Ideal Multipartite Secret Sharing Schemes *

Oriol Farràs, Jaume Martí-Farré, and Carles Padró

Dept. of Applied Maths. IV, Technical University of Catalonia, Barcelona.
{ofarras,jaumem,cpadro}@ma4.upc.edu

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. Several particular families of multipartite schemes, such as the weighted threshold schemes, the hierarchical and the compartmented schemes, and the ones with bipartite or tripartite access structure have been considered in the literature. The characterization of the access structures of ideal secret sharing schemes is one of the main open problems in secret sharing. 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. One of the main contributions of this paper is the application of discrete polymatroids to secret sharing. They are proved to be a powerful tool to study the properties of multipartite matroids. In this way, we obtain some necessary conditions and some sufficient conditions for a multipartite access structure to be ideal.
Our results can be summarized as follows. First, we present a characterization of matroid-related multipartite access structures in terms of discrete polymatroids. As a consequence of this characterization, a necessary condition for a multipartite access structure to be ideal is obtained. Second, we use linear representations of discrete polymatroids to characterize the linearly representable multipartite matroids. In this way we obtain a sufficient condition for a multipartite access structure to be ideal. 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, Discrete polymatroids.

1 Introduction

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

* This work was partially supported by the Spanish Ministry of Education and Science under projects TIC 2003-00866 and TSI2006-02731. This work was done partly while the third 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.

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 will find in [34] an excellent introduction to secret sharing. Observe that the access structure of a secret sharing scheme 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 qualified subset is itself qualified.

Secret sharing was introduced in 1979 by Shamir [31] and Blakley [4], who independently presented two different methods to construct *threshold* secret sharing schemes. Their qualified subsets are those having at least a given number of participants. The threshold schemes proposed in [4, 31] 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 [16].

Dealing only with threshold access structures can be a serious limitation in some applications of secret sharing. In his seminal paper [31], Shamir made the first attempt to overcome this by proposing a construction of *weighted threshold schemes*. 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 proposed construction 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 anymore. Ito, Saito, and Nishizeki [14] 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. 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, very little is known about the construction of efficient secret sharing schemes for general access structures and, in particular, there is a wide gap between the best known lower and upper bounds on the length of the shares.

Due to the difficulty of finding efficient secret sharing schemes for general access structures, it is worthwhile to find families of access structures that admit ideal schemes and have other useful properties for the applications of secret sharing. Brickell [7] proposed a method to construct ideal secret sharing schemes for access structures other than the threshold ones. This method provides ideal schemes for *multilevel* and *compartmented* access structures, two families that were proposed by Simmons [32] because of their interesting applications. These access structures are *multipartite*, that is, the set of participants is divided into several parts and all participants in the same part play an equivalent role. Multipartite access structures are useful in scenarios in which the participants can be divided into different classes, such as hierarchical organizations, or actions that require the agreement of different parties. Other constructions of ideal secret sharing schemes for different classes of multipartite access structures have been presented in [25, 35, 36].

The natural step beyond the construction of ideal schemes for particular structures is the search of a characterization of the *ideal access structures*, that is, the access structures of ideal secret sharing schemes. This is one of the most important open problems in secret sharing. As a consequence of the results by Brickell [7], and Brickell and Davenport [8], this open problem has important connections with matroid theory. Some basic concepts about matroids and their connection to secret sharing are recalled in Section 4.1.

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 $Q = P \cup \{p_0\}$. This matroid determines the access structure of the scheme. Namely, $A \subseteq P$ is a minimal qualified subset if and only if $A \cup \{p_0\}$ is a circuit of $\mathcal{M}$. In this situation, we say that this access structure is *matroid-related* or, more specifically, *related to the matroid* $\mathcal{M}$. Therefore, a necessary condition for an access structure to be ideal is obtained.

Theorem 1. (Brickell and Davenport [8]) *The access structure of every ideal secret sharing scheme is matroid-related.*

The method to construct ideal schemes proposed by Brickell [7], which is based on linear algebra, provides a sufficient condition for an access structure to be ideal.

Theorem 2. (Brickell [7]) *There exists an ideal secret sharing scheme for every access structure that is related to a linearly representable matroid.*

The minimal qualified subsets of a matroid-related access structure form a *matroid port*, a combinatorial object introduced by Lehman [17] in 1964, much before secret sharing was invented. Seymour [29] presented in 1976 a forbidden minor characterization of matroid ports, which has been used recently to obtain new results on the characterization of matroid-related access structures [21]. The *information rate* of a secret sharing scheme is the ratio between the length of the secret and the maximum length of the shares. The main result in [21] is a generalization of Theorem 1.

Theorem 3. (Martí-Farré and Padró [21]) *The access structure of every secret sharing scheme with information rate greater than* $2/3$ *is matroid-related.*

2 Related Work

Due to the difficulty of finding general results, the characterization of ideal access structures has been studied for several particular classes of access structures: the access structures on sets of four [34] and five [15] participants, the ones defined by graphs [6, 8, 9], the bipartite access structures [28], those with three or four minimal qualified subsets [18], the ones with intersection number equal to one [19], the access structures with rank three [20], and the weighted threshold access structures [2]. In most of these families, all the matroids that are related to access structures in the family are representable, and then the matroid-related access structures coincide with the ideal ones. This, combined with Theorem 3, implies that the optimal information rate of every non-ideal access structure in those families is at most 2/3.

Multipartite access structures were first introduced by Shamir [31] in his introductory work, in which weighted threshold access structures were considered. These structures have been studied also in [23, 28] and a characterization of the ideal weighted access structures has been presented in [2]. Brickell [7] constructed ideal secret sharing schemes for several different kinds of multipartite access structures that had been previously considered by Simmons [32]. Other constructions of ideal schemes for these and other multipartite structures have been presented in [12, 25, 35, 36]. A complete characterization of ideal bipartite access structures was given in [28] and, independently, in [24, 26]. Partial results on the characterization of tripartite access structures have been presented in [2, 10, 12]. The first attempt to provide general results on the characterization of ideal multipartite access structures has been made recently by Herranz and Sáez [12]. They present some necessary conditions for a multipartite access structure to be ideal, which generalize the ones given in [10] for the tripartite case. In addition, they present a wide family of ideal tripartite access structures.

3 Our Results

In this paper, we study the characterization of the *ideal multipartite access structures*. Since we can always consider 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 the characterization of the ideal access structures. Of course, we do not solve this long-standing open problem. Nevertheless, we present some new results by looking at it under a different point of view. Namely, we investigate the conditions given in Theorems 1 and 2 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 discrete polymatroids, which appear to be a very powerful tool to characterize the matroid-related multipartite access structures. Even though our results can be applied to the general case, their most meaningful consequences are obtained when applied to some particular families of multipartite access structures. Specifically, in the case that the number of parts is significantly smaller than the number of participants, or in situations in which the parts are distributed in some special way 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. Our main contributions are described with more detail in the following.

First, we investigate how the necessary condition in Theorem 1 can be applied to multipartite access structures. Consequently, we study the properties of matroid-related multipartite access structures. The partition in the set of participants of a matroid-related access structure 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 *discrete polymatroid* on a set of m points. Discrete polymatroids are a particular class of polymatroids. In the same way as matroids abstract the combinatorial properties of a collection of vectors in a vector space, discrete polymatroids abstract the combinatorial properties of a collection of subspaces in a vector space. Discrete polymatroids have been thoroughly studied by Herzog and Hibi [13], and some of the results in that paper are used here. By using discrete polymatroids, we present in Theorem 8 a characterization of matroid-related multipartite access structures, which implies a necessary condition for a multipartite access structure to be ideal. We present some examples showing that this necessary condition is a useful tool to prove that a given multipartite structure is not ideal.

Second, we study the application of Theorem 2 to multipartite access structures. Therefore, we study the existence of linear representations for multipartite matroids, and we relate them to linear representations of discrete polymatroids. In the same way as in a linear representation of a matroid a vector is assigned to each point in the ground set, a subspace is assigned to each point in a linear representation of a discrete polymatroid. We prove in Theorem 13 that a multipartite matroid is linearly representable if and only if the corresponding discrete polymatroid is linearly representable. This implies a sufficient condition for a multipartite access structure to be ideal. We think that Theorem 13 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 linearly representable.

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 8, we characterize the matroid-related tripartite access structures. Theorem 13 is used to prove that all matroids related to these structures are linearly representable, and hence that all matroid-related tripartite access structures are ideal. Moreover, as a consequence of Theorem 3, the optimal information rate of every non-ideal tripartite access structure is at most $2/3$. The application of our general results to the tripartite case requires to solve some non-trivial problems. Therefore, our characterization of the ideal tripartite access structures is not a simple corollary of the main theorems in this paper.

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 [1, 30, 33], which is quadripartite. Hence, there exist matroid-related quadripartite access structures 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 it is demonstrated with some examples.

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.

4 Multipartite Access Structures, Multipartite Matroids, and Discrete Polymatroids

4.1 Ideal Secret Sharing Schemes and Matroids

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

To illustrate these connections, we describe the construction of ideal secret sharing schemes due to Brickell [7]. Given a set P of participants, consider a special participant $p_0 \notin P$, which is usually called *dealer*, and $Q = P \cup \{p_0\}$. Every mapping $\psi \colon Q \to E$, where E is a vector space over some finite field $\mathbb{K}$, determines an ideal secret sharing scheme Σ_ψ on the set P of participants. Given a secret value $s_0 \in \mathbb{K}$, a random vector $\mathbf{x} \in E$ such that the dot product $\mathbf{x} \cdot \psi(p_0)$ is equal to s_0 is chosen uniformly at random. The share of the participant $i \in P$ is the value $s_i = \mathbf{x} \cdot \psi(i) \in \mathbb{K}$. A subset $A \subseteq P$ is in the access structure Γ of the scheme Σ_ψ if and only if the vector $\psi(p_0)$ is a linear combination of the vectors in $\{\psi(i) : i \in A\}$. The ideal schemes of this form are called $\mathbb{K}$*-vector space secret sharing schemes*, and their access structures are called $\mathbb{K}$*-vector space access structures*.

The access structure of Σ_ψ is determined by the *rank function* $r \colon \mathcal{P}(Q) \to \mathbb{Z}$, where $\mathcal{P}(Q)$ is the power set of Q and, for every $X \subseteq Q$, the value $r(X)$ is the dimension of the subspace of E spanned by the set $\{\psi(i) : i \in X\}$. Actually, a subset $A \subseteq P$ is qualified if and only if $r(A \cup \{p_0\}) = r(A)$. It is easy to check that the function r satisfies

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 [27, 37] for general references on matroid theory. One of the many possible equivalent definitions for this concept says that a matroid is 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 properties above. A matroid $\mathcal{M} = (Q, r)$ is said to be $\mathbb{K}$-*linearly representable* if there exists a $\mathbb{K}$-vector space E and a mapping $\psi \colon Q \to E$ assigning a vector to each element in Q such that the rank function r can be defined from ψ as before.

For a matroid $\mathcal{M} = (Q, r)$ and a point $p_0 \in Q$, we define the access structure $\Gamma_{p_0}(\mathcal{M})$ on the set of participants $P = Q - \{p_0\}$ by $\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : r(A \cup \{p_0\}) = r(A)\}$. The access structures of this form are called *matroid-related* (the definition we gave in the Introduction for this concept is equivalent to this one). If the access structure $\Gamma_{p_0}(\mathcal{M})$ is *connected*, that is, if every participant is in a minimal qualified subset, then the matroid $\mathcal{M}$ is univocally determined by $\Gamma_{p_0}(\mathcal{M})$. Observe that Γ is a $\mathbb{K}$-vector space access structure if and only if $\Gamma = \Gamma_{p_0}(\mathcal{M})$ for some $\mathbb{K}$-linearly representable matroid $\mathcal{M}$. Therefore, as a consequence of the construction by Brickell [7], we obtain Theorem 2, a sufficient condition for an access structure to be ideal.

Brickell and Davenport [8] proved that this sufficient condition is not very far from being necessary. Specifically, they 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, a necessary condition for an access structure to be ideal is obtained (Theorem 1).

Matroids that are obtained from ideal secret sharing schemes are said to be *secret sharing representable* (or *ss-representable* for short). Therefore, an access structure is ideal if and only if it is related to a ss-representable matroid. Since there exist non-ss-representable matroids, the necessary condition in Theorem 1 is not sufficient. The first example, the Vamos matroid, was found by Seymour [30]. Other proofs of this fact were presented in [1, 33]. Many other examples non-ss-representable matroids were given by Matúš [22]. In addition, the sufficient condition in Theorem 2 is not necessary because of the non-Pappus matroid, which is not linearly representable but was proved to be ss-representable by Simonis and Ashikhmin [33].

At this point, two open problems arise that are central in the characterization of ideal access structures. First, the characterization of matroid-related access structures and, second, the characterization of ss-representable matroids.

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 [33] and Matúš [22]. 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 [22] presented an infinite family of non-ss-representable matroids with rank three.

4.2 Matroids, Integer Polymatroids, and Discrete Polymatroids

Matroids have been defined in Section 4.1 by using the rank function. There exist many other definitions. We present in the following the ones based on independent sets and on bases. The equivalence between them, which is proved in [27], will be 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 family $\mathcal{I} \subseteq \mathcal{P}(Q)$ of the independent sets of $\mathcal{M}$ is a nonempty family of subsets characterized by the following two properties.

1. If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$, and
2. 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 $I_1 \cup \{x\} \in \mathcal{I}$.

The *bases* of the matroid $\mathcal{M}$ are the maximally independent sets. Similarly to the independent sets, the nonempty family $\mathcal{B}$ of the bases determines the matroid. Moreover, a nonempty subset $\mathcal{B} \subseteq \mathcal{P}(Q)$ is the family of bases of a matroid on Q if and only if 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. A matroid is said to be *connected* if, for every two points $x, y \in Q$, there exists a circuit C with $x, y \in C$.

If E is a $\mathbb{K}$-vector space and $\psi \colon Q \to E$ is a $\mathbb{K}$-linear representation of the matroid $\mathcal{M} = (Q, r)$, then a subset $X \subseteq Q$ is independent (respectively, a basis) if and only if the multiset $\{\psi(i) : i \in X\}$, where some values may be repeated, is a linearly independent set of vectors in E (respectively, a basis of the subspace of E spanned by $\psi(Q)$).

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

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

If the rank function h is integer-valued, we say that $\mathcal{Z}$ is an *integral polymatroid*. The reader is referred to [37] for more information about polymatroids.

The following example of an integral polymatroid illustrates the similarity with matroids. In the same way as matroids abstract some properties of collections of vectors, integral polymatroids do the same with collections of subspaces. Let E be a $\mathbb{K}$-vector space, and $V_1, \dots, V_m$ subspaces of E. It is not difficult to check that the mapping $h \colon \mathcal{P}(\{1, \dots, m\}) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of an integral polymatroid $\mathcal{Z} = (\{1, \dots, m\}, h)$. The integral polymatroids that can be defined in this way are said to be $\mathbb{K}$*-linearly representable*.

Discrete polymatroids were introduced by Herzog and Hibi [13]. They are closely related to integral polymatroids. In addition, we show in the following that discrete polymatroids are extremely useful to study multipartite matroids, and hence they are a very important tool in the characterization of ideal multipartite access structures.

We need to introduce some notation. For every integer $m \geq 1$, we consider the set $J_m = \{1, \ldots, m\}$. Let $\mathbb{Z}_+^m$ denote the set of vectors $u = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ with $u_i \geq 0$ for every $i \in J_m$. If $u, v \in \mathbb{Z}_+^m$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J_m$, and we write $u < v$ if $u \leq v$ and $u \neq v$. The vector $w = u \vee v$ is defined by $w_i = \max\{u_i, v_i\}$. The *modulus* of a vector $u \in \mathbb{Z}_+^m$ is $|u| = u_1 + \cdots + u_m$. For every subset $X \subseteq J_m$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^{|X|}$ and $|u(X)| = \sum_{i \in X} u_i$.

A *discrete polymatroid* with *ground set* J_m is a nonempty finite set of vectors $\mathcal{D} \subset \mathbb{Z}_+^m$ satisfying

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

A *basis* of a discrete polymatroid $\mathcal{D}$ is a maximal element in $\mathcal{D}$, that is, a vector $u \in \mathcal{D}$ such that there does not exist any $v \in \mathcal{D}$ with $u < v$. Similarly to matroids, all bases have the same modulus. In addition, a discrete polymatroid is determined by its bases. Specifically, in [13, Theorem 2.3] it is proved that a nonempty subset $\mathcal{B} \subset \mathbb{Z}_+^m$ is the family of bases of a discrete polymatroid if and only if it satisfies the following *exchange condition*.

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

The mapping $h \colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \max\{|u(X)| : u \in \mathcal{D}\}$ is called the *rank function* of the discrete polymatroid $\mathcal{D}$. As a consequence of a result by Herzog and Hibi [13, Theorem 3.4], there is a one-to-one correspondence between discrete polymatroids and integral polymatroids, as it is stated in the following proposition. Because of that, from now on we will deal only with discrete polymatroids.

Proposition 4. *A mapping $h \colon \mathcal{P}(J_m) \to \mathbb{Z}$ is the rank function of a discrete polymatroid $\mathcal{D} \subset \mathbb{Z}_+^m$ with ground set J_m if and only if (J_m, h) is an integral polymatroid. In addition, a discrete polymatroid $\mathcal{D}$ is univocally determined from its rank function h because $\mathcal{D} = \{u \in \mathbb{Z}_+^m : |u(X)| \leq h(X)$ for every $X \subseteq J_m\}$.*

4.3 Multipartite Access Structures and Multipartite Matroids

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

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

If a multipartite access structure is matroid-related, then the corresponding matroid is multipartite for a similar partition. Specifically, we have the following result.

Lemma 5. *Let $\mathcal{M} = (Q, r)$ be a connected matroid and, for a point $p_0 \in Q$, consider the partitions $\Pi = (P_1, \ldots, P_m)$ and $\Pi_0 = (\{p_0\}, P_1, \ldots, P_m)$ of the sets $P = Q - \{p_0\}$ and Q, respectively. Then the matroid-related connected access structure $\Gamma = \Gamma_{p_0}(\mathcal{M})$ on P is Π-partite if and only if the matroid $\mathcal{M} = (Q, r)$ is Π_0-partite.*

The members of a Π-partite family of subsets are determined by the number of elements they have in each part. We formalize this in the following and we obtain a compact way to represent a multipartite family of subsets. Let $\Pi = (X_1, \ldots, X_m)$ be a partition of a set X. For every $A \subseteq X$ and $i \in J_m$, we define $\Pi_i(A) = |A \cap X_i|$. The partition Π defines a mapping $\Pi\colon \mathcal{P}(X) \to \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A), \ldots, \Pi_m(A))$. If a family $\Lambda \subseteq \mathcal{P}(X)$ of subsets is Π-partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda)$. That is, Λ is completely determined by the set of vectors $\Pi(\Lambda) \subset \mathbb{Z}_+^m$, and hence we can describe an m-partite family of subsets by using vectors in $\mathbb{Z}_+^m$. The following result shows the close connection between multipartite matroids and discrete polymatroids. It can be easily proved by using Proposition 4 and the properties of the independent sets of a matroid.

Proposition 6. *Let $\Pi = (Q_1, \ldots, Q_m)$ be an m-partition of a set Q and let $\mathcal{I} \subseteq \mathcal{P}(Q)$ be a Π-partite family of subsets. Then $\mathcal{I}$ is the family of independent sets of a Π-partite matroid $\mathcal{M} = (Q, r)$ if and only if $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is a discrete polymatroid. In addition, if $\mathcal{M} = (Q, r)$ is a Π-partite matroid and $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ is the rank function of the discrete polymatroid $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$, then $h(X) = r(\bigcup_{i \in X} Q_i)$ for every $X \subseteq J_m$.*

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

5 Matroid-Related Multipartite Access Structures

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

For every integer $m \geq 1$, we consider the sets $J_m = \{1, \ldots, m\}$ and $J'_m = \{0, 1, \ldots, m\}$. Let $\mathcal{D} \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m and rank function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$. We say that a discrete polymatroid $\mathcal{D}' \subset \mathbb{Z}_+^{m+1}$ with ground set J'_m *completes* $\mathcal{D}$ if its rank function $h'\colon \mathcal{P}(J'_m) \to \mathbb{Z}$ is such that $h'(X) = h(X)$ for every $X \subseteq J_m$ while $h'(\{0\}) = 1$ and $h'(J'_m) = h(J_m)$.

Since the rank function of $\mathcal{D}'$ is an extension of the one of $\mathcal{D}$, both will be usually denoted by h. For a polymatroid $\mathcal{D}'$ that completes $\mathcal{D}$, consider the family $\Delta(\mathcal{D}') = \{X \subseteq J_m : h(X \cup \{0\}) = h(X)\} \subseteq \mathcal{P}(J_m)$. Given a discrete polymatroid $\mathcal{D}$ with ground set J_m, every completion $\mathcal{D}'$ of $\mathcal{D}$ is determined by $\Delta(\mathcal{D}')$. The next proposition characterizes the families of subsets $\Delta \subseteq \mathcal{P}(J_m)$ for which there exists $\mathcal{D}'$ with $\Delta = \Delta(\mathcal{D}')$. This result will be very useful in the characterization of ideal tripartite access structures.

Proposition 7. *Let $\mathcal{D}$ be a discrete polymatroid with ground set J_m and rank function h. Consider $\Delta \subseteq \mathcal{P}(J_m)$. Then there exists a completion $\mathcal{D}'$ of $\mathcal{D}$ with $\Delta = \Delta(\mathcal{D}')$ if and only if the following conditions are satisfied.*

1. *The family Δ is monotone increasing, $\emptyset \notin \Delta$, and $J_m \in \Delta$.*
2. *If $X \subset Y \subseteq J_m$ and $X \notin \Delta$ while $Y \in \Delta$, then $h(X) < h(Y)$.*
3. *If $X, Y \in \Delta$ and $X \cap Y \notin \Delta$, then $h(X \cup Y) + h(X \cap Y) < h(X) + h(Y)$.*

We say that $\Delta \subseteq \mathcal{P}(J_m)$ is *$\mathcal{D}$-compatible* if it satisfies the conditions in Proposition 7. For every $X \subseteq J_m$, we define the discrete polymatroid $\mathcal{D}(X)$ with ground set X by $\mathcal{D}(X) = \{u(X) : u \in \mathcal{D}\} \subset \mathbb{Z}_+^{|X|}$, and we consider the set of vectors $\mathcal{B}(X) \subset \mathbb{Z}_+^m$ such that $u \in \mathcal{B}(X)$ if and only if $u(X)$ is a basis of $\mathcal{D}(X)$ and $u_i = 0$ for every $i \in J_m - X$. Finally, for a family $\Delta \subseteq \mathcal{P}(J_m)$, we define $\mathcal{G}(\Delta) = \bigcup_{X \in \Delta} \mathcal{B}(X) \subset \mathbb{Z}_+^m$. Our characterization of matroid-related multipartite access structures is given in the following theorem. Since every ideal access structure must be matroid-related, this result provides a necessary condition for a multipartite access structure to be ideal. Moreover, by Theorem 3, this a a necessary condition for a multipartite access structure to admit a secret sharing scheme with information rate greater than 2/3.

Theorem 8. *Let Π be an m-partition of P and let Γ be a connected Π-partite access structure on P. Then Γ is matroid-related if and only if there exist a discrete polymatroid $\mathcal{D}$ with ground set J_m and a $\mathcal{D}$-compatible family $\Delta \subseteq \mathcal{P}(J_m)$ such that*

$$\Gamma = \{A \subseteq P : \Pi(A) \geq u \text{ for some vector } u \in \mathcal{G}(\Delta)\},$$

or, equivalently, the family $\min \Gamma$ *of the minimal qualified subsets of Γ is determined by*

$$\Pi(\min \Gamma) = \bigcup_{X \in \Delta} \{u \in \mathcal{B}(X) : |u(Y)| < h(Y) \text{ for every } Y \in \Delta \text{ with } Y \subsetneq X\},$$

where h is the rank function of the discrete polymatroid $\mathcal{D}$.

Proof. Let $\Pi = (P_1, \ldots, P_m)$ and $\Pi_0 = (\{p_0\}, P_1, \ldots, P_m)$ be partitions of the sets P and $Q = P \cup \{p_0\}$, respectively. Let $\mathcal{M} = (Q, r)$ be a connected Π_0-partite matroid and let $\mathcal{D}' = \Pi_0(\mathcal{I}) \subset \mathbb{Z}_+^{m+1}$ be the discrete polymatroid with ground set J'_m associated with $\mathcal{M}$. Observe that, since $\mathcal{M}$ is connected, $\mathcal{D}'$ completes the discrete polymatroid $\mathcal{D} = \mathcal{D}'(J_m)$. Consider the matroid-related Π-partite access structure $\Gamma_{p_0}(\mathcal{M})$. We only have to prove that a subset $A \subseteq P$ is in $\Gamma_{p_0}(\mathcal{M})$ if and only if $\Pi(A) \geq u$ for some vector $u \in \mathcal{G}(\Delta(\mathcal{D}'))$.

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

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

The condition in Theorem 8 seems very involved and difficult to check. Nevertheless, as we see in the following corollaries and examples, it provides useful tools to check that a given multipartite access structure is not ideal. An important point to be taken into account is that, given a connected matroid-related multipartite access structure Γ, the discrete polymatroid $\mathcal{D}$ and the family of subsets Δ whose existence is proved in Theorem 8 are univocally determined. Effectively, since Γ is connected and matroid-related, there exists a unique matroid $\mathcal{M}$ with $\Gamma = \Gamma_{p_0}(\mathcal{M})$, which determines $\mathcal{D}$ and Δ. Therefore, we can write $\mathcal{D}(\Gamma)$ and $\Delta(\Gamma)$ to represent these objects. For a partition $\Pi = (P_1, \ldots, P_m)$ of a set P, the *support* of a subset $A \subseteq P$ is $\operatorname{supp}(A) = \{i \in J_m : A \cap P_i \neq \emptyset\} \subseteq J_m$. Observe that, if Γ is a matroid-related Π-partite access structure, then $\Delta(\Gamma) = \operatorname{supp}(\Gamma) = \{\operatorname{supp}(A) : A \in \Gamma\}$.

Corollary 9. *Let Γ be a matroid-related m-partite access structure. For every $X \subseteq J_m$, all minimal qualified subsets $A \in \min \Gamma$ with $\operatorname{supp}(A) = X$ have the same cardinality.*

Example 10. Let Γ be a 4-partite access structure with $\Pi(\min \Gamma) = \{(2, 2, 1, 1), (1, 3, 1, 2), (2, 1, 2, 1), (1, 1, 2, 2)\}$. From Corollary 9, Γ is not matroid-related, and hence it is not ideal. Moreover, by Theorem 3, its optimal information rate is at most 2/3.

Corollary 11. *Let Γ be a connected matroid-related m-partite access structure and consider the discrete polymatroid $\mathcal{D} = \mathcal{D}(\Gamma)$ and the $\mathcal{D}$-compatible family $\Delta = \Delta(\Gamma)$. Let h be the rank function of $\mathcal{D}$. For every $X \in \Delta$ and $A \subseteq \bigcup_{i\in X} P_i$, if $|A| = h(X)$ and $|A \cap (\bigcup_{i\in Y} P_i)| \le h(Y)$ for all $Y \subseteq X$, then $A \in \Gamma$.*

Example 12. Let Γ be a quadripartite access structure such that

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

We claim that Γ is not matroid-related. Assume the Γ is matroid-related and consider $\mathcal{D} = \mathcal{D}(\Gamma)$ and $\Delta = \Delta(\Gamma)$. Observe that $\min \Delta = \{\{1\}\}$. In addition, from Theorem 8, if $u \in \mathcal{B}(J_4)$, then $u \in \Pi(\min \Gamma)$ or there exist $Y \subsetneq J_4$ and $v \in \mathcal{B}(Y)$ such that $v < u$ and $v \in \Pi(\min \Gamma)$. Therefore, the family of bases of $\mathcal{D}$ is $\mathcal{B} = \mathcal{B}(J_4) = \{u \in \mathbb{Z}_+^4 \,:\, (1,1,1,1) \le u \le (4,4,4,4) \text{ and } |u| = 8\}$. Moreover, $h(X) = \max\{|u(X)| \,:\, u \in \mathcal{D}\} = \max\{|u(X)| \,:\, u \in \mathcal{B}\}$ for every $X \subseteq J_4$. Therefore, $h(X) = 4$ if $|X| = 1$, and $h(X) = 6$ if $|X| = 2$, and $h(X) = 7$ if $|X| = 3$, and $h(J_4) = 8$. Since $\{1,2\} \in \Delta$, by Corollary 11, $(3,3,0,0) \in \Pi(\Gamma)$, a contradiction.

6 Representable Multipartite Matroids

Let $\mathbb{K}$ be a field, E a $\mathbb{K}$-vector space, and $V_1, \dots, V_m$ subspaces of E. It is not difficult to check that the mapping $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i\in X} V_i)$ is the rank function of a discrete polymatroid $\mathcal{D} \subset \mathbb{Z}_+^m$. In this situation, we say that $\mathcal{D}$ is $\mathbb{K}$*-linearly representable* and the subspaces $V_1, \dots, V_m$ are a $\mathbb{K}$*-linear representation* of $\mathcal{D}$. The main result of this section is the following theorem.

Theorem 13. *Let $\mathcal{M} = (Q, r)$ be a Π-partite matroid such that $|Q| = n$ and $r(\mathcal{M}) = k$. Let $\mathcal{D} = \Pi(\mathcal{I})$ be its associated discrete polymatroid. If $\mathcal{M}$ is $\mathbb{K}$-linearly representable, then so is $\mathcal{D}$. In addition, if $\mathcal{D}$ is $\mathbb{K}$-representable, then $\mathcal{M}$ is $\mathbb{L}$-linearly representable for every field extension $\mathbb{L}$ of $\mathbb{K}$ such that $|\mathbb{L}| > \binom{n}{k} \cdot k$.*

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

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

Assume that $|\mathbb{K}| > \binom{n}{k} \cdot k$ and that $\mathcal{D}$ is $\mathbb{K}$-linearly representable. Then there exists a $\mathbb{K}$-linear representation of $\mathcal{D}$ consisting of subspaces $V_1, \dots, V_m$ of the

$\mathbb{K}$-vector space $E = \mathbb{K}^k$, where $k = h(J_m) = r(\mathcal{M})$. The proof of the following lemma is not given here due to space limitations. It will be included in the full version of the paper.

Lemma 14. *For every basis u of $\mathcal{D}$, there exists a basis $B = B_1 \cup \cdots \cup B_m$ of the vector space E such that $B_i \subset V_i$ and $|B_i| = u_i$ for every $i \in J_m$, and $B_i \cap B_j = \emptyset$ if $i \neq j$.*

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

Lemma 15. *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 $A \cap (\cup_{j \in X} Q_j)$ must be linearly dependent. □

Therefore, Lemma 17 concludes the proof of Theorem 13. 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 16. *Let $p \in \mathbb{K}[X_1, \ldots, X_N]$ be a nonzero polynomial on N variables of degree $d < |\mathbb{K}|$. Then, there exists a point $(x_1, \ldots, x_N)$ in $\mathbb{K}^N$ such that $p(x_1, \ldots, x_N) \neq 0$.*

Lemma 17. *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 $\phi_i \colon \mathbb{K}^{k_i} \to V_i \subseteq \mathbb{K}^k$. Let $N = \sum_{i=1}^m k_i n_i$. By using the mappings ϕ_i, we can construct a one-to-one mapping $\Psi \colon \mathbb{K}^N = (\mathbb{K}^{k_1})^{n_1} \times \cdots \times (\mathbb{K}^{k_m})^{n_m} \to \mathbf{M}$. 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 $f_B \colon \mathbb{K}^N \to \mathbb{K}$ 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 of degree k, because every entry of the matrix $\Psi(\mathbf{x})_B$ is linear, that 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 14, there exists a basis of $\mathbb{K}^k$ of the form $\widetilde{B} = B_1 \cup \cdots \cup B_m$ with $B_i \subset V_i$ 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 of degree at most $\binom{n}{k} \cdot k < |\mathbb{K}|$, because $|\mathcal{B}(\mathcal{M})| \leq \binom{n}{k}$. From Lemma 16, 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. $\square$

7 Tripartite Access Structures

In this section, we apply our general results on ideal multipartite access structures to completely characterize the ideal tripartite access structures. The characterization of ideal bipartite access structures was done previously in [28], but only partial results [2, 10, 12] were known about the tripartite case.

We begin by characterizing the matroid-related tripartite access structures. Afterwards, we prove that all matroids related to those access structures are representable. Therefore, all matroid-related tripartite access structures are vector space access structures, and hence ideal. We obtain in this way a characterization of the ideal tripartite access structures. In addition, as a consequence of Theorem 3, the optimal information rate of every non-ideal tripartite access structure is at most 2/3.

7.1 Characterizing Matroid-Related Tripartite Access Structures

The values of a rank function $h\colon \mathcal{P}(J_3) \to \mathbb{Z}$ of a discrete polymatroid $\mathcal{D}$ with ground set J_3 will be denoted by $r_i = h(\{i\})$, where $i \in J_3$, and $s_i = h(\{j,k\})$ if $\{i,j,k\} = J_3$, and $s = h(J_3)$. Given integer values r_i, s_i, and s, they univocally determine a discrete polymatroid with ground set J_3 if and only if, for every i,j,k with $\{i,j,k\} = J_3$,

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

Let $\mathcal{D}$ be a discrete polymatroid with ground set J_3. From Proposition 7, a family $\Delta \subseteq \mathcal{P}(J_3)$ is $\mathcal{D}$-compatible if and only if the following conditions are satisfied for every i,j,k with $\{i,j,k\} = J_3$.

1. Δ is monotone increasing, $\emptyset \notin \Delta$, and $J_3 \in \Delta$.
2. $r_i > 0$ if $\{i\} \in \Delta$, and $r_i < s_j$ if $\{i\} \notin \Delta$ and $\{i,k\} \in \Delta$, and $s_i < s$ if $\{j,k\} \notin \Delta$.
3. $s_i < r_j + r_k$ if $\{\{j\},\{k\}\} \subset \Delta$.
4. $s + r_i < s_j + s_k$ if $\{i\} \notin \Delta$ and $\{\{i,j\},\{i,k\}\} \subset \Delta$.
5. $s < s_i + r_i$ if $\{\{i\},\{j,k\}\} \subset \Delta$.

From Theorem 8, a tripartite access structure Γ is matroid-related if and only if there exist integers r_i, s_i, s and a family $\Delta \subseteq J_3$ in the above conditions such that a subset $A \subseteq P$ is in Γ if and only if $\Pi(A) \geq u$ for some $u \in \bigcup_{X \in \Delta} \mathcal{B}(X)$, where

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

and the other sets $\mathcal{B}(X)$ are defined symmetrically.

7.2 All Matroid-Related Tripartite Access Structures Are Ideal

Let $\mathcal{D}$ be a discrete 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 $\mathcal{D}$, 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 $\mathcal{D}$. That is, there can exist different representations of $\mathcal{D}$ with different values of t. Nevertheless, there exist some restrictions on this value. Of course, $t \leq t_i$ for every $i \in J_3$. In addition, since $(V_1 \cap V_3) + (V_2 \cap V_3) \subseteq (V_1 + V_2) \cap V_3$, we have that $\dim((V_1 + V_2) \cap V_3) - \dim((V_1 \cap V_3) + (V_2 \cap V_3)) = \sum s_i - \sum r_i - (s - t) \geq 0$. Therefore, $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$. The proof of the following result will appear in the full version of the paper.

Proposition 18. *Let $\mathcal{D}$ be a discrete polymatroid with ground set J_3. Consider an integer t such that $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$ and take $\ell = \sum s_i - \sum r_i - (s - t)$. Let $\mathbb{K}$ be a field with $|\mathbb{K}| > s_3 + \ell$. Then there exists a $\mathbb{K}$-representation of $\mathcal{D}$ given by subspaces $V_1, V_2, V_3 \subseteq E = \mathbb{K}^s$ with $\dim(V_1 \cap V_2 \cap V_3) = t$.*

As a consequence of Proposition 18, every discrete polymatroid with ground set J_m with $m \leq 3$ is representable over fields of all characteristics. This and Theorem 13 implies that every m-partite matroid with $m \leq 3$ is representable over fields of all characteristics.

Theorem 19 concludes the characterization of ideal tripartite access structures. This result is not a direct consequence of Proposition 18, because the matroids that define tripartite access structures are in general quadripartite, being one of the parts formed by a single point. Therefore, Theorem 19 is proved by showing that every discrete polymatroid $\mathcal{D}'$ with ground set J_3' and $h(\{p_0\}) = 1$ is linearly representable over finite fields of every characteristic. We sketch in the following the proof of this fact. First, a linear representation of the discrete polymatroid $\mathcal{D} = \mathcal{D}'(J_3)$, whose existence is given by Proposition 18, is considered. Afterwards, we have to check that it is possible to find a vector $\mathbf{x}_0$ such that the subspace $V_0 = \langle \mathbf{x}_0 \rangle$, together with the subspaces V_1, V_2, V_3 representing $\mathcal{D} = \mathcal{D}'(J_3)$, form a linear representation of $\mathcal{D}'$. This is done by a case-by-case analysis depending on the family $\Delta(\mathcal{D}')$, and in every case a suitable representation of $\mathcal{D}$ has to be chosen.

Theorem 19. *Every matroid-related tripartite access structure is ideal. More specifically, every matroid-related tripartite access structure is a vector space access structure over finite fields of all positive characteristics.*

Example 20. We prove that the tripartite access structure Γ with

$$\Pi(\min \Gamma) = \{(3,0,0),(2,0,4),(2,4,2),(2,3,3),(1,4,3),(1,3,4)\}.$$

is ideal. Assuming that this is so, we determine $\mathcal{D} = \mathcal{D}(\Gamma)$ and $\Delta = \Delta(\Gamma)$. Observe that $\Delta = \operatorname{supp}(\Gamma) = \{\{1\},\{1,2\},\{1,3\},J_3\}$, and hence $\Pi(\min \Gamma) \subseteq \mathcal{B}(\{1\}) \cup \mathcal{B}(\{1,2\}) \cup \mathcal{B}(\{1,3\}) \cup \mathcal{B}(J_3)$. It is easy to see that $r_1 = 3$, $r_2 = r_3 = 4$, $s_2 = 6$ and $s = 8$. Since there is not any minimal subset in $\mathcal{B}(\{1,2\})$, it follows that $\mathcal{B}(\{1,2\})$ has only one element $(s_3 - r_2, r_2, 0) = (r_1, s_3 - r_1, 0)$, which does not correspond to any minimal qualified subset, and hence $s_3 = 7$. All subsets in $\mathcal{B}(J_3)$ have at least one participant in the first partition, so $s - s_1 = 1$ and $s_1 = 7$. Since the parameters satisfy the above restrictions and Γ coincides with the access structure determined by these parameters, Γ is a matroid-related access structure. Therefore, it is a vector space access structure by Theorem 19.

References

1. A. Beimel, N. Livne. On Matroids and Non-ideal Secret Sharing. *Third Theory of Cryptography Conference, TCC 2006. Lecture Notes in Comput. Sci.* **3876** (2006) 482–501.
2. A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Comput. Sci.* **3378** (2005) 600–619.
3. J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88. Lecture Notes in Comput. Sci.* **403** (1990) 27–35.
4. G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.* **48** (1979) 313–317.
5. C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptogr.* **11** (1997) 107–122.
6. C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology, CRYPTO'92. Lecture Notes in Comput. Sci.* **740** (1993) 148–167.
7. E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.
8. E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.
9. R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. Cryptology* **6** (1993) 157–168.
10. M.J. Collins. A Note on Ideal Tripartite Access Structures. *Cryptology ePrint Archive*, Report **2002/193**, http://eprint.iacr.org/2002/193.
11. L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.
12. J. Herranz, G. Sáez. New Results on Multipartite Access Structures. *IEE Proceedings on Information Security* **153** (2006) 153–162.
13. J. Herzog, T. Hibi. Discrete polymatroids. *J. Algebraic Combin.* **16** (2002) 239–268.
14. M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.* (1987) 99–102.
15. W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286.

16. E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.
17. A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725.
18. J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes Cryptogr.* **34** (2005) 17–34.
19. J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics* **154** (2006) 552–563.
20. J.Martí-Farré, C. Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Fifth Conference on Security and Cryptography for Networks, SCN 2006, Lecture Notes in Comput. Sci.*, **4116** (2006) 201–215.
21. J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Comput. Sci.* **4392** (2007) 273–290.
22. F. Matúš. Matroid representations by partitions. *Discrete Math.* **203** (1999) 169–194.
23. P. Morillo, C. Padró, G. Sáez, J. L. Villar. Weighted Threshold Secret Sharing Schemes. *Inf. Process. Lett.* **70** (1999) 211–216.
24. S.-L. Ng. A Representation of a Family of Secret Sharing Matroids. *Des. Codes Cryptogr.* **30** (2003) 5–19.
25. S.-L. Ng. Ideal secret sharing schemes with multipartite access structures. *IEE Proc.-Commun.* **153** (2006) 165–168.
26. S.-L. Ng, M. Walker. On the composition of matroids and ideal secret sharing schemes. *Des. Codes Cryptogr.* **24** (2001) 49–67.
27. J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
28. C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604.
29. P.D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.
30. P.D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B*, **56** (1992) pp. 69–73.
31. A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.
32. G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO'88, Lecture Notes in Comput. Sci.* **403** (1990) 390–448.
33. J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) pp. 179–197.
34. D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.
35. T. Tassa. Hierarchical Threshold Secret Sharing. *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004. Lecture Notes in Comput. Sci.* **2951** (2004) 473–490.
36. T. Tassa, N. Dyn. Multipartite Secret Sharing by Bivariate Interpolation. *33rd International Colloquium on Automata, Languages and Programming, ICALP 2006 – Lecture Notes in Comput. Sci.* **4052** (2006) 288–299.
37. D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.