structure on P and let $B \subseteq P$ be such that the access structure $\Gamma\backslash B$ has the same minimal points as Γ, that is, $\Pi(\min\Gamma) = \Pi'(\min(\Gamma\backslash B))$, where $\Pi' = \Pi \setminus B$. Then $\kappa(\Gamma) = \kappa(\Gamma \setminus B)$.*

Proof. Clearly, $\kappa(\Gamma \setminus B) \leq \kappa(\Gamma)$. Take $\Pi = (P_1, \ldots, P_m)$ and consider the sets $Q = P \cup \{p_0\}$ and $Q' = (P \smallsetminus B) \cup \{p_0\} = Q \smallsetminus B$. We prove the other inequality by constructing, for every Π_0'-partite $(\Gamma \setminus B)$-polymatroid $\mathcal{S}' = (Q', h')$, a Π_0-partite Γ-polymatroid $\mathcal{S} = (Q, h)$ with $\sigma_{p_0}(\mathcal{S}) = \sigma_{p_0}(\mathcal{S}')$. Consider $\mathbf{Q}' = \Pi_0'(\mathcal{P}(Q')) \subseteq \mathbb{Z}_+^{m+1}$ and the mapping $\widehat{h'}\colon \mathbf{Q}' \to \mathbb{R}$ that determines the Π_0'-partite $(\Gamma \setminus B)$-polymatroid $\mathcal{S}' = (Q', h')$. For every vector $\mathbf{x} = (x_1, \ldots, x_m, x_{m+1}) \in \mathbf{Q} = \Pi_0(\mathcal{P}(Q))$, take

$$\mathbf{x}' = (\min\{x_1, |P_1 \smallsetminus B|\}, \ldots, \min\{x_m, |P_m \smallsetminus B|\}, x_{m+1}) \in \mathbf{Q}'$$

and consider the mapping $\widehat{h}\colon \mathbf{Q} \to \mathbb{R}$ defined by $\widehat{h}(\mathbf{x}) = \widehat{h'}(\mathbf{x}')$. It is not difficult to prove that this mapping defines a Π_0-partite Γ-polymatroid $\mathcal{S} = (Q, h)$ with $\sigma_{p_0}(\mathcal{S}) = \sigma_{p_0}(\mathcal{S}')$. □

As a consequence of Theorem 6.3.3, the value of $\kappa(\Gamma)$ for a bipartite access structure depends only on the family of minimal points, and it does not depend on the number of participants in every part. The next result proves that the value of $\kappa(\Gamma)$ for a bipartite access structure depends only on the relative position of its minimal points.

Theorem 6.3.4. *Let Γ be a Π-partite access structure on P and Δ the family of non-authorized subsets. Let $B \subseteq P$, $P' = P \diagdown B$, $\Pi' = \Pi \setminus B$, and Γ' an access structure on P' with family of non-authorized subsets Δ'. If $|\max \Pi(\Delta)| = |\max \Pi'(\Delta')|$ and*

$$\Gamma' = (\Gamma - \Pi(B)) \cap \mathbb{Z}_+^m$$

then $\kappa(\Gamma) = \kappa(\Gamma')$.

Proof. Let $\Gamma_2 = \Gamma^*$, Γ_3 be the restriction of Γ_2 to P', $\Gamma_4 = \Gamma_3*$, and Δ_2, Δ_3 and Δ_4 the respective families of non-authorized subsets. We claim that $\Gamma_4 = \Gamma'$. This is argued as follows. Observe that $\Delta_2 = \Pi(P) - \Gamma$, and that $\Delta_3 = (\Pi(P) - \Gamma) \cap \mathbf{P'}$. Hence

$$\Gamma_4 = \Pi(P') - (\Pi(P) - \Gamma) \cap \mathbf{P'}$$

. Since $x \in \mathbf{P'}$ if and only if $\Pi(P') - x \in \mathbf{P'}$, then $\Gamma_4 = (\Gamma - (\Pi(P) - \Pi(P'))) \cap \mathbf{P'}$, which proves the claim.

By properties in Section 2.5,

$$\kappa(\Gamma') = \kappa(\Gamma_3) \leq \kappa(\Gamma_2) = \kappa(\Gamma).$$

If $|\max \Delta| = |\max \Delta'|$, then $|\min \Gamma_2| = |\min \Gamma_3|$ because $\max \Delta = \Pi(P) - \min \Gamma_2$ and $\max \Delta' = \Pi(P') - \min \Gamma_3$. Note that in this case $\min \Gamma_2 = \min \Gamma_3$ and so $\kappa(\Gamma_3) = \kappa(\Gamma_2)$ by Theorem 6.3.3, which concludes the proof. □

For the case of bipartite access structures, this theorem admits a more simple presentation.

Corollary 6.3.5. *Let Γ be a bipartite access structure with $\min \Pi(\Gamma) = \{(x_1, y_1), \ldots, (x_r, y_r)\}$. Consider $\alpha = \min\{i : x_i > 0\}$ and $\beta = \max\{i : y_i > 0\}$. Observe that $\alpha \in \{1, 2\}$ and $\beta \in \{r - 1, r\}$. Let $B \subseteq P$ be such that $\Pi(B) = (x_\alpha - 1, y_\beta - 1)$. Then $\kappa(\Gamma/B) = \kappa(\Gamma)$.*

To determine whether the analogous result holds for the parameters κ and λ is an open problem. Nevertheless, as a consequence of the results in [41], in the conditions of Theorem 6.3.3, if $\Gamma \setminus B$ admits a vector space secret sharing scheme, then the same applies for Γ. As we have seen in the previous chapters, in the particular families of bipartite, tripartite and hierarchical access structures, the ideal access structures coincide with the vector space access structures. Therefore, for every access structure Γ in one of these families, $\Gamma \setminus B$ is ideal if and only if Γ is so.

6.4 The Optimal Complexity of Bipartite Access Structures

In this section we present bounds on the optimal complexity of bipartite access structures, and we present an optimal construction for some non-ideal bipartite access structures.

Csirmaz [35] found the following general upper bound on the complexity of any secret sharing schemes.

Theorem 6.4.1. *If Γ is an access structure on a set of n participants, then $\kappa(\Gamma) \leq n$.*

Differently to the general case, the asymptotic behavior of the parameter σ is known for bipartite access structures. Actually, if Γ is $\Pi = (P_1, P_2)$-partite, then $\lambda(\Gamma) \leq \min\{|P_1|, |P_2|\}$. This is due to the fact that the bipartite access structures with one minimal point admit a vector space secret sharing scheme and $\Pi(\min\Gamma)$ consists of at most $\min\{|P_1|, |P_2|\}$ points. It can be proved by using well known basic decomposition techniques (see [98], for instance) that Γ admits a linear secret sharing scheme Σ with $\sigma(\Sigma) = |\Pi(\min\Gamma)|$.

Ideal bipartite access structures were characterized by Padró and Sáez [85] (See Chapter 3), and proved that all ideal bipartite access structures are vector space.

In order to find bounds on κ, we use the *independent sequence method*, that was introduced in [16] and subsequently improved in [85]. We use the description of this method in terms of polymatroids that was presented in [68].

Consider $A \subseteq P$ and an increasing sequence of subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$. We say that $(B_1, \ldots, B_m \mid A)$ is an *independent sequence* in Γ with *length* m and *size* s if $|A| = s$ and, for every $i = 1, \ldots, m$ there exists $X_i \subseteq A$ such that $B_i \cup X_i \in \Gamma$, while $B_m \notin \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$ if $i \geq 2$. The independent sequence method is based on the following result.

Theorem 6.4.2. *Let Γ be an access structure on the set P and let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid on $Q = P \cup \{p_0\}$. If there exists in Γ an independent sequence $(B_1, \ldots, B_m \mid A)$ with length m and size s, then $h(A) \geq m$. As a consequence, $\kappa(\Gamma) \geq m/s$.*

We present next a new lower bound on κ for bipartite access structures. Our result generalize and improve the bound presented in [85, Proposition 4.1]. First, we present two lemmas that are needed in the proof of the result. The first one deals with independent sequences in bipartite access structures.

Lemma 6.4.3. *Let Γ be a bipartite access structure on a set P. Suppose that there exist a vector $(u, v) \in \mathbb{Z}_+^2$ and a monotone increasing sequence $(a_1, b_1) \leq \cdots \leq (a_m, b_m)$ of vectors in $\mathbf{P}$ such that, for every $i = 1, \ldots, m$, there exists a vector $(u_i, v_i) \leq (u, v)$ with $(a_i + u_i, b_i + v_i) \in \Pi(\Gamma)$ while $(a_m, b_m) \notin \Pi(\Gamma)$ and $(a_{i-1} + u_i, b_{i-1} + v_i) \notin \Pi(\Gamma)$ if $i \geq 2$. Then Γ admits an independent sequence $(B_1, \ldots, B_m | A)$ with length m and size $u + v$ such that $\Pi(A) = (u, v)$.*

Proof. Take subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$ and $A \subseteq P$ such that $\Pi(A) = (u, v)$, and $\Pi(B_i) = (a_i, b_i)$. In addition, for every $i = 1, \ldots, m$, consider a subset $X_i \subseteq A$ with $\Pi(X_i) = (u_i, v_i)$ and $X_i \cap B_i = \emptyset$. □

For a polymatroid $\mathcal{S} = (Q, h)$ and subsets $X, Y, Z \subseteq Q$, we notate

- $h(X \mid Y) = h(X \cup Y) - h(Y) \geq 0$,
- $i(X; Y) = h(X) - h(X \mid Y) = h(X) + h(Y) - h(X \cup Y) \geq 0$, and
- $i(X; Y \mid Z) = h(X \mid Z) - h(X \mid Y \cup Z) \geq 0$.

Lemma 6.4.4 ([59])**.** *Let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid and X, Y, Z subsets of $P = Q \setminus \{p_0\}$. If $X \cup Z$ and $Y \cup Z$ are in Γ but Z is not in Γ, then $i(X; Y | Z) \geq 1$.*

Theorem 6.4.5. *Let Γ be a bipartite access structure whose minimal points $\{(x_1, y_1), \ldots, (x_r, y_r)\}$ satisfy $x_1 = 1$ and $y_r = 0$. Consider $k = \max_{i=1,\ldots,r-1}(x_{i+1} - x_i)$ and take $s = x_r$ and $t = y_1$. Then*

$$\kappa(\Gamma) \geq \frac{k+s-2}{k+t-1}.$$

Proof. Consider the vectors $(u, v) = (k-1, t)$ and $(a_i, b_i) = (i-1, 0)$ for $i = 1, \ldots, s$. For every $i = 1, \ldots, s$, we define $\gamma(i)$ as the smallest integer for which $x_{\gamma(i)} \geq a_i$. Then for each $i = 1, \ldots, s$, consider the vector $(u_i, v_i) = (x_{\gamma(i)} - a_i, y_{\gamma(i)}) \leq (u, v)$. From Lemma 6.4.3, there is in Γ an independent sequence $(B_1, \ldots, B_m|A)$ with length s such that $\Pi(A) = (k-1, t)$. Then $h(A) \geq s$ by Theorem 6.4.2. Consider $A \cap P_1 = \{p_1, \ldots, p_{k-1}\}$ and $A \cap P_2 = \{q_1, \ldots, q_t\}$. Since $(1, t) \in \min \Pi(\Gamma)$, by Lemma 6.4.4 we obtain that

$$\begin{aligned}
h(A) &= h(q_1) + \sum_{i=2}^{t} h(q_i \mid q_{i-1} \ldots q_1) + h(p_1 \mid q_{s+1} \ldots q_1) + \sum_{i=2}^{k-1} h(p_i \mid p_{i-1} \ldots p_1 q_{s+1} \ldots q_1) \\
&\leq \sum_{i=1}^{t} h(q_i) + h(p_1) + \sum_{i=2}^{k-1} h(p_i \mid p_1 q_{s+1} \ldots q_1) \\
&= \sum_{i=1}^{t} h(q_i) + h(p_1) + \sum_{i=2}^{k-1} (h(p_i \mid q_{s+1} \ldots q_1) - i(p_i; p_1 \mid q_{s+1} \ldots q_1)) \\
&\leq \sum_{i=1}^{t} h(q_i) + h(p_1) + \sum_{i=2}^{k-1} h(p_i \mid q_{s+1} \ldots q_1) - (k-2) \\
&\leq \sum_{i=1}^{t} h(q_i) + \sum_{i=1}^{k-1} h(p_i) - (k-2).
\end{aligned}$$

Hence, taking into account the previous inequality it follows that $\sum_{p \in A} h(p) \geq k + s - 2$. Therefore, there is some $p \in A$ that satisfies $h(p) \geq (k+s-2)/(k+t-1)$. □

Theorem 6.4.5 can be used to find lower bounds on $\kappa(\Gamma)$ for every bipartite access structure Γ, because $\kappa(\Gamma) \geq \kappa(\Gamma')$ for every minor Γ' of Γ whose minimal points are in the conditions of Theorem 6.4.5. In addition, other lower bounds can be obtained from that result by changing the order of the parts in the bipartition of the set of participants. We apply next Theorem 6.4.5 to find a lower bound for the particular case of bipartite access structures having exactly two minimal points.

Corollary 6.4.6. *Let $\{(x_1, y_1), (x_2, y_2)\}$ be the set of minimal points of a bipartite access structure Γ. If $x_1 = y_2 = 0$, then Γ is ideal. If $x_1 > 0$, then*

$$\kappa(\Gamma) \geq 2 - \frac{1}{x_2 - x_1}.$$

Proof. Suppose that $x_1 > 0$ and consider $B \subseteq P$ with $\Pi(B) = (x_1 - 1, y_1 - 1)$. The minimal points of the minor Γ/B are $\{(1, 1), (x_2 - x_1 + 1, 0)\}$. By Theorem 6.4.5,

$$\kappa(\Gamma/B) \geq \frac{2(x_2 - x_1) - 1}{x_2 - x_1}.$$

□

The exact values of the optimal complexities of the bipartite access structures with minimal points $\min\Pi(\Gamma) = \{(1,1),(x_2,0)\}$ such that $|X| = x_2$ and $|Y| = 1$ were given in [76]. Specifically, for those access structures,

$$\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 2 - \frac{1}{x_2 - 1}.$$

Next theorem generalizes this result. Observe that the number of participants in each part can be arbitrarily large.

Theorem 6.4.7. *Let Γ be a bipartite access structure whose set of minimal points is $\{(x_1,y_1),(x_2,0)\}$, where $x_1 > 0$. Then*

$$\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 2 - \frac{1}{x_2 - x_1}.$$

Proof. By Corollary 6.4.6, $\kappa(\Gamma) \geq 2 - 1/(x_2 - x_1)$. The proof is concluded by constructing a linear secret sharing scheme Σ for Γ whose complexity is equal to this lower bound on $\kappa(\Gamma)$, because then $\lambda(\Gamma) \leq 2 - 1/(x_2 - x_1) \leq \kappa(\Gamma)$.

Set $N_1 = |X|$ and $N_2 = |Y|$ and consider a finite field $\mathbb{K}$ with $|\mathbb{K}| > \max\{N_1 + x_2 - x_1, N_2\}$. The scheme Σ is constructed by combining two $\mathbb{K}$-linear secret sharing schemes with access structure Γ.

In the first scheme, the secret value $k \in \mathbb{K}$ is distributed into shares among the participants in X by using Shamir's (x_2, N_1)-threshold scheme. In addition, Shamir's (x_1, N_1)-threshold scheme is used to distribute a random value $k_1 \in \mathbb{K}$ into shares among the participants in X, and the value $k_2 = k - k_1$ is distributed into shares among the participants in Y by Shamir's (y_1, N_2)-threshold scheme. We obtain in this way a $\mathbb{K}$-linear secret sharing scheme Σ_1 for Γ such that the secret value and the shares of the participants in Y are elements in $\mathbb{K}$, while the shares of the participants in X are in $\mathbb{K}^2$.

The second linear secret sharing scheme Σ_2 for Γ is described in the following. Consider a set Z of virtual participants with $|Z| = x_2 - x_1$. The secret value $k \in \mathbb{K}$ is distributed into shares among the participants in $X \cup Z$ by using Shamir's $(x_2, N_1 + x_2 - x_1)$-threshold scheme, and the share $s_i \in \mathbb{K}$ of every virtual participant $i \in Z$ is distributed among the participants in Y by using Shamir's (y_1, N_2)-threshold scheme. Clearly, Σ_2 is a $\mathbb{K}$-linear secret sharing scheme for Γ in which the secret value and the shares of the participants in X are taken from the finite field $\mathbb{K}$ while the participants in Y receive a share in $\mathbb{K}^{x_2 - x_1}$.

Finally, a $\mathbb{K}$-linear secret sharing scheme Σ is constructed by combining the scheme Σ_2 with $x_2 - x_1 - 1$ copies of the scheme Σ_1. Specifically, the secret value in the scheme Σ is a vector $(k_1, k_2, \ldots, k_{x_2 - x_1}) \in \mathbb{K}^{x_2 - x_1}$. Every one of the values $k_1, k_2, \ldots, k_{x_2 - x_1 - 1}$ is distributed by using the scheme Σ_1, while the value $k_{x_2 - x_1}$ is distributed by using the scheme Σ_2. Observe that the share of a participant in X is formed by $2(x_2 - x_1 - 1) + 1 = 2(x_2 - x_1) - 1$ elements in $\mathbb{K}$, while the share of a participant in Y is formed by $(x_2 - x_1 - 1) + (x_2 - x_1) = 2(x_2 - x_1) - 1$ elements in $\mathbb{K}$. Therefore, $\sigma(\Sigma) = (2(x_2 - x_1) - 1)/(x_2 - x_1)$. □

6.5 A Linear Programming Approach

To find the value of $\kappa(\Gamma)$ for a given access structure Γ can be formulated as a linear programming problem [37, 87]. Observe that, by ordering in some way the elements in

$\mathcal{P}(Q)$, a polymatroid $\mathcal{S} = (Q, h)$ can be represented as a vector $(h(A))_{A\subseteq Q} \in \mathbb{R}^k$, where $k = |\mathcal{P}(Q)| = 2^{n+1}$. By considering an additional variable v, the value of $\kappa(\Gamma)$ can be computed by solving the optimization problem

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & (h(A))_{A\subseteq Q} \text{ is a } \Gamma\text{-polymatroid and} \\ & v \geq h(\{i\}) \text{ for every } i \in Q. \end{array}$$

Clearly, the constraints on the vector $(v, (h(A))_{A\subseteq Q}) \in \mathbb{R}^{k+1}$ are given by linear inequalities, and hence this is actually a linear programming problem. In general, the number of variables and the number of constraints grow exponentially with the number of participants. In addition, as it was pointed out in [36, 37], the system of conditions is overdetermined, even after reducing it by using the characterization of polymatroids given by Matúš [73].

Nevertheless, if Γ is bipartite, the optimization problem to determine $\kappa(\Gamma)$ can be restricted to $(X, Y, \{p_0\})$-partite Γ-polymatroids by Proposition 6.2.1. Such a polymatroid $\mathcal{S} = (Q, h)$ is determined by its reduced rank function $\widehat{h}\colon \mathbf{P} \times \{0, 1\} \to \mathbb{R}$, where $\widehat{h}(x, y, z) = h(A)$ for every $A \subseteq Q$ with $\Pi(A) = (x, y, z)$. Therefore, the value of $\kappa(\Gamma)$ for a bipartite access structure Γ can be determined by solving the linear programming problem

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & (\widehat{h}(\mathbf{x}))_{\mathbf{x}\in\mathbf{P}\times\{0,1\}} \text{ determines a } \Pi_0\text{-partite } \Gamma\text{-polymatroid and} \\ & v \geq \widehat{h}(1, 0, 0) \text{ and } v \geq \widehat{h}(0, 1, 0). \end{array}$$

In this way, the number of variables has been reduced from $2^{N_1+N_2}+1$ to $2(N_1+1)(N_2+1)$ and the number of constraints grows also polynomially on the number of participants.

We describe in the following the set of constraints for this linear programming problem. By the characterization of polymatroids in [73], $h\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a Γ-polymatroid if and only if the following conditions are satisfied.

1. $h(\emptyset) = 0$.
2. $h(Q \smallsetminus \{p\}) \leq h(Q)$ for all $p \in Q$.
3. $h(X) + h(X \cup \{p, q\}) \leq h(X \cup \{p\}) + h(X \cup \{q\})$ for all $X \subseteq Q$ and $p, q \in Q \smallsetminus X$.
4. $h(X \cup \{p_0\}) = h(X)$ for every $X \in \min \Gamma$.
5. $h(X \cup \{p_0\}) = h(X) + 1$ for every maximal unqualified subset $X \subseteq P$.

Consider $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$, and $\mathbf{e}_3 = (0, 0, 1)$. Therefore, $\widehat{h}\colon \mathbf{P} \times \{0, 1\} \to \mathbb{R}$ is the reduced rank function of a Π_0-partite Γ-polymatroid if and only if the vector $(\widehat{h}(\mathbf{x}))_{\mathbf{x}\in\mathbf{P}\times\{0,1\}}$ satisfies the following linear constraints.

1. $\widehat{h}(0, 0, 0) = 0$.
2. $\widehat{h}((N_1, N_2, 1) - \mathbf{e}_i) \leq \widehat{h}(N_1, N_2, 1)$ for $i = 1, 2, 3$.

3. For every pair $(i,j) \in \{1,2,3\}^2$ with $i \leq j$, and for every $\mathbf{x} \in \mathbf{P} \times \{0,1\}$ such that $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j \in \mathbf{P} \times \{0,1\}$,

$$\widehat{h}(\mathbf{x}) + \widehat{h}(\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j) \leq \widehat{h}(\mathbf{x} + \mathbf{e}_i) + \widehat{h}(\mathbf{x} + \mathbf{e}_j).$$

4. $\widehat{h}(x,y,1) = \widehat{h}(x,y,0)$ for every $(x,y) \in \min \Pi(\Gamma)$.

5. $\widehat{h}(x,y,1) = \widehat{h}(x,y,0) + 1$ for every $(x,y) \in \max(\mathbf{P} \smallsetminus \Pi(\Gamma))$.

By using this linear programming approach, we have computed the value of $\kappa(\Gamma)$ for several bipartite access structures.

For instance, some bipartite access structures such that $\min \Pi(\Gamma) = \{(x_1,y_1),(x_2,y_2)\}$ with $x_1, y_2 > 0$ and $y_2 - y_1 \leq x_2 - x_1$ have been checked, and in all of them the lower bound in Corollary 6.4.6 is attained. Because of that, we conjecture that $\kappa(\Gamma) = 2 - 1/(x_2 - x_1)$ for every such access structure. Recall that this fact has been proved in Theorem 6.4.7 for the case $y_2 = 0$.

A gap in the values of the parameter κ was proved in [68]. Namely, there does not exist any access structure Γ with $1 < \kappa(\Gamma) < 3/2$. The existence of other gaps in the values of this parameter is thus a natural question. For instance, from the results in [36, 37, 100], one could conjecture that, if $\kappa(\Gamma) < 2$, then $\kappa(\Gamma) = 2 - 1/s$ for some positive integer s. Moreover, the values of $\kappa(\Gamma)$ for the bipartite access structures with two minimal points seem to confirm this conjecture.

There are also many cases of bipartite access structures with three minimal points for which $\kappa(\Gamma) = 2 - 1/s$. For instance, the access structure Γ with minimal points $\{(0,4),(1,3),(4,1)\}$ satisfies $\kappa(\Gamma) = 5/3$. Observe that it coincides with the value of $\kappa(\Gamma')$ of the access structure Γ' with minimal points $\{(1,2),(4,0)\}$, which is a minor of Γ.

Nevertheless, we have found some bipartite access structures whose complexity does not satisfy this property. Specifically, by solving the corresponding linear programming problem, we obtained that the bipartite access structure Γ with minimal points $\{(1,4),(3,3),(5,1)\}$ has $\kappa(\Gamma) = 22/13$. Another example is the structure with minimal points $\{(1,4),(4,3),(6,1)\}$, which satisfies $\kappa(\Gamma) = 99/53$. Moreover, we have found access structures for which κ is greater than 2. This is the case, for instance, of the access structures with minimal points $\{(1,4),(4,3),(8,1)\}$, $\{(1,4),(4,3),(9,1)\}$, and $\{(1,4),(6,3),(8,1)\}$, for which $\kappa(\Gamma)$ is, respectively, 23/11, 15/7, and 263/121.

Finally, the value of the parameter κ has been computed for a number of bipartite access structures whose families of minimal points are of the form

$$\{(x_i,y_i) = (1 + m(i-1), r - i) \,:\, i = 1, \ldots, r\}$$

for some integer $m \geq 2$. For all of them, $\kappa(\Gamma)$ equals the lower bound in Theorem 6.4.5.

6.6 Bipartite Polymatroids

In the previous sections, some ideas and techniques to study the optimization of secret sharing schemes with bipartite access structure have been presented. They improve the first results on this topic that were presented in [85].

Nevertheless, the problem is very far from being solved for this family. For instance, some fundamental questions about the construction of optimal linear secret sharing schemes for bipartite access structures remain open. Namely, it is not known if there exists some separation between the parameters κ and λ among the bipartite access structures. But even more basic questions have not been solved. For instance, it is not known wether the value of $\lambda(\Gamma)$ depends only on minimal points of Γ or it depends as well on the number of participants in each part.

Let Γ be a bipartite access structure such that there exists a $\mathbb{K}$-linear secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = \kappa(\Gamma)$. In this situation, $\kappa(\Gamma) = \lambda(\Gamma)$. Moreover, by using a similar argument as in the proof of Proposition 6.2.1, we can assume that $\mathcal{S}(\Sigma)$ is a Π_0-partite polymatroid. In particular $\mathcal{S}(\Sigma) \setminus \{p_0\}$ is a $\mathbb{K}$-linearly entropic bipartite polymatroid that is compatible with Γ.

Therefore, characterizing the linearly entropic bipartite polymatroids and, by extension, the representable integer bipartite polymatroids, are interesting open problems for the optimization of bipartite secret sharing schemes.

We prove in the following that the *uniform* integer polymatroids, which are precisely the m-partite integer polymatroids with $m = 1$, are representable. In addition, all m-partite matroids with $m \leq 3$ are representable [41]. Unfortunately, this does not apply to bipartite polymatroids. Actually, we present a bipartite integer polymatroid that is not entropic, and hence it is not representable.

A polymatroid $\mathcal{S} = (Q, h)$ is said to be *uniform* if the value of $h(X)$ depends only on the cardinality of X, that is, $h(X) = h(Y)$ if $|X| = |Y|$. A uniform polymatroid is determined by the values $h_0, h_1, \ldots, h_n$, where $n = |Q|$ and $h(X) = h_i$ if $|X| = i$. For $i = 1, \ldots, n$, consider the values $\delta_i = h_i - h_{i-1}$, which form the *increment vector* $(\delta_1, \ldots, \delta_n)$ of $\mathcal{S}$. A sequence $(h_i)_{0 \leq i \leq n}$ of real numbers determines a uniform polymatroid if and only if $h_0 = 0$ and $\delta_1 \geq \cdots \geq \delta_n \geq 0$. Obviously, a uniform polymatroid is determined by its increment vector, and it is an integer polymatroid if and only if its increment vector has integer components. If $\mathcal{S} = (Q, h)$ is a uniform matroid, then there exists an integer r with $0 \leq r \leq |Q|$ such that the increment vector of $\mathcal{S}$ satisfies $\delta_i = 1$ if $i \leq r$ and $\delta_i = 0$ otherwise. We notate $U_{r,n}$ for such a uniform matroid. It is well known that the uniform matroid $U_{r,n}$ is $\mathbb{K}$-representable for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n$.

Proposition 6.6.1. *Every uniform integer polymatroid is a sum of uniform matroids.*

Proof. Let $\mathcal{S} = (Q, h)$ be a uniform integer polymatroid, with increment vector $(\delta_1, \ldots, \delta_n)$. Then there exists a sequence of integers $n = r_0 \geq r_1 \geq \cdots \geq r_{\delta_1} \geq r_{\delta_1+1} = 0$ such that $r_{\delta_i} \geq i > r_{\delta_i+1}$ for every $i = 1, \ldots, n$. We claim that $\mathcal{S} = U_{r_1,n} + \cdots + U_{r_{\delta_1},n}$. We have to check that $\delta_i = \delta_i^1 + \cdots + \delta_i^{\delta_1}$ for every $i = 1, \ldots, n$, where δ^k is the increment vector of the uniform matroid $U_{r_k,n}$. Recall that $\delta_i^k = 1$ if $r_k \geq i$ and $\delta_i^k = 0$ otherwise. □

Theorem 6.6.2. *Every uniform integer polymatroid is representable, and hence entropic.*

Proof. Straightforward from Propositions 4.2.3 and 6.6.1 and the fact that the uniform matroid $U_{r,n}$ is representable over every finite field with at least n elements. □

Proposition 6.6.3. *There exist bipartite integer polymatroids that are not entropic.*

Proof. The Vamos matroid V is the matroid of dimension four on the set $\{1,\ldots,8\}$ with rank function r such that $r(A) = 4$ for every $A \subseteq \{1,\ldots,8\}$ of size 4 except $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{3,4,5,6\}$ $\{3,4,7,8\}$ and $\{5,6,7,8\}$. Take $a = \{1,2\}$, $b = \{3,4\}$, $c = \{5,6\}$, $d = \{7,8\}$, and the set $Q = \{a,b,c,d\}$. Let $\mathcal{S} = (Q,h)$ be the integer polymatroid whose rank function is derived from the rank function of V. It is not difficult to check that $\mathcal{S}$ is Π-partite with $\Pi = (\{a,b\},\{c,d\})$. Matúš [74] pointed out that the rank function of $\mathcal{S}$ violates the non-Shannon information inequality given by Zhang and Yeung [110]. This implies that $\mathcal{S}$ is not entropic. □

Nevertheless, Proposition 6.6.3 does not exclude the possibility that $\kappa(\Gamma) = \lambda(\Gamma)$ for every bipartite access structure. Separation results between these parameters could be obtained by adding Ingleton inequality [56], an information inequality that applies only to linear random variables, to the linear programming approach that was presented in Section 6.5. In this way, lower bounds on $\lambda(\Gamma)$ would be obtained and, maybe, a bipartite access structure with $\kappa(\Gamma) < \lambda(\Gamma)$ could be found. Similarly, the use of non-Shannon information inequalities, as for instance the one from [110], could provide some separation result between the parameters κ and σ for bipartite access structures.

As a consequence of the results in [41,85], the existence of a vector space secret sharing for a multipartite access structure Γ does not depend on the number of participants in every part, but only on the minimal points. The same applies to the parameter κ, as we proved in Proposition 6.3.3 for the bipartite case. The validity of a similar result for the parameters σ and λ is an open problem.

Actually, much more basic questions remain open about the optimization of bipartite secret sharing schemes. For instance, even though partial results have been presented in Corollary 6.4.6 and Theorem 6.4.7, the problem has not been solved for bipartite access structures with only two minimal points.

Bibliography

[1] A. Beimel and B. Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

[2] A. Beimel and Y. Ishai. On the power of nonlinear secret-sharing. *SIAM J. of Discrete Mathematics*, 19(1):258–280, 2005.

[3] A. Beimel and N. Livne. On matroids and nonideal secret sharing. *IEEE Transactions on Information Theory*, 54(6):2626–2643, 2008.

[4] A. Beimel, N. Livne, and C. Padró. Matroids can be far from ideal secret sharing. In *TCC*, volume 4948 of *Lecture Notes in Computer Science*, pages 194–212. Springer, 2008.

[5] A. Beimel and I. Orlov. Secret sharing and non-shannon information inequalities. In *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 539–557. Springer, 2009.

[6] A. Beimel, T. Tassa, and E. Weinreb. Characterizing ideal weighted threshold secret sharing. *SIAM J. Discrete Math.*, 22(1):360–397, 2008.

[7] A. Beimel and E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.*, 34(5):1196–1215, 2005.

[8] A. Beimel and E. Weinreb. Monotone circuits for monotone weighted threshold functions. *Information Processing Letters*, 97(1):12–18, 2006.

[9] M. Belenkiy. Disjunctive multi-level secret sharing. Cryptology ePrint Archive, Report 2008/018, 2008. `http://eprint.iacr.org/`.

[10] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC*, pages 1–10, Chicago, Illinois, USA, May 1988. ACM.

[11] J. C. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret sharing. In *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 1986.

[12] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988.

[13] A. Beutelspacher and F. Wettl. On 2-level secret sharing. *Des. Codes Cryptography*, 3(2):127–134, 1993.

[14] G. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, 48:313–317, 1979.

[15] C. Blundo, P. D'Arco, V. Daza, and C. Padró. Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures. In *ISC*, volume 2200 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2001.

[16] C. Blundo, A. D. Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes (extended abstract). In *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 148–167. Springer, 1992.

[17] C. Blundo, A. D. Santis, R. D. Simone, and U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptography*, 11(2):107–122, 1997.

[18] C. Blundo, A. D. Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology*, 8(1):39–64, 1995.

[19] E. F. Brickell. Some ideal secret sharing schemes. In *EUROCRYPT*, pages 468–475, 1989.

[20] E. F. Brickell and D. M. Davenport. On the classification of idea secret sharing schemes. In *CRYPTO*, pages 278–285, 1989.

[21] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology*, 5(3):153–166, 1992.

[22] C. Cachin. *Entropy Measures and Unconditional Security in Cryptography.* PhD thesis, Swiss Federal Institute of Technology, Zürich, 1997.

[23] R. M. Capocelli, A. D. Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6(3):157–167, 1993.

[24] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *STOC*, pages 11–19, Chicago, Illinois, USA, May 1988. ACM.

[25] H. Chen and R. Cramer. Algebraic geometric secret sharing schemes and secure multiparty computations over small fields. In *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 521–536. Springer, 2006.

[26] H. Chen, R. Cramer, R. de Haan, and I. C. Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. In *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 451–470. Springer, 2008.

[27] H. Chen, S. Ling, and C. Xing. Access structures of elliptic secret sharing schemes. *IEEE Transactions on Information Theory*, 54(2):850–852, 2008.

[28] M. J. Collins. A note on ideal tripartite access structures. Cryptology ePrint Archive, Report 2002/193, 2002. `http://eprint.iacr.org/`.

[29] T. M. Cover and J. A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[30] R. Cramer and I. Damgård. On the amortized complexity of zero-knowledge protocols. In *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 177–191. Springer, 2009.

[31] R. Cramer, I. Damgård, and U. M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT*, pages 316–334, 2000.

[32] R. Cramer, V. Daza, I. Gracia, J. J. Urroz, G. Leander, J. Martí-Farré, and C. Padró. On codes, matroids, and secure multiparty computation from linear secret-sharing schemes. *IEEE Transactions on Information Theory*, 54(6):2644–2657, 2008.

[33] R. Cramer and S. Fehr. Optimal black-box secret sharing over arbitrary abelian groups. In *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 272–287. Springer, 2002.

[34] R. Cramer, S. Fehr, and M. Stam. Black-box secret sharing from primitive sets in algebraic number fields. In *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 344–360. Springer, 2005.

[35] L. Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.

[36] L. Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptography*, 53(3):195–209, 2009.

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

[38] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer-Verlag, 1992.

[39] Y. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM Journal on Discrete Mathematics*, 7(4):667–679, 1994.

[40] J. Edmonds. Submodular functions, matroids, and certain polyhedra. In *Proc. Inf. Conf. on Combinatorics (Calgary)*, pages 69–87. Gordon and Breach (New York), 1970.

[41] O. Farràs, J. Martí-Farré, and C. Padró. Ideal multipartite secret sharing schemes. In *EUROCRYPT*, volume 4515 of *Lecture Notes in Computer Science*, pages 448–465. Springer, 2007.

[42] O. Farràs, J. R. Metcalf-Burton, C. Padró, and L. Vázquez. On the optimization of bipartite secret sharing schemes. In *ICITS*, 2009.

[43] O. Farràs and C. Padró. Families of multipartite secret sharing schemes. Manuscript, 2010.

[44] O. Farràs and C. Padró. Ideal hierarchical secret sharing schemes. In *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 219–236. Springer, 2010.

[45] S. Fehr. Efficient construction of the dual span program. Manuscript, 1999. Available at the author's webpage.

[46] S. Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39(1):55–72, 1978.

[47] S. Fujishige. Submodular functions and optimization. *Annals of Discrete Mathematics*, 47, 1991.

[48] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. In *STOC*, pages 429–437, 1998.

[49] M. Giuletti and R. Vincenti. Three-level secret sharing schemes. *Discrete Mathematics*, 2010. to appear.

[50] S. D. Gordon and J. Katz. Rational secret sharing, revisited. In *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 229–241. Springer, 2006.

[51] J. Y. Halpern and V. Teague. Rational secret sharing and multiparty computation: extended abstract. In *36th Annual ACM Symposium on Theory of Computing (STOC)*, pages 623–632, 2004.

[52] D. Hammer, A. E. Romashchenko, A. Shen, and N. K. Vereshchagin. Inequalities for shannon entropy and kolmogorov complexity. *J. Comput. Syst. Sci.*, 60(2):442–464, 2000.

[53] J. Herzog and T. Hibi. Discrete polymatroids. *J. Algebraic Comb.*, 16(3):239–268, 2002.

[54] J. Herzog, T. Hibi, and M. Vladoiu. Ideals of fiber typer and polymatroids. *Osaka J. Math.*, 42(4):807–829, 2005.

[55] M. Hirt and U. M. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract). In *PODC*, pages 25–34, 1997.

[56] A. W. Ingleton. Conditions for representability and transversability of matroids. In *Fr. Br. Conf. 1970*. Springer-Verlag, 1971.

[57] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structures. In *Proc. IEEE Globecom'87*, pages 99–102, 1987.

[58] W. Jackson, K. M. Martin, and C. M. O'Keefe. Ideal secret sharing schemes with multiple secrets. *J. of Cryptology*, 9(4):233–250, 1996.

[59] W.-A. Jackson and K. M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptography*, 4(1):83–95, 1994.

[60] W.-A. Jackson and K. M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptography*, 9(3):267–286, 1996.

[61] M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102—-111, 1993.

[62] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.

[63] S. C. Kothari. Generalized linear threshold scheme. In *CRYPTO*, pages 231–241, 1984.

[64] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii. Nonperfect secret sharing schemes and matroids. In *Advances in Cryptology – EUROCRYPT '93*, volume 765, pages 126–141. Springer-Verlag, 1994.

[65] A. Lehman. A solution of the shannon switching game. *J. Soc. Indust. Appl. Math.*, 12:687–725, 1964.

[66] J. Martí-Farré and C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes Cryptography*, 34(1):17–34, 2005.

[67] J. Martí-Farré and C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics*, 154(3):552–563, 2006.

[68] J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. In *TCC*, volume 4392 of *Lecture Notes in Computer Science*, pages 273–290. Springer, 2007.

[69] J. Martí-Farré and C. Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Des. Codes Cryptography*, 52(1):1–14, 2009.

[70] J. Martí-Farré, C. Padró, and L. Vázquez. Optimal complexity of secret sharing schemes optimal complexity of secret sharing schemes with four minimal qualified subsets. Manuscript, 2010.

[71] J. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory*, pages 269–279, 1993.

[72] J. Massey. Some applications of coding theory in cryptography. In *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

[73] F. Matús. Adhesivity of polymatroids. *Discrete Mathematics*, 307(21):2464–2477, 2007.

[74] F. Matúš. Two constructions on limits of entropy functions. *IEEE Trans. on Information Theory*, 53:320–330, 2007.

[75] J. R. Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the vamos matroid. *CoRR*, abs/0809.3010, 2008.

[76] J. R. Metcalf-Burton. Information rates of minimal non-matroid-related access structures. *CoRR*, abs/0801.3642, 2008.

[77] P. Morillo, C. Padró, G. Sáez, and J. L. Villar. Weighted threshold secret sharing schemes. *Inf. Process. Lett.*, 70(5):211–216, 1999.

[78] K. Murota. *Discrete Convex Analysis*. SIAM Monographs on Discrete Mathematics and Applications. SIAM, Philadelphia, USA, 2003.

[79] S.-L. Ng. A representation of a family of secret sharing matroids. *Des. Codes Cryptography*, 30(1):5–19, 2003.

[80] S.-L. Ng. Ideal secret sharing schemes with multipartite access structures. *IEE Proc.-Commun.*, 153:165–168, 2006.

[81] S.-L. Ng and M. Walker. On the composition of matroids and ideal secret sharing schemes. *Des. Codes Cryptography*, 24(1):49–67, 2001.

[82] J. G. Oxley. *Matroid theory*. The Clarendon Press Oxford University Press, New York, 1992.

[83] C. Padró and I. Gracia. Representing small identically self-dual matroids by self-dual codes. *SIAM J. Discrete Math.*, 20(4):1046–1055, 2006.

[84] C. Padró, I. Gracia, S. M. Molleví, and P. Morillo. Linear key predistribution schemes. *Des. Codes Cryptography*, 25(3):281–298, 2002.

[85] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 46(7):2596–2604, 2000.

[86] C. Padró and G. Sáez. Correction to "secret sharing schemes with bipartite access structure". *IEEE Trans. Inform. Theory*, 50:1373–1373, 2004.

[87] C. Padró and L. Vázquez. Finding lower bounds on the complexity of secret sharing schemes by linear programming. In *Ninth Latin American Theoretical Informatics Symposium, LATIN 2010.*, , Lecture Notes in Computer Science, 2010.

[88] I. C. Pueyo, H. Chen, R. Cramer, and C. Xing. Asymptotically good ideal linear secret sharing with strong multiplication over *any* fixed finite field. In *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 466–486. Springer, 2009.

[89] G. Sáez and J. Herranz. New results on multipartite access structures. *IEE Proceedings of Information Security*, 153:153–162, 20026.

[90] A. Schrijver. *Combinatorial Optimization. Polyhedra and Efficiency*. Springer-Verlag, Berlin, 2003.

[91] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[92] P. D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.*, 27:407–413, 1976.

[93] P. D. Seymour. On secret-sharing matroids. *J. Comb. Theory, Ser. B*, 56(1):69–73, 1992.

[94] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[95] V. Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.

[96] G. J. Simmons. How to (really) share a secret. In *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer, 1988.

[97] J. Simonis and A. E. Ashikhmin. Almost affine codes. *Des. Codes Cryptography*, 14(2):179–197, 1998.

[98] D. R. Stinson. New general lower bounds on the information rate of secret sharing schemes. In *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 168–182. Springer, 1992.

[99] D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.

[100] G. Tardos and L. Csirmaz. Secret sharing on trees: problem solved. *Cryptology ePrint Archive*, 2009.

[101] T. Tassa. Hierarchical threshold secret sharing. *J. Cryptology*, 20(2):237–264, 2007.

[102] T. Tassa and N. Dyn. Multipartite secret sharing by bivariate interpolation. *J. Cryptology*, 22(2):227–258, 2009.

[103] P. Vamos. On the representation of independence structures. (unpublished manuscript), 1968.

[104] M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptography*, 6:143–169, 1995.

[105] M. van Dijk, T. A. M. Kevenaar, G. J. Schrijen, and P. Tuyls. Improved constructions of secret sharing schemes by applying (lambda, omega)-decompositions. *Inf. Process. Lett.*, 99(4):154–157, 2006.

[106] D. J. A. Welsh. *Matroid theory*. Academic Press [Harcourt Brace Jovanovich Publishers], London, 1976.

[107] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.*, 57:509–533, 1935.

[108] R. W. Yeung. A framework for linear information inequalities. *IEEE Transactions on Information Theory*, 43(6):1924–1934, 1997.

[109] R. W. Yeung. *A First Course in Information Theory*. Kluwer, New York, 2002.

[110] Z. Zhang and R. W. Yeung. On characterization of entropy function via information inequalities. *IEEE Transactions on Information Theory*, 44(4):1440–1452, 1998.