J. Cryptol. (2012) 25: 434–463
DOI: 10.1007/s00145-011-9101-6

Journal of
CRYPTOLOGY

Ideal Multipartite Secret Sharing Schemes*

Oriol Farràs[†]
Dep. d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
oriol.farras@urv.cat

Jaume Martí-Farré
Dep. de Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, Barcelona, Catalonia, Spain
jaume.marti@ma4.upc.edu

Carles Padró[‡]
Division of Mathematical Sciences, Nanyang Technological University, Singapore, Singapore
cpadro@ma4.upc.edu, carlespl@ntu.edu.sg

Communicated by Stefan Wolf

Received 17 March 2010
Online publication 31 March 2011

Abstract. Multipartite secret sharing schemes are those having a multipartite access structure, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role. In this work, the characterization of ideal multipartite access structures is studied with all generality. Our results are based on the well-known connections between ideal secret sharing schemes and matroids and on the introduction of a new combinatorial tool in secret sharing, *integer polymatroids*.

Our results can be summarized as follows. First, we present a characterization of multipartite matroid ports in terms of integer polymatroids. As a consequence of this characterization, a necessary condition for a multipartite access structure to be ideal is obtained. Second, we use representations of integer polymatroids by collections of vector subspaces to characterize the representable multipartite matroids. In this way we obtain a sufficient condition for a multipartite access structure to be ideal, and also a

* A previous version of this paper appeared in *Advances in Cryptology*, *Eurocrypt 2007*, *Lecture Notes in Computer Science* **4515**, 448–465 (2007). Most of the research was done while the three authors were at UPC Barcelona. The authors' work was partially supported by the Spanish Ministry of Education and Science under projects TIC2003-00866 and TSI2006-02731.

[†] O. Farràs' research partially supported by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia through grant 2009 SGR 1135. The author is with the UNESCO Chair in Data Privacy, but the views expressed in this paper are his own and do not commit UNESCO.

[‡] C. Padró's research partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03. Part of the work was done while the author was in a sabbatical stay at CWI, Amsterdam. This stay was funded by the *Secretaría de Estado de Educación y Universidades* of the Spanish Ministry of Education.

unified framework to study the open problems about the efficiency of the constructions of ideal multipartite secret sharing schemes. Finally, we apply our general results to obtain a complete characterization of ideal tripartite access structures, which was until now an open problem.

Key words. Secret sharing, Ideal secret sharing schemes, Ideal access structures, Multipartite secret sharing, Multipartite matroids, Integer polymatroids.

1. Introduction

Secret sharing was introduced in 1979 by Shamir [38] and Blakley [5]. Since then many applications to several different kinds of cryptographic protocols have appeared. At the same time, research in some basic open problems in secret sharing has developed a rich mathematical theory with connections to combinatorics, information theory, coding theory, algebra and algebraic geometry.

In a *secret sharing scheme*, every *participant* receives a *share* of a *secret value*. Only the *qualified sets* of participants, which form the *access structure* of the scheme, can recover the secret value from their shares. This paper deals exclusively with *unconditionally secure perfect secret sharing schemes*, that is, the shares of the participants in an unqualified set do not provide any information about the secret value. The reader is referred to [41] for an introduction to secret sharing.

An *access structure* on a set P of *participants* is a *monotone increasing* family $\Gamma \subseteq \mathcal{P}(P)$, where $\mathcal{P}(P)$ is the power set of P. That is, every subset of P containing a subset in Γ is itself in Γ. The members of Γ are called the *qualified subsets* of the access structure.

The first proposed secret sharing schemes [5,38] have *threshold access structures*, in which the qualified subsets are those having at least a given number of participants. In addition, those schemes are *ideal*, that is, the share of every participant has the same length as the secret, which is the best possible situation in a perfect scheme [20]. While the construction by Shamir [38] is based on polynomial interpolation, the one by Blakley [5] uses finite geometries.

Secret sharing schemes for non-threshold access structures were first considered in the seminal paper by Shamir [38], where *weighted threshold secret sharing schemes* were introduced. In such a scheme, every participant has a weight (a positive integer) and the sets whose weight sum is greater than a given threshold are qualified. The construction proposed by Shamir is very simple: take a threshold scheme and give to every participant as many shares as its weight. Nevertheless, the obtained scheme is not ideal.

Ito, Saito, and Nishizeki [18] proved, in a constructive way, that there exists a secret sharing scheme for every access structure, but the schemes that are obtained by this method are very far from ideal. Actually, the length of the shares grows exponentially with the number of participants. Benaloh and Leichter [3] proved that there exist access structures that do not admit any ideal scheme and, as a consequence of the results in [9, 11] and other works, in some cases the shares must be much larger than 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.

Another important and longstanding open problem is the characterization of the *ideal access structures*, that is, the ones admitting an ideal secret sharing scheme. As a consequence of the results by Brickell [7] and by Brickell and Davenport [8], this open problem is strongly connected to matroid theory. Matroid ports, which were introduced in 1964 by Lehman [22] to solve the Shannon switching game, play a fundamental role. Basic definitions and facts about matroids and matroid ports and their connections to secret sharing are recalled in Sect. 4.

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 the applications of secret sharing. This line of research was initiated by Kothari [21], who posed the open problem of constructing ideal hierarchical secret sharing schemes, and by Simmons [39], who introduced the *multilevel* and *compartmented* access structures that are described in Sect. 8. Multilevel access structures are suitable for hierarchical organizations, while compartmented access structures can be used to initiate actions that require the agreement of different parties. By generalizing the geometric method by Blakley [5], Simmons [39] presented ideal secret sharing schemes for some particular examples of multilevel and compartmented access structures and provided ideas for more general constructions. By introducing a new method to construct ideal secret sharing schemes, which was partially anticipated by Kothari [21], Brickell [7] was able to find ideal schemes for all multilevel and compartmented access structures.

The multilevel and compartmented access structures introduced by Simmons [39] are *multipartite*, that is, the set of participants is divided into several parts and all participants in the same part play an equivalent role. Secret sharing schemes for multipartite access structures have received considerable attention. This is due to the fact that multipartite secret sharing can be seen as a natural and useful generalization of threshold secret sharing. While in threshold access structures all participants are equivalent, multipartite access structures can used in situations in which the participants are distributed into different classes, as for instance in hierarchical organizations. In addition, similarly to threshold access structures, multipartite access structures can be described in a compact way, by using a few conditions that are independent of the total number of participants.

On the basis of the well-known connection between ideal secret sharing schemes and matroids, the characterization of the ideal multipartite access structures is studied in this paper in all generality. Even though polymatroids have been used before in secret sharing [11,24], in this paper *integer polymatroids* are used for the first time in the characterization of ideal access structures. These combinatorial objects are proved to be a very useful tool to study multipartite matroids and, in particular, the matroids defined from ideal multipartite secret sharing schemes. Two general results are obtained by combining the connection between integer polymatroids and multipartite matroids that we present in this paper with the geometric representation of multipartite access structures that was introduced in [34] for the bipartite case. Namely, a necessary condition and a (different) sufficient condition for a multipartite access structure to be ideal.

As a consequence of our main general results, we obtain a complete characterization of the ideal tripartite access structures, which was until now an open problem. In addition, they are the main tool in the complete characterization of the ideal hierarchical access structures that has been presented in a recent paper [12]. Moreover, our results provide a unified framework, which encloses most of the constructions 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.

Therefore, this paper contains contributions to the two aforementioned lines of research: the characterization of the ideal access structures and the construction of ideal multipartite secret sharing schemes for interesting families of access structures.

2. Related Work

2.1. *On the Construction of Ideal Multipartite Secret Sharing Schemes*

The method to construct ideal secret sharing schemes proposed by Brickell [7] is a linear algebra reformulation of the geometric ideas by Blakley [5] and Simmons [39]. In addition, Brickell's construction can be seen also as a generalization of Shamir's threshold scheme [38], and hence it unifies the two seminal approaches to secret sharing. Some of the ideas by Brickell [7] were anticipated by Kothari [21]. We use in this paper the description of Brickell's method in terms of linear codes due to Massey [25,26]. Namely, every linear code C over a finite field $\mathbb{K}$ defines an ideal secret sharing scheme in which both the secret value and the shares are elements in $\mathbb{K}$. Every codeword of C corresponds to a possible distribution of shares. Such an ideal scheme is called a $\mathbb{K}$-*vector space secret sharing scheme* and its access structure is called a $\mathbb{K}$-*vector space access structure*. The vast majority of the constructions of ideal secret sharing schemes that are found in the literature fit into this general method. This applies in particular to all the constructions of ideal multipartite secret sharing schemes that are discussed next.

The search for ideal multipartite secret sharing schemes for interesting families of access structures, the line of research that was initiated by Kothari [21], Simmons [39], and Brickell [7], has been pursued by other authors. 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 [1,2,16,31,42,43]. All these constructions provide vector space secret sharing schemes, but some interesting new techniques are introduced in the ones by Tassa [42] and Tassa and Dyn [43]. Specifically, a random polynomial and some of its derivatives are evaluated in several points to obtain the shares in the scheme proposed in [42], and hence it is based on Birkhoff interpolation, while the constructions in [43] 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 aforementioned 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 [7] proposed a method to avoid these checkings, but it requires the base field of the scheme to be very large. Another strategy has been proposed in [42,43]. 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 [4,14], and it appears to be a very difficult open problem.

2.2. *On the Characterization of Ideal Access Structures*

The other line of research that is considered in this paper is the characterization of the ideal access structures. As we mentioned before, tight connections of this open problem to matroid theory were pointed out in the works by Brickell [7] and by Brickell and Davenport [8]. Associated to every linear code C, there exists a unique representable matroid $\mathcal{M}$. The access structure Γ of the ideal secret sharing scheme defined from the code C is determined by $\mathcal{M}$. Actually, Γ is a *port of the matroid* $\mathcal{M}$. Because of that, the vector space access structures coincide with the ports of representable matroids. Therefore, a sufficient condition for an access structure to be ideal is derived from the construction by Brickell [7]: every port of a representable matroid is an ideal access structure. As a consequence of the results by Brickell and Davenport [8], this sufficient condition is not very far from being necessary. They proved that every ideal secret sharing scheme determines a matroid such that the access structure is one of its ports. Therefore, being a matroid port is a necessary condition for an access structure to be ideal. These results are summarized in the following theorem.

Theorem 2.1 [7,8]. *The ports of representable matroids are ideal access structures. The access structure of every ideal secret sharing scheme is a matroid port.*

Seymour [36] presented in 1976 a forbidden minor characterization of matroid ports that has been used recently in [24] to obtain the following generalization of the result by Brickell and Davenport [8].

Theorem 2.2 [24]. *An access structure is a matroid port if it admits a secret sharing scheme in which the length of every share is less than* $3/2$ *times the length of the secret.*

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 precisely the ports of ss-representable matroids. Since there exist non-ss-representable matroids, the necessary condition in Theorem 2.1 is not sufficient. The first example, the Vamos matroid, was found by Seymour [37]. In addition, the sufficient condition in Theorem 2.1 is not necessary because of the non-Pappus matroid, which is not representable but was proved to be ss-representable by Simonis and Ashikhmin [40]. A number of important results and interesting ideas for future research on the characterization of ss-representable matroids can be found in the works by Simonis and Ashikhmin [40] and Matúš [27]. The first one deals with the geometric structure that lies behind ss-representations of matroids. The second one analyzes the algebraic properties that the matroid induces in all its ss-representations. These properties make it possible to find some restrictions on the ss-representations of a given matroid and, in some cases, to exclude the existence of such representations. By using these tools, Matúš [27] presented an infinite family of non-ss-representable matroids with rank three.

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 [41] and five [19] participants, the ones defined by graphs [6,8,9], and those with three or four minimal qualified subsets [23]. This problem has been considered as well for some families of multipartite access structures. Partial results about weighted threshold access structures were given in [28,34]. Subsequently, a complete characterization of the ideal access structures in this family was presented by Beimel, Tassa and Weinreb [1]. The ideal bipartite access structures were characterized in [34] and, independently, similar results were presented in [30,32]. Partial results on the characterization of tripartite access structures were presented in [1, 10,16]. The first attempt to provide general results on the characterization of ideal multipartite access structures was made by Herranz and Sáez [16], who gave some necessary conditions for a multipartite access structure to be ideal.

3. Our Results

In this paper, 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 2.1 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 natural 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. In particular, we present a complete characterization of the ideal tripartite access structures, which was an open question until now. In addition, the results in this paper have been applied recently to obtain a complete characterization of the ideal hierarchical access structures [12] that, in particular, provides a new proof for the characterization of ideal weighted threshold access structures in [1]. Our main contributions are described in more detail in the following.

First, we investigate how the necessary condition in Theorem 2.1 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. This leads us to introduce the natural concept of *multipartite 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 [13,29,35]. We use here the concise presentation of the basic facts about integer polymatroids by Herzog and Hibi [17], who applied these combinatorial objects to commutative algebra. We present in Theorem 5.3 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 [34] for the bipartite case. We present some examples showing that this necessary condition is a useful tool to prove that a given multipartite access structure is not ideal.

Second, we study the application of the sufficient condition in Theorem 2.1 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 6.1 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 6.1 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. However, Theorem 6.1 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 5.3 and 6.1 provide a framework in which those open problems can be better described and studied.

And third, we apply our general results to the tripartite case, and we present a complete characterization of the ideal tripartite access structures. By using Theorem 5.3, we characterize the tripartite matroid ports. Theorem 6.1 is used to prove that all matroids related to these structures are representable, and hence that all tripartite matroid ports are vector space access structures. Our characterization of the ideal tripartite access structures is not a simple corollary of the main theorems in this paper, and it requires to solve some non-trivial problems.

We observe that the last result above cannot be extended to m-partite access structures with $m \geq 4$, because there does not exist any ideal secret sharing scheme defining the Vamos matroid [37], which is quadripartite. Hence, there exist quadripartite matroid ports that are not ideal. Nevertheless, this does not mean that our general results are not useful for m-partite access structures with $m \geq 4$, as is demonstrated by the examples that are given later and, specially, by the characterization of the ideal hierarchical secret sharing schemes that has been presented recently in [12].

After the results in this paper, the open problems about the characterization of ideal multipartite access structures are as difficult as the open problems in the general case. That is, closing the gap between the necessary and the sufficient conditions requires to solve very difficult problems about representations of matroids and polymatroids, both by vectors and vector subspaces and by random variables.

4. Multipartite Matroids and Integer Polymatroids

4.1. *Ideal Secret Sharing Schemes, Matroids, and Matroid Ports*

As a consequence of the results by Brickell [7], and Brickell and Davenport [8], the characterization of ideal access structures has important connections with matroid theory.

To illustrate these connections, we discuss in the following the method by Brickell [7] to construct ideal secret sharing schemes, as described by Massey [25,26] in terms of linear codes. Let $P = \{p_1, \dots, p_n\}$ be a set of participants and consider a special participant $p_0 \notin P$, which is usually called *dealer*, and the set $Q = P \cup \{p_0\}$. Let C be an $[n+1, k]$-linear code over a finite field $\mathbb{K}$ and let M be a generator matrix of C, that is, a $k \times (n+1)$ matrix over $\mathbb{K}$ whose rows span C. Such a code defines an ideal secret sharing scheme on P. Specifically, every random choice of a codeword $(s_0, s_1, \dots, s_n) \in C$ 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 p_i. Such an ideal scheme is called a $\mathbb{K}$-*vector space secret sharing scheme* and its access structures is called a $\mathbb{K}$-*vector space access structure*. The access structure of this scheme is determined from the linear dependencies among the columns of the matrix M. Namely, it is easy to check that a set $A \subseteq P$ is qualified if and only if the column of M corresponding to the dealer p_0 is a linear combination of the columns corresponding to the participants in A.

Let $\mathcal{P}(Q)$ denote the power set of Q. For every $X \subseteq Q$, let $r(X)$ be the rank of the submatrix of M formed by the columns corresponding to the participants in X. This defines a mapping $r\colon \mathcal{P}(Q) \to \mathbb{Z}$ with the following properties:

1. $0 \le r(X) \le |X|$ for every $X \subseteq Q$, and
2. r is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $r(X) \le r(Y)$, and
3. r is *submodular*: $r(X \cup Y) + r(X \cap Y) \le r(X) + r(Y)$ for every pair of subsets X, Y of Q.

Matroids are combinatorial objects that abstract and generalize many concepts from linear algebra, including ranks, independent sets, bases, and subspaces. The reader is referred to [33,44] for general references on matroid theory. A *matroid* is defined as a pair (Q, r) formed by a finite set Q, the *ground set*, and a *rank function* $r\colon \mathcal{P}(Q) \to \mathbb{Z}$ satisfying the three properties above. A matroid $\mathcal{M} = (Q, r)$ is said to be $\mathbb{K}$-*representable* if there exists a matrix M with coefficients in $\mathbb{K}$ such that the rank function r can be defined from M as before. In this situation, the matrix M is called a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$.

All generator matrices of a linear code represent the same matroid. The access structure Γ of the ideal secret sharing scheme defined from a linear code C is determined from the representable matroid $\mathcal{M} = (Q, r)$ associated to C. Actually,

$$\Gamma = \Gamma_{p_0}(\mathcal{M}) = \bigl\{A \subseteq P \,:\, r\bigl(A \cup \{p_0\}\bigr) = r(A)\bigr\}.$$

That is, Γ is the *port of the matroid* $\mathcal{M}$ *at the point* p_0. Consequently, a sufficient condition for an access structure to be ideal is obtained: the ports of representable matroids are ideal access structures. Actually, they coincide with the vector space access structures.

Brickell and Davenport [8] proved that every ideal secret sharing scheme on a set P of participants determines a matroid $\mathcal{M}$ with ground set $Q = P \cup \{p_0\}$ such that the access structure of the scheme is $\Gamma_{p_0}(\mathcal{M})$. Therefore, being a matroid port is a necessary condition for an access structure to be ideal.

Matroids have been defined before by using the rank function, but this is only one of the many different but equivalent existing definitions for this concept. We present next the ones based on independent sets and on bases. The equivalence between these three definitions, whose proof can be found in [33], is very useful to obtain our results.

Let $\mathcal{M} = (Q, r)$ be a matroid. The subsets $X \subseteq Q$ with $r(X) = |X|$ are said to be *independent*. The following properties hold for the family $\mathcal{I} \subseteq \mathcal{P}(Q)$ of the independent sets of $\mathcal{M}$.

1. $\emptyset \in \mathcal{I}$.
2. If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.
3. If I_1 and I_2 are in $\mathcal{I}$ and $|I_1| < |I_2|$, then there exists $x \in I_2 - I_1$ such that $I_1 \cup \{x\} \in \mathcal{I}$.

Moreover, for every family $\mathcal{I} \subseteq \mathcal{P}(Q)$ satisfying these conditions, there exists a unique matroid whose independent sets are the members of $\mathcal{I}$. Actually, such a family $\mathcal{I}$ determines the rank function by taking $r(X)$ as the maximum cardinality of the subsets of X that are in $\mathcal{I}$. If a matroid $\mathcal{M}$ is represented over a finite field $\mathbb{K}$ by a matrix M, then a subset $X \subseteq Q$ is independent if and only if the corresponding columns of M are linearly independent.

The *bases* of the matroid $\mathcal{M}$ are the maximally independent sets. Similarly to the independent sets, the family $\mathcal{B}$ of the bases determines the matroid. Moreover, $\mathcal{B} \subseteq \mathcal{P}(Q)$ is the family of bases of a matroid with ground set Q if and only if

1. $\mathcal{B}$ is nonempty, and
2. the following *exchange condition* is satisfied: for every $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, there exists $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\}$ is in $\mathcal{B}$.

All bases have the same number of elements, which is the *rank* of $\mathcal{M}$ and is denoted $r(\mathcal{M})$. Actually, $r(\mathcal{M}) = r(Q)$. The *dependent* sets are those that are not independent, and a *circuit* is a minimally dependent set. The minimal sets of a matroid port $\Gamma_{p_0}(\mathcal{M})$ are determined from the circuits of $\mathcal{M}$. Specifically,

$$\min \Gamma_{p_0}(\mathcal{M}) = \bigl\{A \subseteq P \,:\, A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\bigr\}.$$

A matroid is said to be *connected* if, for every two points in the ground set, there exists a circuit containing them. In a *connected* access structure, 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 [33, 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 [33, Theorem 4.3.2].

4.2. *Multipartite Access Structures and Multipartite Matroids*

An *m-partition* $\Pi = (X_1, \dots, X_m)$ of a set X is a disjoint family of m subsets of X with $X = X_1 \cup \dots \cup X_m$. A permutation σ on X is a *Π-permutation* if $\sigma(X_i) = X_i$ for all $i = 1, \dots, m$. A combinatorial object defined on the set X is said to be *Π-partite* if every Π-permutation is an automorphism of it. We say that a combinatorial object on X is *m-partite* if it is Π-partite for some m-partition Π. In particular, a family $\Lambda \subseteq \mathcal{P}(X)$ of subsets of X is *Π-partite* if $\sigma(\Lambda) = \Lambda$ for every Π-permutation σ on X, where $\sigma(\Lambda) = \{\sigma(A) : A \in \Lambda\}$. These concepts can be applied to access structures, which are actually families of subsets of the set of participants. Observe that a matroid $\mathcal{M}$ is *Π-partite* for a partition Π of its ground set Q if and only if its family $\mathcal{I} \subseteq \mathcal{P}(Q)$ of independent subsets is Π-partite. A matroid port is m-partite if and only if the corresponding matroid is $(m+1)$-partite for a similar partition. Specifically, we have the following result.

Lemma 4.1. *Let $\mathcal{M}$ be a connected matroid with ground set Q. Consider a point $p_0 \in Q$ and partitions $\Pi = (P_1, \dots, P_m)$ and $\Pi_0 = (\{p_0\}, P_1, \dots, P_m)$ of the sets $P = Q - \{p_0\}$ and Q, respectively. Then the matroid port $\Gamma_{p_0}(\mathcal{M})$ is Π-partite if and only if the matroid $\mathcal{M}$ is Π_0-partite.*

Proof. Let σ be a permutation on Q with $\sigma(p_0) = p_0$. It induces a permutation $\widetilde{\sigma}$ on P. If σ is an automorphism of $\mathcal{M}$ then $\widetilde{\sigma}$ is an automorphism of $\Gamma = \Gamma_{p_0}(\mathcal{M})$, that is, $\widetilde{\sigma}(\Gamma) = \Gamma$. Conversely, since $\mathcal{M}$ is connected, it is univocally determined by its port $\Gamma = \Gamma_{p_0}(\mathcal{M})$, and hence σ is an automorphism of $\mathcal{M}$ if $\widetilde{\sigma}$ is an automorphism of Γ. □

We present in the following a very useful geometric representation of multipartite access structures, which was first used in [34] for the bipartite case. We need to introduce first some notation on vectors that will be used all through the paper. For a finite set J, let $\mathbb{R}_+^J$ denote the set of vectors $u = (u_i)_{i \in J} \in \mathbb{R}^J$ with $u_i \ge 0$ for every $i \in J$, and take $\mathbb{Z}_+^J = \mathbb{R}_+^J \cap \mathbb{Z}^J$. If $u, v \in \mathbb{R}_+^J$, we write $u \le v$ if $u_i \le v_i$ for every $i \in J$, and we write $u < v$ if $u \le v$ and $u \ne v$. The vector $w = u \vee v$ is defined by $w_i = \max\{u_i, v_i\}$. The *modulus* of a vector $u \in \mathbb{R}_+^J$ is $|u| = \sum_{i \in J} u_i$. For every subset $X \subseteq J$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{R}_+^X$ and $|u(X)| = \sum_{i \in X} u_i$. For every $i \in J$, we take the vector $\mathbf{e}^i \in \mathbb{R}_+^J$ with $\mathbf{e}^i_j = 1$ if $j = i$ and $\mathbf{e}^i_j = 0$ otherwise. For every positive integer m, we notate $J_m = \{1, \dots, m\}$ and $J'_m = \{0, 1, \dots, m\}$. Of course the vector notation that has been introduced here applies as well to $\mathbb{R}_+^m = \mathbb{R}_+^{J_m}$.

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 $\Pi = (P_1, \dots, P_m)$ be a partition of a set P. The partition Π defines a mapping $\Pi : \mathcal{P}(P) \to \mathbb{Z}_+^m$ by taking $\Pi(A) = (|A \cap P_1|, \dots, |A \cap P_m|)$. Consider $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{u \in \mathbb{Z}_+^m : 0 \le u \le \Pi(P)\}$. If a family $\Lambda \subseteq \mathcal{P}(X)$ of subsets is Π-partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda) = \{\Pi(B) : B \in \Lambda\}$. That is, Λ is completely determined by the partition Π and the set of vectors $\Pi(\Lambda) \subseteq \mathbf{P} \subseteq \mathbb{Z}_+^m$. If $\Gamma \subseteq \mathcal{P}(P)$ is a Π-partite access structure, then the set $\Pi(\Gamma) \subseteq \mathbf{P}$ is monotone increasing, that is, if $u \in \Pi(\Gamma)$ and $v \in \mathbf{P}$ are such that $u \le v$, then $v \in \Pi(\Gamma)$. Therefore, $\Pi(\Gamma)$ is univocally determined by $\min \Pi(\Gamma)$, the family of its minimal vectors, that is, those representing the minimal qualified subsets of Γ.

The *support of a vector* $u \in \mathbb{Z}_+^J$ is defined by $\operatorname{supp}(u) = \{i \in J : u_i \ne 0\} \subseteq J$, and the *support of a set* $S \subseteq \mathbb{Z}_+^J$ *of vectors* by $\operatorname{supp}(S) = \{\operatorname{supp}(u) : u \in S\} \subseteq \mathcal{P}(J)$. For a partition $\Pi = (P_1, \dots, P_m)$ of a set P, the *support of a subset* $A \subseteq P$ is $\operatorname{supp}(A) = \operatorname{supp}(\Pi(A)) \subseteq J_m$, and the *support of a* Π*-partite family* $\Lambda \subseteq \mathcal{P}(P)$ is $\operatorname{supp}(\Lambda) = \operatorname{supp}(\Pi(\Lambda)) \subseteq \mathcal{P}(J_m)$. Observe that, if Γ is a Π-partite access structure, then $\operatorname{supp}(\Gamma)$ is an access structure on the set J_m.

4.3. *Integer Polymatroids*

As we saw before, every ideal m-partite access structure is a port of an $(m+1)$-partite matroid. Therefore, multipartite matroids are fundamental for the characterization of ideal multipartite access structures. In this section, we present a connection between multipartite matroids and integer polymatroids that will be very useful for our purposes. Specifically, we prove that every m-partite matroid can be described by an integer polymatroid on a ground set with m elements. We introduce first some definitions and facts about polymatroids and we discuss in more detail the special class of the integer polymatroids. Afterwards, we discuss the connections between multipartite matroids and integer polymatroids. The reader is referred to [33,35,44] for more information about polymatroids. A detailed exposition about basic facts on integer polymatroids and the different ways to define them, including full proofs for the results that are not proved in this section, can be found in [17].

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

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

If the rank function h is integer-valued, we say that $\mathcal{S}$ is an *integer polymatroid*. Observe that every matroid is an integer polymatroid and that an integer polymatroid $\mathcal{S} = (J, h)$ is a matroid if and only if $h(X) \le |X|$ for every $X \subseteq J$.

The following example of an integer polymatroid illustrates how these objects generalize matroids. In the same way as matroids abstract some properties of collections of vectors, integer polymatroids do the same with collections of subspaces. Let E be a $\mathbb{K}$-vector space, and let $(V_i)_{i \in J}$ be a finite collection of subspaces of E. It is not difficult to check that the mapping $h : \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of an integer polymatroid $\mathcal{Z} = (J, h)$. The integer polymatroids that can be defined in this way are said to be $\mathbb{K}$-*representable*.

Polymatroids can be defined as well in terms of convex polytopes. Specifically, a polymatroid $\mathcal{S} = (J, h)$ is determined by its *independent vectors*, which are the elements in the convex polytope

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

Actually, the rank function of $\mathcal{S}$ satisfies $h(X) = \max\{|u(X)| : u \in \mathcal{T}\}$ for every $X \subseteq J$. The maximal elements in $\mathcal{T}$, that is, the vectors $u \in \mathcal{T}$ such that there does not exist any $v \in \mathcal{T}$ with $u < v$, are the *bases of the polymatroid* $\mathcal{S}$. All bases of a polymatroid have the same modulus, which equals $h(J)$, the *rank of the polymatroid* $\mathcal{S}$. More details about these concepts can be found in [44].

By formalizing known results from combinatorial optimization [13,29,35], Herzog and Hibi [17] presented two characterizations of integer polymatroids, one in terms of the integer independent vectors and another one in terms of the integer bases. Complete proofs for the facts that are stated in the following are given in [17]. Let $\mathcal{Z} = (J, h)$ be an integer polymatroid. Consider the set $\mathcal{D}$ of the *integer independent vectors* of $\mathcal{Z}$. That is, if $\mathcal{T} \subseteq \mathbb{R}_+^J$ is the set of independent vectors of $\mathcal{Z}$, then

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

The set $\mathcal{D} \subseteq \mathbb{Z}_+^J$ satisfies the following properties.

1. $\mathcal{D}$ is nonempty and finite.
2. If $u \in \mathcal{D}$ and $v \in \mathbb{Z}_+^J$ are 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 $i \in J$ with $u_i < v_i$ such that $u + \mathbf{e}^i \in \mathcal{D}$.

Recall that $\mathbf{e}^i_j = 1$ if $j = i$ and $\mathbf{e}^i_j = 0$ otherwise. Moreover, for every set $\mathcal{D} \subseteq \mathbb{Z}_+^J$ satisfying these properties, there exists a unique integer polymatroid $\mathcal{Z} = (J, h)$ such that $\mathcal{D}$ is the set of the integer independent vectors of $\mathcal{Z}$, and the rank function of $\mathcal{Z}$ is determined by

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

Such sets of vectors are called *discrete polymatroids* in [17], but we prefer to consider them simply as an alternative way to define integer polymatroids instead of as a new combinatorial object.

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

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

As happened with the integer independent vectors, every integer polymatroid $\mathcal{Z} = (J, h)$ is univocally determined by the family $\mathcal{B} \subseteq \mathbb{Z}_+^J$ of its integer bases. Observe that the rank function is determined by the bases because $h(X) = \max\{|u(X)| : u \in \mathcal{B}\}$ for every $X \subseteq J$.

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

We conclude this section by showing the connection between multipartite matroids and integer polymatroids. Specifically, we show how m-partite matroids can be described by integer polymatroids with ground set J_m. This connection, which is based on the next proposition, is fundamental for our results.

Proposition 4.2. *Let $\Pi = (Q_1, \dots, Q_m)$ 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 $\mathcal{M}$ with ground set Q if and only if $\Pi(\mathcal{I}) \subseteq \mathbb{Z}_+^m$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}$ with ground set J_m.*

Proof. Suppose that $\mathcal{I} \subseteq \mathcal{P}(Q)$ is the family of independent sets of a Π-partite matroid $\mathcal{M}$ with ground set Q. Since $0 = \Pi(\emptyset) \in \Pi(\mathcal{I})$ and $\Pi(\mathcal{I}) \subseteq \Pi(\mathcal{P}(Q))$, it is clear that $\Pi(\mathcal{I}) \subseteq \mathbb{Z}_+^m$ is nonempty and finite. Consider $u \in \Pi(\mathcal{I})$ and $v \in \mathbb{Z}_+^m$ such that $v \le u$. Take $A \in \mathcal{I}$ with $\Pi(A) = u$. Obviously, there exists $B \subseteq A$ such that $\Pi(B) = v$. Since $B \in \mathcal{I}$, we have $v \in \Pi(\mathcal{I})$. Consider now two vectors $u, v \in \Pi(\mathcal{I})$ with $|u| < |v|$. Then there exist sets $A, B \in \mathcal{I}$ such that

- $\Pi(A) = u$ and $\Pi(B) = v$, and
- if $u_i \le v_i$, then $A \cap Q_i \subseteq B \cap Q_i$, and
- if $v_i \le u_i$, then $B \cap Q_i \subseteq A \cap Q_i$.

Since $|A| < |B|$, there exists $p \in B - A$ such that $A \cup \{p\} \in \mathcal{I}$. Take the only $i \in J_m$ such that $p \in Q_i$. Clearly, $u_i < v_i$ and $u + \mathbf{e}^i = \Pi(A \cup \{p\}) \in \Pi(\mathcal{I})$.

We prove now the converse. Suppose that $\Pi(\mathcal{I}) \subseteq \mathbb{Z}_+^m$ is the family of independent vectors of an integer polymatroid with ground set J_m. Observe that $\emptyset \in \mathcal{I}$ because $0 \in \Pi(\mathcal{I})$. Consider $A \in \mathcal{I}$ and $B \subseteq Q$ such that $B \subseteq A$. Then $u = \Pi(A) \in \Pi(\mathcal{I})$ and $v = \Pi(B) \le u$, and hence $v \in \Pi(\mathcal{I})$ and $B \in \mathcal{I}$. Finally, consider two subsets $A, B \in \mathcal{I}$ with $|A| < |B|$ and take $u = \Pi(A)$ and $v = \Pi(B)$. Since $u, v \in \Pi(\mathcal{I})$ and $|u| < |v|$, there exists $i \in J$ such that $u_i < v_i$ and $u + \mathbf{e}^i \in \Pi(\mathcal{I})$. Since $u_i < v_i$ there exists $p \in Q_i \cap (B - A)$. Then $A \cup \{p\} \in \mathcal{I}$ because $\Pi(A \cup \{p\}) = u + \mathbf{e}^i \in \Pi(\mathcal{I})$. □

For an m-partite matroid $\mathcal{M}$ with family of independent sets $\mathcal{I}$, the *integer polymatroid associated with* $\mathcal{M}$ is the one having ground set J_m and family of independent vectors $\Pi(\mathcal{I})$. The rank function of an m-partite matroid and the one of its associated integer polymatroid are also tightly connected.

Proposition 4.3. *Let $\Pi = (Q_1, \dots, Q_m)$ be an m-partition of a set Q. Let $\mathcal{M} = (Q, r)$ be a Π-partite matroid and let $\mathcal{Z} = (J_m, h)$ be its associated integer polymatroid. Then $h(X) = r(\bigcup_{i \in X} Q_i)$ for every $X \subseteq J_m$.*

Proof. Let $\mathcal{I} \subseteq \mathcal{P}(Q)$ be the family of independent sets of $\mathcal{M}$. Recall that the rank $r(A)$ of every subset $A \subseteq Q$ is the maximum cardinality of the subsets of A that are independent. Then

$$r\left(\bigcup_{i\in X} Q_i\right) = \max\left\{|B| : B \in \mathcal{I} \text{ and } B \subseteq \bigcup_{i\in X} Q_i\right\}.$$

On the other hand, $h(X) = \max\{|u(X)| : u \in \Pi(\mathcal{I})\}$. Clearly, this concludes the proof. □

Finally, we prove in the following proposition that an m-partite matroid is univocally determined by its associated integer polymatroid and the m-partition of the ground set.

Proposition 4.4. *Let $\Pi = (Q_1, \dots, Q_m)$ be an m-partition of Q. For every integer polymatroid $\mathcal{Z} = (J_m, h)$ with $h(\{i\}) \le |Q_i|$ for every $i \in J_m$, there exists a unique Π-partite matroid $\mathcal{M}$ with ground set Q such that its associated integer polymatroid is $\mathcal{Z}$.*

Proof. Let $\mathcal{D} \subseteq \mathbb{Z}_+^m$ be the family of independent vectors of $\mathcal{Z}$. Observe that $\mathcal{D} \subseteq \Pi(\mathcal{P}(Q)) = \{u \in \mathbb{Z}_+^m : 0 \le u \le \Pi(Q)\}$ because $h(\{i\}) \le |Q_i|$ for every $i \in J_m$. Let $\mathcal{I} \subseteq \mathcal{P}(Q)$ be the only Π-partite family of subsets of Q such that $\Pi(\mathcal{I}) = \mathcal{D}$. By Proposition 4.2, $\mathcal{I}$ is the family of independent sets of a Π-partite matroid $\mathcal{M}$. Clearly, $\mathcal{Z}$ is the integer polymatroid associated with $\mathcal{M}$ and $\mathcal{M}$ is the only Π-partite matroid with this property. □

5. 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.

Before presenting the main result of this section, Theorem 5.3, we need to introduce some terminology and notation, as well as some basic facts about the connection between secret sharing and polymatroids.

For an integer polymatroid $\mathcal{Z} = (J, h)$ and for every subset $X \subseteq J$, the integer polymatroid $\mathcal{Z}(X) = (X, h)$ has ground set X and its rank function is the restriction to $\mathcal{P}(X)$ of the one of $\mathcal{Z}$. Let $\mathcal{D} \subseteq \mathbb{Z}_+^J$ be the family of independent vectors of $\mathcal{Z}$. Clearly, the family of independent vectors of $\mathcal{Z}(X)$ is $\mathcal{D}(X) = \{u(X) : u \in \mathcal{D}\} \subseteq \mathbb{Z}_+^X$. We consider as well the set $\mathcal{B}(\mathcal{Z}, X) \subseteq \mathbb{Z}_+^J$ 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 $i \in J - X$. Recall that, for every integer $m \ge 1$, we notate $J_m = \{1, \dots, m\}$ and $J'_m = \{0, 1, \dots, m\}$.

The connection between ideal secret sharing and matroids can be extended to general secret sharing and polymatroids [11,24]. Namely, every secret sharing scheme defines a polymatroid that determines the access structure. This connection between secret sharing and polymatroids will be used here in a slightly different way. Similarly to matroids, polymatroids define access structures. In particular, every integer polymatroid $\mathcal{Z}' = (J'_m, h)$ defines an access structure $\Delta = \Delta_0(\mathcal{Z}')$ on the set J_m by

$$\Delta_0(\mathcal{Z}') = \left\{X \subseteq J_m : h\left(X \cup \{0\}\right) = h(X)\right\}.$$

Every integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $h(\{0\}) \le 1$ and $\Delta = \Delta_0(\mathcal{Z}')$ is said to be an *integer Δ-polymatroid*. The proof of the following result is straightforward.

Proposition 5.1. *Let $\Pi = (P_1, \dots, P_m)$ be a partition of a set P, and consider the corresponding partition $\Pi_0 = (\{p_0\}, P_1, \dots, P_m)$ of the set $Q = P \cup \{p_0\}$. Let $\mathcal{M}$ be a connected Π_0-partite matroid and let $\mathcal{Z}' = (J'_m, h)$ be its associated integer polymatroid. Finally, consider the Π-partite matroid port $\Gamma = \Gamma_{p_0}(\mathcal{M})$ and take $\Delta = \operatorname{supp}(\Gamma)$. Then $\mathcal{Z}'$ is an integer Δ-polymatroid.*

An integer polymatroid $\mathcal{Z} = (J_m, h)$ and an access structure Δ on the set J_m are said to be *compatible* if $\mathcal{Z}$ can be extended to an integer Δ-polymatroid $\mathcal{Z}' = (J'_m, h)$ with $\mathcal{Z}'(J_m) = \mathcal{Z}$. Clearly, in this situation there exists a unique such integer Δ-polymatroid $\mathcal{Z}'$. The next result, which is a consequence of [11, Proposition 2.3], will be very useful in the characterization of ideal tripartite access structures presented in Sect. 7.

Proposition 5.2 [11]. *An access structure Δ on J_m is compatible with an integer polymatroid $\mathcal{Z} = (J_m, h)$ if and only if the following conditions are satisfied.*

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

Our characterization of multipartite matroid ports is given in the following theorem. Since every ideal access structure is a matroid port, this result provides a necessary condition for a multipartite access structure to be ideal.

Theorem 5.3. *Let $\Pi = (P_1, \dots, P_m)$ be a partition of a set P and let Γ be a connected Π-partite access structure on P. Consider $\Delta = \operatorname{supp}(\Gamma)$. Then Γ is a matroid port if and only if there exists an integer polymatroid $\mathcal{Z} = (J_m, h)$ with $h(\{i\}) \le |P_i|$ for every $i \in J_m$ such that Δ is compatible with $\mathcal{Z}$ and $\min \Pi(\Gamma) = \min \{u \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}$.*

Proof. Consider $\Pi = (P_1, \dots, P_m)$, a partition of the set P, and the corresponding partition $\Pi_0 = (\{p_0\}, P_1, \dots, P_m)$ 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 $\Gamma_{p_0}(\mathcal{M})$. Consider as well the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ associated with $\mathcal{M}$. Since $\mathcal{M}$ is connected, $h(\{0\}) = 1$ and $h(J_m) = h(J'_m)$. Moreover, $h(\{i\}) = r(P_i) \le |P_i|$ for every $i \in J_m$. Finally, take $\mathcal{Z} = \mathcal{Z}'(J_m)$ and $\Delta = \Delta_0(\mathcal{Z}') = \operatorname{supp}(\Gamma_{p_0}(\mathcal{M})) \subseteq \mathcal{P}(J_m)$. By Proposition 4.4, 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 $\Pi(A) \ge u$.

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

Let $A \subseteq P$ be a minimal qualified subset of $\Gamma_{p_0}(\mathcal{M})$ and take $X = \mathrm{supp}(A) \subseteq J_m$. We can suppose that $X = \{1, \dots, r\}$. Consider $u = \Pi_0(A) = (0, u_1, \dots, u_r, 0, \dots, 0)$. Observe that $u \in \mathcal{D}'$ because A is an independent set of $\mathcal{M}$. The proof is concluded by checking 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 $v = (0, u_1 + 1, u_2, \dots, u_r, 0, \dots, 0)$ is in $\mathcal{D}'$. 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 $B = (A \cup \{p_0\}) - \{p_1\}$ is an independent set of $\mathcal{M}$ if $p_1 \in A \cap P_1$. Then $w = \Pi_0(B) = (1, u_1 - 1, u_2, \dots, u_r, 0, \dots, 0) \in \mathcal{D}'$. Since $|v| > |w|$, there exists $i \in J'_m$ such that $w_i < v_i$ and $w + \mathbf{e}^i \in \mathcal{D}'$. This implies that $(1, u_1, u_2, \dots, u_r, 0, \dots, 0) = \Pi_0(A \cup \{p_0\}) \in \mathcal{D}'$, a contradiction concluding the proof. □

As a consequence of Theorem 5.3, we present in Proposition 5.5 several necessary conditions for a multipartite access structure to be a matroid port that are efficiently checkable from the family of its minimal vectors. The following lemma is used in its proof.

Lemma 5.4. *Let Γ be a connected m-partite matroid port and let $\mathcal{Z} = (J_m, h)$ be the integer polymatroid whose existence is given by Theorem 5.3. Then $u \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(u))$ for every $u \in \min \Pi(\Gamma)$.*

Proof. If $u \in \min \Pi(\Gamma)$, then $u \in \mathcal{B}(\mathcal{Z}, X)$ for some $X \subseteq J_m$. That is, u is an independent vector of $\mathcal{Z}$ with $\mathrm{supp}(u) \subseteq X$ and $|u| = h(X)$. Therefore, $|u| \le h(\mathrm{supp}(u)) \le h(X) = |u|$, and hence $|u| = h(\mathrm{supp}(u))$ and $u \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(u))$. □

Proposition 5.5. *Let Γ be a connected m-partite matroid port. Then the following conditions are satisfied.*

1. *All minimal qualified subsets of Γ having the same support have the same cardinality.*
2. *If $A, B \in \min \Gamma$ are such that $\mathrm{supp}(A) \subseteq \mathrm{supp}(B)$, then $|A| \le |B|$.*
3. *If $A, B, C \in \min \Gamma$ are such that $\mathrm{supp}(C) = \mathrm{supp}(A) \cup \mathrm{supp}(B)$, then $|C| \le |A| + |B|$.*

Proof. By Lemma 5.4, $|A| = h(\mathrm{supp}(A))$ for every $A \in \min \Gamma$, where h is the rank function of the integer polymatroid given by Theorem 5.3. This implies that all minimal qualified subsets with the same support have the same cardinality. The other results are now direct consequences of the properties of the rank function h. □

Collins [10] 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 [16] conjectured an affirmative answer. Proposition 5.5 proves and generalizes this conjecture.

We present in the following several examples showing how Theorem 5.3 and Proposition 5.5 can be applied to decide whether an m-partite access structure is a matroid port.

Example 5.6. 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 5.5.

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

Therefore, these access structures are not ideal. Moreover, by Theorem 2.2, 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.

Example 5.7. Let Γ be a quadripartite access structure such that

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

This structure satisfies the necessary conditions in Proposition 5.5. Suppose that Γ is a matroid port and consider the integer polymatroid $\mathcal{Z}' = (J_4', h)$ associated to the corresponding 5-partite matroid. From Theorem 5.3, all vectors $u \in \min \Pi(\Gamma)$ with $\operatorname{supp}(u) = J_4$ are in $\mathcal{B}$, the family of the bases of the integer polymatroid $\mathcal{Z} = \mathcal{Z}'(J_4)$. We claim that

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

Consider $u \in \mathcal{B}$. If $u \in \min \Pi(\Gamma)$, then $u \in \mathcal{A}$. If $u \notin \min \Pi(\Gamma)$, by Theorem 5.3 there exist $Y \subsetneq J_4$ and $v \in \mathcal{B}(\mathcal{Z}, Y)$ such that $v < u$ and $v \in \min \Pi(\Gamma)$. Clearly, this implies that $(4,0,0,0) < u$, and hence $u_i \le 4$ if $2 \le i \le 4$ because $|u| = 8$. Suppose that $u \not\le (4,4,4,4)$. This implies that $u_1 \ge 5$, but this is a contradiction with the fact that $h(\{1\}) = 4$ because $(4,0,0,0) \in \min \Pi(\Gamma)$. Suppose now that $(1,1,1,1) \not\le u$. 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, $(1,1,1,1) \le u \le (4,4,4,4)$ and our claim 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 5.8. Consider now the quadripartite access structure defined by

$$\min \Pi(\Gamma_1) = \big\{(2,0,0,0), (1,2,0,0), (1,0,2,0), (1,1,0,2), (1,0,1,2), \\ (0,2,1,1), (0,1,2,1), (0,1,1,2), (1,1,1,1)\big\}.$$

In this case, $\Delta = \operatorname{supp}(\Gamma_1)$ is such that $\min \Delta = \{\{1\}, \{2,3,4\}\}$. Clearly, Γ_1 satisfies the necessary conditions in Proposition 5.5. At this point, we can assume that Γ_1 is a matroid port and we can try to determine the integer polymatroid $\mathcal{Z}_1 = (J_4, h_1)$ whose existence is given by Theorem 5.3. By inspecting the vectors in $\min \Pi(\Gamma_1)$, we can determine the rank function of this integer polymatroid. From Lemma 5.4, $h_1(\{1\}) = 2$, and $h_1(\{1,2\}) = h_1(\{1,3\}) = 3$, and $h_1(\{1,2,4\}) =$

$h_1(\{1,3,4\}) = h_1(\{2,3,4\}) = h_1(J_4) = 4$. In addition, by taking into account that the minimal vectors in $\Pi(\Gamma)$ are independent vectors of $\mathcal{Z}_1$, we obtain that $h_1(\{i\}) \geq 2$ for all $i \in J_4$, and $h_1(X) \geq 3$ for every $X \subseteq J_4$ with $|X| = 2$. Since Δ must be compatible with $\mathcal{Z}_1$, we have by Proposition 5.2 that $h_1(\{i\}) < h_1(\{1,i\})$ for every $i \neq 2$ and $h_1(X) < h_1(\{2,3,4\}) = 4$ for every $X \subsetneq \{2,3,4\}$. This implies that $h_1(\{2\}) = h_1(\{3\}) = 2$ and $h_1(X) = 3$ for every $X \subseteq \{2,3,4\}$ with $|X| = 2$. By applying Proposition 5.2 again, $3 = h_1(\{2,3\}) < h_1(\{1,2,3\})$, and hence $h_1(\{1,2,3\}) = 4$. If $h_1(\{1,4\}) = 3$, then $(1,0,0,2) \in \mathcal{B}(\mathcal{Z}_1, \{1,4\})$ and $(1,0,0,2) \in \Pi(\Gamma_1)$, a contradiction. Therefore, $h_1(\{1,4\}) = 4$. Analogously, $(1,0,0,3) \in \Pi(\Gamma_1)$ if $h_1(\{4\}) = 3$, which implies that $h_1(\{4\}) = 2$. At this point, the rank function is completely determined. Summarizing,

- $h_1(\{i\}) = 2$ for all $i \in J_4$, and
- $h_1(X) = 3$ for every $X \subseteq J_4$ with $|X| = 2$ except for $h_1(\{1,4\}) = 4$, and
- $h_1(X) = 4$ for all $X \subseteq J_4$ with $|X| \geq 3$.

Observe that Δ is compatible with $\mathcal{Z}_1$ and, moreover, it is easy to check that Γ_1 is actually the quadripartite matroid port determined by Δ and $\mathcal{Z}_1$.

Example 5.9. Our last example is the quadripartite access structure with

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

This access structure is also a matroid port. Actually, the corresponding integer polymatroid $\mathcal{Z}_2 = (J_4, h_2)$ can be determined by using similar arguments as in Example 5.8. In this case, we have $h_2(\{1,3\}) = h_2(\{1,4\}) = 4$ and the other values of the rank function h_2 coincide with the ones of rank function h_1 in the previous example.

6. Representable Multipartite Matroids

The main result of this section, Theorem 6.1, deals with the application to multipartite access structures of the sufficient condition in Theorem 2.1. Specifically, it relates the linear representations of a multipartite matroid with the linear representations of its associated polymatroid. In particular, it provides a sufficient condition for a multipartite access structure to be ideal that depends only on the minimal vectors 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 Sect. 6.2, can be derived from Theorem 6.1.

Theorem 6.1. *Let $\mathcal{M} = (Q, r)$ be an m-partite matroid such that $|Q| = n$ and $r(\mathcal{M}) = k$ and let $\mathcal{Z} = (J_m, h)$ be its associated integer polymatroid. Let $\mathbb{K}$ be a finite field. If $\mathcal{M}$ is $\mathbb{K}$-representable, then so is $\mathcal{Z}$. In addition, if $\mathcal{Z}$ is $\mathbb{K}$-representable, then $\mathcal{M}$ is $\mathbb{L}$-representable for every field extension $\mathbb{L}$ of $\mathbb{K}$ such that $|\mathbb{L}| > \binom{n}{k}$.*

6.1. *Proof of Theorem 6.1*

The first claim in the statement is not difficult to prove. Let $\Pi = (Q_1, \ldots, Q_m)$ be an m-partition of Q and let $\mathcal{M} = (Q, r)$ be a Π-partite matroid, and consider its associated integer polymatroid $\mathcal{Z} = (J_m, h)$. 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 $h(X) = r(\bigcup_{i \in X} Q_i) = \dim(\sum_{i \in X} V_i)$ 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. Since a $\mathbb{K}$-representable integer polymatroid is also $\mathbb{L}$-representable for every field extension $\mathbb{L}$ of $\mathbb{K}$, it is enough to prove that, for every finite field with $|\mathbb{K}| > \binom{n}{k}$, the matroid $\mathcal{M}$ is $\mathbb{K}$-representable if the associated integer polymatroid $\mathcal{Z}$ is $\mathbb{K}$-representable.

Assume that $|\mathbb{K}| > \binom{n}{k}$ and that $\mathcal{Z}$ is $\mathbb{K}$-representable. Since $h(J_m) = r(\mathcal{M}) = k$, there exists a $\mathbb{K}$-representation of $\mathcal{Z}$ consisting of subspaces $V_1, \ldots, V_m$ of the $\mathbb{K}$-vector space $E = \mathbb{K}^k$. Consider the subset $\widetilde{\mathcal{D}} \subseteq \mathbb{Z}_+^m$ defined as follows. 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. $A_i \subseteq V_i$ and $|A_i| = u_i$ for every $i \in J_m$,
2. $A_i \cap A_j = \emptyset$ if $i \neq j$, and
3. $A_1 \cup \cdots \cup A_m \subseteq E$ is an independent set of vectors.

Lemma 6.2. *In this situation, $\widetilde{\mathcal{D}}$ is the family of independent vectors of the integer polymatroid $\mathcal{Z}$.*

Proof. Let $\mathcal{D}$ be the family of independent vectors of $\mathcal{Z}$. 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 $u \in \mathcal{D}$. Therefore, $\widetilde{\mathcal{D}} \subseteq \mathcal{D}$.

We assert that the subset $\widetilde{\mathcal{D}} \subseteq \mathbb{Z}_+^m$ is the family of independent vectors of some integer polymatroid $\widetilde{\mathcal{Z}} = (J_m, \widetilde{h})$. 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 $\mathbf{x} \in B - A$ 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 $\mathbf{y} \in A_i - B_i$. Then $(A'_1, \ldots, A'_i, \ldots, A'_m)$, where $A'_i = (A_i \cup \{\mathbf{x}\}) - \{\mathbf{y}\}$ and $A'_j = A_j$ if $j \neq i$, is a sequence corresponding to u 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 $u + \mathbf{e}^i \in \widetilde{\mathcal{D}}$. This proves our assertion.

Take $X \subseteq J_m$. Clearly, $\widetilde{h}(X) = \max\{|u(X)| : u \in \widetilde{\mathcal{D}}\} \leq \dim(\sum_{j \in X} V_j) = h(X)$. 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, $\widetilde{\mathcal{Z}} = \mathcal{Z}$ and $\widetilde{\mathcal{D}} = \mathcal{D}$. □

Lemma 6.3. *If the integer vector $u \in \mathbb{Z}_+^m$ is a basis of $\mathcal{Z}$, then there exists a basis $B = B_1 \cup \cdots \cup B_m$ of the vector space E such that $B_i \subseteq V_i$ 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 6.2. □

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 6.1 is concluded by proving that there exists a matrix $M \in \mathbf{M}$ whose columns are a $\mathbb{K}$-representation of the matroid $\mathcal{M}$.

Lemma 6.4. *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 $u = \Pi(A) \notin \mathcal{D}$, 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 $A \cap (\bigcup_{j \in X} Q_j)$ must be linearly dependent. □

Therefore, Lemma 6.6 concludes the proof of Theorem 6.1. 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 6.5. *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 $p = \sum_{i=0}^{t} p_i X_N^i$, where p_i is a polynomial on the variables $X_1, \ldots, X_{N-1}$ for $i = 0, \ldots, t$, 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 $p(x_1, \ldots, x_{N-1}, x_N) \neq 0$. □

Lemma 6.6. *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. By fixing a basis of V_i for every $i \in J_m$, we obtain one-to-one mappings $\phi_i : \mathbb{K}^{k_i} \to V_i \subseteq \mathbb{K}^k$. Let $N = \sum_{i=1}^m k_i n_i$. By using the mappings ϕ_i, we can construct a one-to-one mapping $\Psi : \mathbb{K}^N = (\mathbb{K}^{k_1})^{n_1} \times \cdots \times (\mathbb{K}^{k_m})^{n_m} \to \mathbf{M}$. That is, by choosing an element in $\mathbb{K}^N$, we obtain n_i vectors in V_i for every $i \in J_m$. For every basis $B \subseteq Q$ of the matroid $\mathcal{M}$, we consider the mapping $f_B : \mathbb{K}^N \to \mathbb{K}$ defined by $f_B(\mathbf{x}) = \det(\Psi(\mathbf{x})_B)$, where $\Psi(\mathbf{x})_B$ 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 6.3, there exists a basis of $\mathbb{K}^k$ of the form $\widetilde{B} = B_1 \cup \cdots \cup B_m$ with $B_i \subseteq V_i$ and $|B_i| = u_i$ 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 6.5, 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. □

6.2. *Constructing Ideal Multipartite Secret Sharing Schemes*

A sufficient condition for a multipartite access structure to be ideal is easily derived from Theorem 6.1. More precisely, a necessary and sufficient condition for a multipartite access structure to admit a vector space secret sharing scheme is obtained. In addition, an upper bound on the minimum size of the fields for which such a scheme exists is given.

Corollary 6.7. *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 an $\mathbb{L}$-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 $\mathcal{M}$.*

Example 6.8. We apply this condition to the multipartite matroid ports $\Gamma_1 = \Gamma_{p_0}(\mathcal{M}_1)$ and $\Gamma_2 = \Gamma_{p_0}(\mathcal{M}_2)$ from Examples 5.8 and 5.9, respectively. The first one does not admit any vector space secret sharing scheme because the rank function of the integer polymatroid $\mathcal{Z}_1 = (J_4, h_1)$ violates Ingleton inequality (see [15], for instance), which has to be satisfied by every representable integer polymatroid. This implies that the integer polymatroid $\mathcal{Z}'_1$ associated with $\mathcal{M}_1$ 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 are not ideal [37] and the folklore results about minors of access structures that are discussed in [24], we see 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 $\{v_1, \dots, v_4\}$ 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 $\mathcal{Z}'_2$ associated with $\mathcal{M}_2$.

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 6.1 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 6.1 an efficient method to construct a vector space secret sharing scheme for every given multipartite matroid port satisfying the condition in Corollary 6.7.

Another open problem is to determine the minimum size of the finite fields $\mathbb{K}$ for which a matroid port in the conditions of Corollary 6.7 admits a $\mathbb{K}$-vector space secret sharing scheme. Upper and lower bounds on the field size were given by Beutelspacher and Wettl [4] for some multilevel access structures with two levels. Upper bounds for the case of three levels have been presented recently by Giuletti and Vincenti [14]. Observe that a general upper bound can be derived from Corollary 6.7, 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 [1,2,4,7,14,16,31,34,42,43], our approach makes it possible to state them in the most general possible way.

Open Problem 6.9. Determine the existence of efficient algorithms to find representations of multipartite matroids from representations of their associated polymatroids.

Open Problem 6.10. 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 6.10 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 6.9 is derived from the proof of Theorem 6.1. 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 6.1. The constructions of ideal multipartite secret sharing schemes in [1,2,7,16,31,34,42,43] 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 linear 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 linear independence, which can grow exponentially with the number of participants. Brickell [7] proposed a method to avoid these checks, but it requires the size of the base field to be extremely large. The same happens in the random approach if a reasonable success probability is required.

7. 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 [34], but only partial results were known about the tripartite case [1,10,16].

We begin by characterizing the bipartite and tripartite matroid ports. This is done in Sect. 7.1 by applying Theorem 5.3 to the particular cases $m = 2$ and $m = 3$. In Sect. 7.2, we use Theorem 6.1 to prove that all matroids corresponding to those access structures are representable. Therefore, all matroid ports in these families are ideal and, by Theorem 2.2, 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.

7.1. *Characterizing Bipartite and Tripartite Matroid Ports*

Let Γ be a bipartite matroid port, that is, a Π-partite matroid port for some bipartition $\Pi = (P_1, P_2)$ of the set P of participants. The rank function of the integer polymatroid $\mathcal{Z} = (J_2, h)$ whose existence is given by Theorem 5.3 is completely determined by the values $r_i = h(\{i\}) \le |P_i|$ for $i \in J_2$ and $s = h(\{1, 2\})$. Moreover, from the definition of polymatroid and Proposition 5.2, 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 $\Delta = \operatorname{supp}(\Gamma)$ if and only if the following conditions are satisfied for every $i \in J_2$.

1. $0 \le r_i \le s \le r_1 + r_2$.
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

- $\mathcal{B}(\mathcal{Z}, J_2) = \{v \in \mathbb{Z}_+^2 : (s - r_2, s - r_1) \le v \le (r_1, r_2) \text{ and } |v| = s\}$, 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 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 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 $r_i = h(\{i\}) \le |P_i|$, 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 $\Delta = \operatorname{supp}(\Gamma)$ if and only if the following conditions are satisfied for every i, j, k with $\{i, j, k\} = J_3$.

1. $0 \le r_i \le s_j \le s$.
2. $s_i \le r_j + r_k$, and $s \le s_i + r_i$, and $s + r_i \le s_j + s_k$.

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

7.2. *All Bipartite and Tripartite Matroid Ports Are Ideal*

Hammer, Romashchenko, Shen and Vereshchagin [15] proved that every integer polymatroid with ground set J_m with $m \leq 3$ is representable. Nevertheless, to prove that every tripartite matroid port is ideal we need the slightly more general result in Proposition 7.1.

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 $\dim((V_1 + V_2) \cap V_3) - \dim((V_1 \cap V_3) + (V_2 \cap V_3)) = \sum s_i - \sum r_i - (s - t) \geq 0$. Therefore, $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$.

Proposition 7.1. *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 $\{v_1, \dots, v_{s_3}\}$ of V, consider the mapping $\mathbf{v}: \mathbb{K} \to V$ 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 $\dim(V_1 \cap V_2 \cap V_3) = t$. □

As we said before, next corollary was proved in [15], but we need the more general result in Proposition 7.1 for our characterization of ideal tripartite access structures. Corollary 7.3 is a direct consequence of Theorem 6.1 and Corollary 7.2.

Corollary 7.2. *Every integer polymatroid with ground set J_m with $m \leq 3$ is representable over finite fields of all characteristics.*

Corollary 7.3. *Every m-partite matroid with $m \leq 3$ is representable over finite fields of all characteristics.*

Corollary 7.4. *Every bipartite matroid port is ideal. More specifically, every bipartite matroid port is a vector space access structure over finite fields of all characteristics.*

Proof. If $\Gamma_{p_0}(\mathcal{M})$ is a bipartite matroid port, then the matroid $\mathcal{M}$ is tripartite and, from Corollary 7.3, it is representable over finite fields of all characteristics. □

The next lemma is a well-known result of linear algebra. It will be used in the proof of Theorem 7.6.

Lemma 7.5. *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 7.6. *Every tripartite matroid port is ideal. More specifically, every tripartite matroid port is a vector space access structure over finite fields of all characteristics.*

Proof. Let $\Gamma = \Gamma_{p_0}(\mathcal{M})$ be a tripartite matroid port. By Theorem 6.1, we only have to prove that the integer polymatroid $\mathcal{Z}' = (J'_3, h)$ associated to $\mathcal{M}$ is representable over finite fields of all characteristics. Consider $\Delta = \operatorname{supp}(\Gamma)$ 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 7.1, 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 Sect. 7.1.

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 $V' = V_2 + (V_1 \cap V_3) \subseteq V$,
$$E = (V_1 + V_3) + V' \subseteq (V_1 + V_3) + V \subseteq E, \tag{1}$$
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 (1), $\dim W = \sum s_i - 2s$. 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. □

8. Other Ideal Multipartite Access Structures

Several constructions of ideal secret sharing schemes for different families of multipartite access structures have been proposed in the literature [2,7,16,21,31,39,42,43]. In order to illustrate the connection of our general results on ideal multipartite secret sharing schemes with those previous works on the topic, we prove in an alternative way that some of those access structures are ideal. Similar proofs can be obtained for the other ones.

8.1. *Multilevel Access Structures*

We consider first a family of multipartite access structures with hierarchical properties. Given a partition $\Pi = (P_1, \dots, P_m)$ of the set P of participants and a monotone increasing sequence of integer values $0 < t_1 < \cdots < t_m$, consider the Π-partite access structure determined by

$$\Pi(\Gamma) = \left\{ u \in \mathbf{P} : \text{ there exists } i \in J_m \text{ such that } \sum_{j=1}^{i} u_j \geq t_i \right\},$$

where $\mathbf{P} = \Pi(\mathcal{P}(P)) \subseteq \mathbb{Z}_+^m$. This structure is *hierarchical*, in the sense that, if $A \in \Gamma$ and $j < i$, then a participant in $A \cap P_i$ can be replaced by a participant in $P_j - A$ and the new set is still qualified. This family of access structures was introduced by Simmons [39], who called them *multilevel access structures*. Brickell [7] showed how to construct ideal secret sharing schemes for them.

By using our general results on multipartite secret sharing, we present in the following an alternative proof for the fact that these multipartite access structures are ideal. We use a special class of integer polymatroids, the *boolean polymatroids*. Given a finite set B and a family of subsets $\{B_1, \dots, B_m\} \subseteq \mathcal{P}(B)$, it is easy to check that the mapping $h : \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = |\bigcup_{i \in X} B_i|$ is the rank function of an integer polymatroid $\mathcal{Z} = (J_m, h)$. Such integer polymatroids are called *boolean* and we prove next that they are representable over every finite field. Let $\mathbb{K}$ be a finite field and take a basis $\{e_1, \dots, e_k\}$ of $E = \mathbb{K}^k$, where $k = |B|$. We can assume that $B = \{e_1, \dots, e_k\}$. For every $i \in J_m$, consider the subspace $V_i \subseteq E$ spanned by the vectors in B_i. Clearly, the subspaces $(V_1, \dots, V_m)$ are a $\mathbb{K}$-representation of the integer polymatroid $\mathcal{Z}$.

Given a sequence of integers $0 < t_1 < \cdots < t_m$, consider the set $B = \{1, \dots, t_m\}$ and, for every $i \in J_m$, the subset $B_i = \{1, \dots, t_i\}$ together with $B_0 = \{1\}$. This defines a boolean polymatroid $\mathcal{Z}' = (J'_m, h)$ with $h(\{0\}) = 1$ and $h(\{i\}) = t_i$ for every $i \in J_m$. We claim that, if $|P_i| \geq t_i$ for every $i \in J_m$, the access structure Γ that was defined before coincides with the Π-partite matroid port $\widehat{\Gamma}$ that is determined by the integer polymatroid $\mathcal{Z}'$. Recall that $\widehat{\Gamma}$ is such that $\min \Pi(\widehat{\Gamma}) = \min\{u \in \mathcal{B}(\mathcal{Z}, X) : X \in \Delta\}$, where $\mathcal{Z} = \mathcal{Z}'(J_m)$ and $\Delta = \operatorname{supp}(\widehat{\Gamma}) = \Delta_0(\mathcal{Z}')$. Clearly, Δ consists of all nonempty subsets of J_m. In addition, $h(X) = t_i$, where $i \in J_m$ is the maximum element in $X \subseteq J_m$. Consider $u \in \Pi(\Gamma)$, let $i \in J_m$ be the minimum value such that $\sum_{j=1}^{i} u_j \geq t_i$, and consider a vector $v \leq u$ such that $\sum_{j=1}^{i} v_j = t_i$ and $v_j = 0$ for all $j > i$. Clearly, $|v(\{1, \dots, i\})| = t_i = h(\{1, \dots, i\})$ and $|v(X)| \leq h(X)$ for every $X \subseteq \{1, \dots, i\}$. Therefore, $v \in \mathcal{B}(\mathcal{Z}, \{1, \dots, i\})$, which implies that $v \in \Pi(\widehat{\Gamma})$, and hence $u \in \Pi(\widehat{\Gamma})$. Suppose now that $u \in \min \Pi(\widehat{\Gamma})$. Then there exists $X \subseteq J_m$ such that $u \in \mathcal{B}(\mathcal{Z}, X)$. If $i = \max X$, then $|u| = h(X) = h(\{1, \dots, i\}) = t_i$, which implies that $u \in \Pi(\Gamma)$. This proves our claim. Since the integer polymatroid $\mathcal{Z}'$ is representable over every finite field, the multilevel access structure Γ is a vector space access structure over fields of all characteristics if $|P_i| \geq t_i$ for all $i \in J_m$. If $|P_i| < t_i$ for some $i \in J_m$, then Γ is also a vector space access structure because of the results about minors that are described in [24].

8.2. *Compartmented Access Structures*

The first examples of *compartmented access structures* were introduced by Simmons [39], and ideal secret sharing schemes were constructed by Brickell [7] for a more general family of such structures, which is described in the following. For a partition $\Pi = (P_1, \dots, P_m)$ of the set P of participants and positive integers $t, t_1, \dots, t_m$ with $t \geq \sum_{i=1}^{m} t_i$, consider the access structure Γ consisting of all subsets with at least t participants in total and least t_i participants in every compartment P_i. That is,

$$\Pi(\Gamma) = \bigl\{u \in \mathbf{P} : |u| \geq t \text{ and } u_i \geq t_i \text{ for every } i \in J_m\bigr\}.$$

Since the set $\mathcal{B} = \min \Pi(\Gamma) \subseteq \mathbb{Z}_+^m$ satisfies the required exchange property, $\mathcal{B}$ is the family of bases of some integer polymatroid $\mathcal{Z} = (J_m, h)$. We assume that $|P_i| \geq t - \sum_{j \neq i} t_j$ for every $i \in J_m$. Observe that the access structure $\Delta = \operatorname{supp}(\Gamma) = \{J_m\}$ is compatible with the integer polymatroid $\mathcal{Z}$ because $h(J_m - \{i\}) = \max\{|u(J_m - \{i\})| : u \in \mathcal{B}\} = t - t_i \leq t - 1 = h(J_m) - 1$ for every $i \in J_m$. Therefore, there exists an integer polymatroid $\mathcal{Z}' = (J'_m, h)$ with $h(\{0\}) = 1$, and $\mathcal{Z}'(J_m) = \mathcal{Z}$, and $\Delta = \Delta_0(\mathcal{Z}')$. From Theorem 5.3, Γ is a matroid port. We prove next that $\mathcal{Z}'$ is representable over every large enough finite field, and hence Γ is a vector space access structure over finite fields of all characteristics. Consider a set B with $|B| = t$ and a partition $B = T \cup T_1 \cup \cdots \cup T_m$ with $|T| = t - \sum_{i \in J_m} t_i$ and $|T_i| = t_i$ for every $i \in J_m$. We claim that $\mathcal{Z}$ coincides with the boolean polymatroid $\widehat{\mathcal{Z}} = (J_m, \widehat{h})$ defined from the subsets $B_i = T \cup T_i \subseteq B$ for $i \in J_m$. Actually, for every nonempty $X \subseteq J_m$,

$$h(X) = \max\bigl\{\bigl|u(X)\bigr| : u \in \mathcal{B}\bigr\} = t - \sum_{j \notin X} t_j,$$

while

$$\widehat{h}(X) = \left|\bigcup_{j \in X} B_j\right| = \left|T \cup \left(\bigcup_{j \in X} T_j\right)\right| = t - \sum_{j \notin X} t_j,$$

and our claim is proved. Therefore, for every finite field $\mathbb{K}$, there exists a $\mathbb{K}$-representation of $\mathcal{Z}$ formed by vector subspaces $V_1, \dots, V_m \subseteq \mathbb{K}^t$. For $i \in J_m$, consider $W_i = \sum_{j \neq i} V_i$. Then $W_i \neq \mathbb{K}^t$ because $\dim W_i = h(J_m - \{i\}) < h(J_m) = t$. By Lemma 7.5, if $|\mathbb{K}| > m$, there exists a vector $x_0 \in \mathbb{K}^t$ such that $x_0 \notin W_i$ for all $i \in J_m$. Therefore, if $V_0 = \langle x_0 \rangle$, the vector subspaces $V_0, V_1, \dots, V_m \subseteq \mathbb{K}^t$ provide a $\mathbb{K}$-representation of the integer polymatroid $\mathcal{Z}'$. As before, the access structure Γ is ideal also in the case that $|P_i| < t - \sum_{j \neq i} t_j$ for some $i \in J_m$.

Tassa and Dyn [43] presented a construction of ideal secret sharing schemes, based on bivariate polynomial interpolation, for a different class of compartmented access structures. In this case, given positive integers $t, t_1, \dots, t_m$ with $t_i \leq t \leq \sum_{i=1}^{m} t_i$, one considers the access structure defined by

$$\Pi(\Gamma) = \bigl\{u \in \mathbf{P} : \text{there exists } v \leq u \text{ with } |v| = t \text{ and } v_i \leq t_i \text{ for every } i \in J_m\bigr\}.$$

Consider $t_0 = 1$ and the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ defined by $h(X) = \min\{t, \sum_{i \in X} t_i\}$ for every $X \subseteq J'_m$. Suppose that $|P_i| \geq t_i$ for all $i \in J_m$. Observe that the family $\mathcal{B}$ of the bases of $\mathcal{Z} = \mathcal{Z}'(J_m)$ coincides with $\min \Pi(\Gamma)$. Actually, $u \in \min \Pi(\Gamma)$ if and only if $|u| = t$ and $|u(X)| \le \min\{t, \sum_{i\in X} t_i\} = h(X)$ for all $X \subseteq J_m$, that is, if and only if $u \in \mathcal{B}$. Therefore, Γ is the port of the Π_0-partite matroid determined by $\mathcal{Z}'$. We prove in the following that $\mathcal{Z}'$ is $\mathbb{K}$-representable for every finite field with $|\mathbb{K}| \ge \sum_{i\in J'_m} t_i$, and hence Γ is a vector space access structure over fields of all characteristics. Consider the mapping $\mathbf{v}\colon \mathbb{K} \to \mathbb{K}^t$ defined by $\mathbf{v}(x) = (1, x, x^2, \dots, x^{t-1})$ and consider $\sum_{i\in J'_m} t_i$ distinct values $(x_{i,j})_{0\le i\le m, 1\le j\le t_i}$ in $\mathbb{K}$. For every $i \in J'_m$, consider the vector subspace $V_i \subseteq \mathbb{K}^t$ spanned by $\{\mathbf{v}(x_{i,j}) : 1 \le j \le t_i\}$. Clearly, these subspaces form a $\mathbb{K}$-representation of $\mathcal{Z}'$.

References

[1] A. Beimel, T. Tassa, E. Weinreb, Characterizing ideal weighted threshold secret sharing. *SIAM J. Discrete Math.* **22**(1), 600–619 (2008)

[2] M. Belenkiy, Disjunctive multi-level secret sharing, *Cryptology ePrint Archive*, report 2008/018, http://eprint.iacr.org/2008/018

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

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

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

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

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

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

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

[10] M.J. Collins, A note on ideal tripartite access structures, *Cryptology ePrint Archive*, report no. 2002/193, http://eprint.iacr.org/2002/193

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

[12] O. Farràs, C. Padró, Ideal hierarchical secret sharing schemes, in *7th Theory of Cryptography Conference, TCC 2010*. Lecture Notes in Comput. Sci., vol. 5978, pp. 219–236 (2010)

[13] S. Fujishige, *Submodular Functions and Optimization*. Ann. Discrete Math., vol. 47, (North-Holland/Elsevier, Amsterdam, 1991)

[14] M. Giuletti, R. Vincenti, Three-level secret sharing schemes from the twisted cubic. *Discrete Math.* **310**(22), 3236–3240 (2010)

[15] D. Hammer, A.E. Romashchenko, A. Shen, N.K. Vereshchagin, Inequalities for Shannon entropy and Kolmogorov complexity. *J. Comput. Syst. Sci.* **60**, 442–464 (2000)

[16] J. Herranz, G. Sáez, New results on multipartite access structures. *IEE Proc. Inf. Secur.* **153**, 153–162 (2006)

[17] J. Herzog, T. Hibi, Discrete polymatroids. *J. Algebr. Comb.* **16**, 239–268 (2002)

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

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

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

[21] S.C. Kothari, Generalized linear threshold scheme, in *Advances in Cryptology—CRYPTO '84*. Lecture Notes in Comput. Sci., vol. 196, pp. 231–241 (1985)

[22] A. Lehman, A solution of the Shannon switching game. *J. Soc. Ind. Appl. Math.* **12**, 687–725 (1964)

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

[24] J. Martí-Farré, C. Padró, On secret sharing schemes, matroids and polymatroids. *J. Math. Cryptol.* **4**, 95–120 (2010)

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

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

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

[28] P. Morillo, C. Padró, G. Sáez, J.L. Villar, Weighted threshold secret sharing schemes. *Inf. Process. Lett.* **70**, 211–216 (1999)

[29] K. Murota, *Discrete Convex Analysis*. SIAM Monographs on Discrete Mathematics and Applications (SIAM, Philadelphia, 2003)

[30] S.-L. Ng, A representation of a family of secret sharing matroids. *Des. Codes Cryptogr.* **30**, 5–19 (2003)

[31] S.-L. Ng, Ideal secret sharing schemes with multipartite access structures. *IEE Proc. Commun.* **153**, 165–168 (2006)

[32] S.-L. Ng, M. Walker, On the composition of matroids and ideal secret sharing schemes. *Des. Codes Cryptogr.* **24**, 49–67 (2001)

[33] J.G. Oxley, *Matroid Theory*. Oxford Science Publications (Clarendon Oxford University Press, New York, 1992)

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

[35] A. Schrijver, *Combinatorial Optimization. Polyhedra and Efficiency* (Springer, Berlin, 2003)

[36] P.D. Seymour, A forbidden minor characterization of matroid ports. *Q. J. Math. Oxf. Ser.* **27**, 407–413 (1976)

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

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

[39] G.J. Simmons, How to (really) share a secret. *Advances in Cryptology—CRYPTO 88*. Lecture Notes in Comput. Sci., vol. 403, pp. 390–448 (1990)

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

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

[42] T. Tassa, Hierarchical threshold secret sharing. *J. Cryptol.* **20**, 237–264 (2007)

[43] T. Tassa, N. Dyn, Multipartite secret sharing by bivariate interpolation. *J. Cryptol.* **22**, 227–258 (2009)

[44] D.J.A. Welsh, *Matroid Theory* (Academic Press, London, 1976)