Ideal Multipartite Secret Sharing Schemes *

Oriol Farràs, Jaume Martí-Farré, Carles Padró
Dep. de Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, Barcelona

September 3, 2006

Abstract

The characterization of the access structures of ideal secret sharing schemes is one of the main open problems in secret sharing. Because of its difficulty, it has been studied for several particular families of access structures. In this paper, we deal with multipartite access structures, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role. Some particular classes of multipartite structures have been studied in seminal works on secret sharing by Shamir, Simmons, and Brickell, and also recently by several authors. In this work, the characterization of ideal multipartite access structures is studied with all generality. Actually, every access structure is multipartite and, hence, the results in this paper can be seen as an attack under a different point of view to the general open of the characterization of ideal access structures. Namely, we present some necessary conditions and some sufficient conditions for an access structure to be ideal in terms of the classification of its participants into equivalence classes. These conditions can be specially useful if the number of classes is small or these classes are distributed in some special way. More specifically, our results are the following:

1. We present a characterization of matroid-related multipartite access structures in terms of discrete polymatroids. To do that, we study the relation between multipartite matroids and discrete polymatroids. As a consequence of this characterization, a necessary condition for a multipartite access structure to be ideal is obtained.
2. We use a special class of discrete polymatroids, the linearly representable ones, to characterize the representable multipartite matroids. In this way we obtain a sufficient condition for a multipartite access structure to be ideal.
3. We apply those general results to obtain a complete characterization of ideal tripartite access structures, which was until now an open problem. In particular, we prove that the matroid-related tripartite access structures coincide with the ideal ones.

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

*This work was partially supported by the Spanish Ministry of Education and Science under project TIC 2003-00866. This work was done 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.

1 Introduction

Secret sharing schemes were introduced independently by Shamir [33] and Blakley [3] in 1979. 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 a non-qualified set do not provide any information about the secret value.

The length of the shares is the main measure of the complexity of secret sharing schemes. In all schemes, the length of every share is at least the length of the secret [17]. If all shares have the same length as the secret, the scheme is said to be *ideal*. There exists a secret sharing scheme for every access structure [15], but, in general, the shares must be much larger than the secret [12]. An access structure is said to be *ideal* if it admits an ideal secret sharing scheme.

This paper deals with the characterization of ideal access structures, which is one of the main open problems in secret sharing and has important connections with matroid theory.

For a matroid $\mathcal{M}$ with ground set Q 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 determining its minimal qualified subsets:

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

The access structures of this form are called *matroid-related*. 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 $\Gamma_{p_0}(\mathcal{M})$.

A necessary condition for an access structure to be ideal was given by Brickell and Davenport [8], who proved that every ideal access structure is matroid-related. 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 $\Gamma_{p_0}(\mathcal{M})$.

Matroids that are obtained from ideal secret sharing schemes are said to be *secret sharing representable* (or *ss-representable* for short). Since there exist non-ss-representable matroids [24, 32], that necessary condition is not sufficient. Nevertheless, as a consequence of the results in [7], all linearly representable matroids are ss-representable. This implies a sufficient condition for an access structure to be ideal. Namely, an access structure is ideal if it is related to a linearly representable matroid.

Due to the difficulty of finding general results on the characterization of ideal access structures, a number of works, which we enumerate later, have appeared dealing with the restriction of this open problem to several particular classes of access structures.

In this paper, we study the characterization of ideal multipartite access structures. Informally, an access structure is *multipartite* if its set of participants can be divided into several parts in such a way that all participants in the same part play an equivalent role in the structure. Because of its practical interest, secret sharing for multipartite access structures has been studied by several authors.

Since we can always consider as many parts as participants, every access structure is multipartite. More accurately, we can consider in any access structure the partition that is derived from a suitable equivalence relation on the set of participants. Therefore, we are not restricting ourselves to a family of access structures, but we study the characterization of ideal access structures under a different point of view. Specifically, we investigate the above conditions by taking into account that there can be participants playing equivalent roles in the structure. We obtain in this way a new necessary condition and a new sufficient condition for an access structure to be ideal in terms of the classification of its participants into equivalence classes.

Our results can be applied to any access structure and, hence, they can be viewed as a new contribution to the open problem of the characterization of ideal access structures. Nevertheless, the most interesting consequences of our results are obtained when applied to some particular families of access structures. In particular, we present a complete characterization of the ideal tripartite access structures, which was an open question until now.

2 Related Work

The relation between ideal secret sharing schemes and matroids discovered by Brickell and Davenport [8] have led to a number of works dealing with the characterization of ss-representable matroids. The Vamos matroid was the first matroid that was proved to be non-ss-representable. This was done by Seymour [32] and a shorter proof was given later by Simonis and Ashikhmin [35]. Many other examples have been given by Matúš [24]. The results by Brickell [7] imply that all representable matroids (that is, matroids that can be represented by a matrix over some finite field) are ss-representable. The first example of a ss-representable matroid that is not representable, the non-Pappus matroid, was presented in [35]. This matroid can be represented by an ideal *linear* secret sharing scheme. The matroids with this property are said to be *multilinearly representable*, a class that includes the representable matroids. The existence of ss-representable matroids that are not multilinearly representable is an open question.

The minimal qualified subsets of a matroid-related access structure form a *matroid port*, a combinatorial object introduced by Lehman [18] in 1964, much before secret sharing was invented. Seymour [31] 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 [22]. The main result in [22] is a generalization of the result by Brickell and Davenport [8]. Namely, if the *information rate* (that is, the ratio between the length of the secret and the maximum length of the shares) of a secret sharing scheme is greater than $2/3$, then its access structure is matroid-related.

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 [36] and five [16] participants, the access structures defined by graphs [4, 5, 6, 8, 10], the bipartite access structures [30], the access structures with three or four minimal qualified subsets [20], the access structures with intersection

number equal to one [21], the access structures with rank three [19, 23], and the weighted threshold access structures [2]. In all 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 the results in [22], 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 [33] in his seminal work, in which weighted threshold access structures were considered. These structures have been studied also in [25, 30] 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, called *multilevel* and *compartmented*, that had been previously considered by Simmons [34]. Other constructions of ideal schemes for these and other multipartite structures have been presented in [13, 27, 37, 38], where some complexity issues related to the construction of those ideal schemes are studied. A complete characterization of ideal bipartite access structures was given in [30] and, independently, in [26, 28]. Partial results on the characterization of ideal tripartite access structures have been presented in [2, 11, 13]. The first attempt to provide general results on the characterization of ideal multipartite access structures has been made recently by Herranz and Sáez [13]. They present some necessary conditions for a multipartite access structure to be ideal, which generalize the ones given in [11] for the tripartite case. In addition, they present a wide family of ideal tripartite access structures.

3 Our Results

This paper deals with the characterization of ideal multipartite access structures. Since every access structure is multipartite, the problem we consider in this paper is actually the characterization of ideal access structures in general. Therefore, this work can be seen as a new attack to this long-standing open problem under a different point of view. Our main contributions can be divided into three parts.

First, a characterization of matroid-related multipartite access structures, which implies a necessary condition for a multipartite access structure to be ideal. The partition in the set of participants of a matroid-related multipartite 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, which are a particular class of polymatroids, were introduced by Herzog and Hibi [14]. By using discrete polymatroids, we present in Theorem 6.2 a characterization of matroid-related multipartite access structures.

Second, a necessary and sufficient condition for a multipartite matroid to be representable, which implies a sufficient condition for a multipartite access structure to be ideal. Linear representations of matroids are obtained by assigning a vector to every point. If, instead of a vector, we assign a subspace to every point, we will obtain a linear representation of a discrete polymatroid. We prove in Theorem 7.1 that a mul-

tipartite matroid is representable if and only if the corresponding discrete polymatroid is representable. We think that this theorem 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.

And third, the application of the general results to the tripartite case, by means of which a complete characterization of tripartite access structures is obtained. By using Theorem 6.2, we characterize the matroid-related tripartite access structures. Theorem 7.1 is used to prove that all matroids related to these structures are representable and, hence, that all matroid-related tripartite access structures are ideal. Moreover, as a consequence of the results in [22], the information rate of every non-ideal tripartite access structure is at most 2/3. We observe that these results cannot be extended to quadripartite access structures, because the Vamos matroid is quadripartite and it is not ss-representable. Hence, there exist matroid-related quadripartite access structures that are not ideal.

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. For instance, which discrete polymatroids are representable?

The size of the field and the number of checks for linear independence are important efficiency issues when constructing actual ideal schemes for ideal multipartite access structures. Such issues have been studied for several particular families of multipartite access structures [2, 27, 30, 37, 38]. The proof of our sufficient condition for a multipartite access structure to be ideal is purely existential and it does not give many hints about those complexity questions, whose analysis in the general case is deferred to future work.

4 Matroids and Ideal Secret Sharing Schemes

The reader is referred to [36] for an introduction to secret sharing and to [29, 39] for general references on Matroid Theory.

A *matroid* $\mathcal{M} = (Q, \mathcal{I})$ is formed by a finite set Q together with a family $\mathcal{I}$ of subsets of Q such that

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

The set Q is the *ground set* of the matroid $\mathcal{M}$ and the elements of $\mathcal{I}$ are called the *independent sets* of $\mathcal{M}$. The *bases* of the matroid are the maximally independent sets. The family $\mathcal{B}$ of the bases determines the matroid. Moreover, by [29, Theorem 1.2.5], $\mathcal{B} \subseteq \mathcal{P}(Q)$ is the family of bases of a matroid on Q if and only if

1. $\mathcal{B}$ is nonempty, and

2. 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 $r(\mathcal{M})$. The *dependent* sets are those that are not independent. A *circuit* is a minimally dependent subset. A matroid is said to be *connected* if, for every two points $x, y \in Q$, there exists a circuit C with $x, y \in C$. The *rank* of $X \subseteq Q$, which is denoted $r(X)$, is the maximum cardinality of the subsets of X that are independent. Observe that the rank of Q is the rank of the matroid $\mathcal{M}$ that was defined before. The *rank function* $r\colon \mathcal{P}(Q) \to \mathbb{Z}$ of a matroid satisfies

1. $0 \leq r(X) \leq |X|$ for every $X \subseteq Q$, and

2. r is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $r(X) \leq r(Y)$, and

3. r is *submodular*: $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$ for every pair of subsets X, Y of Q.

Moreover, every function $r\colon \mathcal{P}(Q) \to \mathbb{Z}$ satisfying these properties is the rank function of a matroid [29, Theorem 1.3.2].

Let $\mathbb{K}$ be a field. A matroid $\mathcal{M} = (Q, \mathcal{I})$ is $\mathbb{K}$-*representable* if there exists a matrix M over $\mathbb{K}$ whose columns are indexed by the elements of Q such that a subset $I = \{i_1, \ldots, i_k\} \subseteq Q$ is independent if and only if the corresponding columns of M are independent. In this situation, we say that the matrix M is a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$.

Let Q be a finite set of *participants* and $p_0 \in Q$ a special participant called *dealer*. Let E be a finite set with a probability distribution on it and, for every $i \in Q$, consider a finite set E_i and a surjective mapping $\pi_i\colon E \to E_i$. Those mappings induce random variables on the sets E_i. We notate $H(E_i)$ for the Shannon entropy of those random variables. For a subset $A = \{i_1, \ldots, i_r\} \subseteq Q$, we write $H(A)$ for the joint entropy $H(E_{i_1} \ldots E_{i_r})$, and a similar convention is used for conditional entropies as, for instance, in $H(E_j|A) = H(E_j|E_{i_1} \ldots E_{i_r})$. The mappings π_i define a *secret sharing scheme* Σ with *access structure* Γ on the set $P = Q - \{p_0\}$ of participants if $H(E_{p_0}) > 0$ and $H(E_{p_0}|A) = 0$ if $A \in \Gamma$ while $H(E_{p_0}|A) = H(E_{p_0})$ if $A \notin \Gamma$. In that situation, every random choice of an element $\mathbf{x} \in E$, according to the given probability distribution, results in a *distribution of shares* $((s_i)_{i \in P}, s)$, where $s_i = \pi_i(\mathbf{x}) \in E_i$ is the *share* of the participant $i \in P$ and $s = \pi_{p_0}(\mathbf{x}) \in E_{p_0}$ is the *shared secret value*.

The ratio $\rho(\Sigma) = H(E_{p_0})/(\max_{i \in P} H(E_i))$ is called the *information rate* of the scheme Σ, and the *optimal information rate* $\rho(\Gamma)$ of the access structure Γ is the supremum of the information rates of all secret sharing schemes with access structure Γ. It is not difficult to check that $H(E_i) \geq H(E_{p_0})$ for every $i \in P$ and, hence, $\rho(\Sigma) \leq 1$. Secret sharing schemes with $\rho(\Sigma) = 1$ are said to be *ideal* and their access structures are called *ideal* as well. Of course, $\rho(\Gamma) = 1$ for every ideal access structure Γ.

If Σ is an ideal secret sharing scheme, then there exists $r_0 > 0$ such that $H(E_i) = r_0$ for every $i \in Q$. Brickell and Davenport [8] proved that the mapping $r\colon \mathcal{P}(Q) \to \mathbb{R}$

defined by $r(A) = H(A)/r_0$ is the rank function of a matroid $\mathcal{M} = \mathcal{M}(\Sigma)$. In particular, $r(A)$ is a positive integer for every $A \subseteq Q$. The access structure Γ of the scheme Σ is formed by the subsets $A \subseteq P$ with $r(A \cup \{p_0\}) = r(A)$ and, hence, $\Gamma = \Gamma_{p_0}(\mathcal{M})$. A matroid $\mathcal{M}$ is said to be *secret sharing representable* (or *ss-representable* for short) if $\mathcal{M} = \mathcal{M}(\Sigma)$ for some ideal secret sharing scheme Σ.

Let $\mathbb{K}$ be a finite field and let $\mathcal{M} = (Q, \mathcal{I})$ be a $\mathbb{K}$-representable matroid. For every $k \times (n+1)$ matrix M representing $\mathcal{M}$ over $\mathbb{K}$, the linear mappings $\pi_i \colon E = \mathbb{K}^k \to E_i = \mathbb{K}$ defined by the columns of M define an ideal secret sharing scheme with access structure $\Gamma_{p_0}(\mathcal{M})$. Therefore, the access structures that are related to representable matroids are ideal.

5 Multipartite Access Structures, Multipartite Matroids, and Discrete Polymatroids

We write $\mathcal{P}(P)$ for the power set of the set P. An *m-partition* $\Pi = \{P_1, \ldots, P_m\}$ of a set P is a disjoint family of m nonempty subsets of P with $P = P_1 \cup \cdots \cup P_m$. Let $\Lambda \subseteq \mathcal{P}(P)$ be a family of subsets of P. For a permutation σ on P, we define $\sigma(\Lambda) = \{\sigma(A) : A \in \Lambda\} \subseteq \mathcal{P}(P)$. A family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is said to be *Π-partite* if $\sigma(\Lambda) = \Lambda$ for every permutation σ such that $\sigma(P_i) = P_i$ for every $P_i \in \Pi$. 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, which are actually families of subsets, and they can be applied as well to the family of independent sets of a matroid. A matroid $\mathcal{M} = (Q, \mathcal{I})$ is *Π-partite* if $\mathcal{I} \subseteq \mathcal{P}(Q)$ is Π-partite.

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

The partition Π' is a *refinement* of the partition Π if every set in Π' is a subset of some set in Π. Clearly, if $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite and Π' is a refinement of Π, then Λ is Π'-partite. Among all partitions Π for which a family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite, there exists a partition Π_Λ that is not a refinement of any other such partition. Following [13], we consider the following equivalence relation: two elements $p, q \in P$ are said to be *equivalent according to* Λ if the transposition τ_{pq} satisfies $\tau_{pq}(\Lambda) = \Lambda$. The partition Π_Λ is the one defined by this equivalence relation. It is not difficult to check that Λ is Π-partite if and only if Π is a refinement of Π_Λ.

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 $i \in J_m$. For a partition $\Pi = \{P_1, \ldots, P_m\}$ of a set P and for every $A \subseteq P$ and $i \in J_m$, we define $\Pi_i(A) = |A \cap P_i|$. Then the partition Π defines a mapping $\Pi \colon \mathcal{P}(P) \to \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A), \ldots, \Pi_m(A))$. If $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda)$. That is, Λ is completely determined by the partition Π and the set of vectors $\Pi(\Lambda) \subset \mathbb{Z}_+^m$.

Discrete polymatroids, a combinatorial object introduced by Herzog and Hibi [14], are closely related to multipartite matroids and, because of that, they play an important

role in the characterization of ideal multipartite access structures. Before giving the definition of discrete polymatroid, we need to introduce some notation. 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* on the *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 $u < w \leq u \vee v$.

The next proposition, which is easily proved from the axioms of the independent sets of a matroid, shows the relation between multipartite matroids and discrete polymatroids.

Proposition 5.1. *Let Π be a 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 the independent sets of a Π-partite matroid $\mathcal{M} = (Q, \mathcal{I})$ if and only if $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is a discrete polymatroid.*

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, a discrete polymatroid is determined by its bases. Specifically, the following result is proved in [14, Theorem 2.3].

Proposition 5.2. *A nonempty subset $\mathcal{B} \subset \mathbb{Z}_+^m$ is the family of bases of a discrete polymatroid if and only if it satisfies:*

1. *all elements in $\mathcal{B}$ have the same modulus, and*
2. *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 *rank function* of a discrete polymatroid $\mathcal{D}$ with ground set J_m is the function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \max\{|u(X)| : u \in \mathcal{D}\}$. The next proposition is a consequence of [14, Theorem 3.4].

Proposition 5.3. *A function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ is the rank function of a discrete polymatroid with ground set J_m if and only if it satisfies*

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

Moreover, a polymatroid $\mathcal{D}$ is completely determined by its rank function. Specifically, $\mathcal{D} = \{u \in \mathbb{Z}_+^m : |u(X)| \leq h(X) \text{ for all } X \subseteq J_m\}$.

For a discrete polymatroid $\mathcal{D}$ with ground set J_m and for every $X \subseteq J_m$, we define the discrete polymatroid $\mathcal{D}(X)$ with ground set X by $\mathcal{D}(X) = \{u(X) : u \in \mathcal{D}\} \subset \mathbb{Z}_+^{|X|}$.

6 A Characterization of Matroid-Related Multipartite Access Structures

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 $h'(J'_m) = h'(J_m)$. In particular, $\mathcal{D}(J'_m) = \mathcal{D}$. 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 $\Delta = \Delta(\mathcal{D}') = \{X \subseteq J_m : h(X \cup \{0\}) = h(X)\} \subseteq \mathcal{P}(J_m)$. Observe that Δ is monotone increasing. Effectively, if $X \in \Delta$ and $X \subseteq Y$, then $h(X) + h(Y) = h(X \cup \{0\}) + h(Y) \geq h(Y \cup \{0\}) + h(X)$ and, hence, $Y \in \Delta$.

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 6.1. *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 $h(X \cup Y) + h(X \cap Y) < h(X) + h(Y)$.*

Proof. Let $h'\colon \mathcal{P}(J'_m) \to \mathbb{Z}$ be the only extension of h such that, if $X \subseteq J_m$, then $h'(X \cup \{0\}) = h(X)$ if $X \in \Delta$ and $h'(X \cup \{0\}) = h(X) + 1$ otherwise. Then $\Delta = \Delta(\mathcal{D}')$ for some completion $\mathcal{D}'$ of $\mathcal{D}$ if and only if h' is monotone increasing and submodular, $h'(\{0\}) = 1$, and $h'(J'_m) = h(J_m)$. These conditions are equivalent to the ones in the statement. □

We say that $\Delta \subseteq \mathcal{P}(J_m)$ is *$\mathcal{D}$-compatible* if it satisfies the conditions in Proposition 6.1. For every $X \subseteq J_m$ 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 $\mathcal{G}(\Delta) = \bigcup_{X \in \Delta} \mathcal{B}(X) \subset \mathbb{Z}_+^m$.

Theorem 6.2. *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*

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

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 $\mathcal{M} = (Q, \mathcal{I})$ 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 induced

by $\mathcal{M}$. 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 $\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : \Pi(A) \geq u \text{ for some vector } u \in \mathcal{G}(\Delta(\mathcal{D}'))\}$.

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, $X \in \Delta(\mathcal{D}')$. □

As a consequence, a necessary condition for an m-partite access structure to be matroid-related is obtained. It is a generalization of a result conjectured, but not proved, in [13]. The *support* of $A \subseteq P$ is defined as $\operatorname{supp}(A) = \{i \in J_m : A \cap P_i \neq \emptyset\}$.

Proposition 6.3. *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.*

7 Representable Multipartite Matroids

Let $\mathbb{K}$ be a field, E a $\mathbb{K}$-vector space, and $V_1, \ldots, V_m$ 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 *$\mathbb{K}$-representable* and the subspaces $V_1, \ldots, V_m$ are a *$\mathbb{K}$-representation* of $\mathcal{D}$. The main goal of this section is to prove the following result.

Theorem 7.1. *Let $\mathcal{M} = (Q, \mathcal{I})$ be a Π-partite matroid and let $\mathcal{D} = \Pi(\mathcal{I})$ be its associated discrete polymatroid. If $\mathcal{M}$ is $\mathbb{K}$-representable, then so is $\mathcal{D}$. In addition, if $\mathcal{D}$ is $\mathbb{K}$-representable, then $\mathcal{M}$ is representable over some finite extension of $\mathbb{K}$.*

Let $\Pi = (Q_1, \ldots, Q_r)$ be a partition of Q and let $\mathcal{M} = (Q, \mathcal{I})$ be a Π-partite matroid. Consider the discrete polymatroid $\mathcal{D} = \Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ and its rank function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$.

We begin by proving the first claim in the statement of Theorem 7.1. Suppose that $\mathcal{M}$ is represented over the field $\mathbb{K}$ by a matrix M. For every $i \in J_m$, consider the subspace V_i spanned by the columns of M corresponding to the points in Q_i. Then $h(X) = r(\cup_{i\in X} Q_i) = \dim(\sum_{i\in X} V_i)$ for every $X \subseteq J_m$. Therefore, the subspaces $V_1, \ldots, V_m$ are a $\mathbb{K}$-representation of the discrete polymatroid $\mathcal{D}$.

The proof for the second claim in the theorem is much more involved and needs several partial results. Assume now that the discrete polymatroid $\mathcal{D} = \Pi(\mathcal{I})$ is $\mathbb{K}$-representable. Then there exists a $\mathbb{K}$-representation of $\mathcal{D}$ consisting of subspaces $V_1, \ldots, V_m$ of the $\mathbb{K}$-vector space $E = \mathbb{K}^s$, where $s = h(J_m) = r(\mathcal{M})$. Consider the subset $\widetilde{\mathcal{D}} \subset \mathbb{Z}_+^m$ defined in the following way: an integer vector $u \in \mathbb{Z}_+^m$ is in $\widetilde{\mathcal{D}}$ if and only if there exists a sequence $(A_1, \ldots, A_m)$ of subsets of E such that

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

Lemma 7.2. *In this situation, $\widetilde{\mathcal{D}} = \mathcal{D}$.*

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

We prove now that the subset $\widetilde{\mathcal{D}} \subset \mathbb{Z}_+^m$ is a discrete polymatroid. Clearly, $\widetilde{\mathcal{D}} \neq \emptyset$ and, since $\widetilde{\mathcal{D}} \subseteq \mathcal{D}$, it is finite. Moreover, it is obvious that $v \in \widetilde{\mathcal{D}}$ if $v \leq u$ and $u \in \widetilde{\mathcal{D}}$. Consider $u, v \in \widetilde{\mathcal{D}}$ with $|u| < |v|$. Among all possible pairs of sequences $(A_1, \ldots, A_m)$ and $(B_1 \ldots, B_m)$ corresponding, respectively, to the integer vectors u and v, we choose one maximizing $\sum_{j=1}^m |A_j \cap B_j|$. Let $A = A_1 \cup \cdots \cup A_m$ and $B = B_1 \cup \cdots \cup B_m$. Since $|B| > |A|$, there exists a vector $\mathbf{x} \in B - A$ 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 and such that $\sum_{j=1}^m |A_j' \cap B_j| > \sum_{j=1}^m |A_j \cap B_j|$, a contradiction. Therefore, by considering the sequence $(A_1, \ldots, A_i \cup \{\mathbf{x}\}, \ldots, A_m)$, we see that there exists $w \in \widetilde{\mathcal{D}}$ such that $u < w \leq u \vee v$. This proves that $\widetilde{\mathcal{D}}$ is a discrete polymatroid.

Consider the rank function $\widetilde{h} \colon \mathcal{P}(J_m) \to \mathbb{Z}$ of $\widetilde{\mathcal{D}}$. Given a subset $X \subseteq J_m$, it is clear that $\widetilde{h}(X) = \max\{|u(X)| : u \in \widetilde{\mathcal{D}}\} \leq \dim(\sum_{j\in X} V_j) = h(X)$. On the other hand, by considering a basis of the subspace $\sum_{j\in X} V_j$ formed by vectors in $\bigcup_{j\in X} V_j$, we can find a vector $u \in \widetilde{\mathcal{D}}$ with $|u(X)| = \dim(\sum_{j\in X} V_j)$ and, hence, $\widetilde{h}(X) \geq h(X)$. Therefore, $\widetilde{\mathcal{D}} = \mathcal{D}$. □

The next lemma is a direct consequence Lemma 7.2.

Lemma 7.3. *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 $i \neq j$.*

Let $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$. From now on, V_i will denote both the subspace of $E = \mathbb{K}^s$ and its extension to $\overline{\mathbb{K}}^s$. Clearly, those subspaces provide a $\overline{\mathbb{K}}$-representation of $\mathcal{D}$. For every $i \in J_m$, let $r_i = \dim V_i$ and $n_i = |Q_i|$, and take $n = n_1 + \cdots + n_m$. Consider the space $\mathbf{M}$ of all $s \times n$ matrices over $\overline{\mathbb{K}}$ of the form $(M_1|M_2|\cdots|M_m)$, where M_i is a $s \times n_i$ 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 7.1 is concluded by proving that there exists a matrix $M \in \mathbf{M}$ representing the matroid $\mathcal{M}$ over $\overline{\mathbb{K}}$ because, in this case, $\mathcal{M}$ is representable over some finite extension of $\mathbb{K}$ (the one containing all entries of the matrix M).

Lemma 7.4. *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 $A \cap (\cup_{j\in X} Q_j)$ must be linearly dependent. □

Therefore, the following lemma concludes the proof of Theorem 7.1.

Lemma 7.5. *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 get one-to-one mappings

$$\phi_i \colon \overline{\mathbb{K}}^{r_i} \to V_i \subseteq \overline{\mathbb{K}}^s.$$

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

$$\Psi \colon \overline{\mathbb{K}}^N = (\overline{\mathbb{K}}^{r_1})^{n_1} \times \cdots \times (\overline{\mathbb{K}}^{r_m})^{n_m} \to \mathbf{M}.$$

That is, by choosing an element in $\overline{\mathbb{K}}^N$, we obtain n_1 vectors in V_1, n_2 vectors in V_2, and so on. For every basis $B \subseteq Q$ of the matroid $\mathcal{M}$, we consider the mapping $f_B \colon \overline{\mathbb{K}}^N \to \overline{\mathbb{K}}$ 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 s columns corresponding to the elements in B. Clearly, f_B is a polynomial. Let B be a basis of $\mathcal{M}$ and $u = \Pi(B) \in \mathbb{Z}_+^m$. From Lemma 7.3, there exists a basis of $\overline{\mathbb{K}}^s$ of the form $\widetilde{B} = B_1 \cup \cdots \cup B_m$ such that $B_i \subset V_i$ 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 $\mathbf{X}_B \in \overline{\mathbb{K}}^N$ such that $f_B(\mathbf{X}_B) \neq 0$. Therefore, the polynomial f_B is non-zero for every basis B of $\mathcal{M}$. Since the field $\overline{\mathbb{K}}$ is algebraically closed, there exists a point $\mathbf{X}_0 \in \overline{\mathbb{K}}^N$ such that $f_B(\mathbf{X}_0) \neq 0$ for every basis B of $\mathcal{M}$. Clearly, the matrix $\Psi(\mathbf{X}_0)$ is the one we need. □

Theorem 7.1 provides a sufficient condition for a multipartite access structure to be ideal. Namely, a multipartite access structure is ideal if it is of the form $\Gamma_{p_0}(\mathcal{M})$, where $\mathcal{M} = (Q, \mathcal{I})$ is a Π_0-partite matroid such that the discrete polymatroid $\Pi_0(\mathcal{I})$ is representable. In addition, the interest of Theorem 7.1 goes beyond its implications

to secret sharing. As far as we now, the representability of multipartite matroids has not been studied before. Therefore, the connection between multipartite matroids and discrete polymatroids we presented here and Theorem 7.1 are interesting new results about representability of matroids.

The remaining open problems about the characterization of multipartite access structures are now as difficult as the open problems for the general case. The gap between the necessary and the sufficient conditions is due to very difficult problems about matroid and polymatroid representations as, for instance, the following one.

Open Problem 7.6. Characterize the representable discrete polymatroids.

Analogously to the matroid case, in which there exist ss-representable matroids that are not representable, we have to consider a different kind of polymatroid representation. A discrete polymatroid $\mathcal{D}$ with ground set J_m and rank function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ is *probabilistically representable* if there exist a finite set E with a probability distribution on it and, for every $i \in J_m$, a surjective mapping $\pi_i\colon E \to E_i$ such that $h(X) = H(X)$ for every $X \subseteq J$, where, as in Section 4, $H(X)$ denotes the Shannon entropy on the corresponding random variable. The next proposition is not difficult to prove. Nevertheless, to prove or disprove its converse, which would be in any case a very interesting result about the characterization of ideal multipartite access structures, seems to be a very difficult open problem.

Proposition 7.7. *Let $\mathcal{M} = (Q, \mathcal{I})$ be a Π-partite matroid and let $\mathcal{D} = \Pi(\mathcal{I})$ be its associated discrete polymatroid. If $\mathcal{M}$ is ss-representable, then $\mathcal{D}$ is probabilistically representable.*

Open Problem 7.8. Is the converse of Proposition 7.7 true?

Open Problem 7.9. Characterize the probabilistically representable polymatroids.

8 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 [30], but only partial results were known about the tripartite case [2, 11, 13].

We begin by characterizing the matroid-related bipartite and tripartite access structures. Afterwards, we prove that all matroids related to those access structures are representable and, hence, all matroid-related bipartite and tripartite access structures are ideal. We obtain in this way a characterization of the ideal bipartite and tripartite access structures. In addition, as a consequence of the results in [22], the optimal information rate of every non-ideal bipartite or tripartite access structure is at most 2/3.

We observe that we cannot obtain in this way 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 matroid-related quadripartite access structures that are not ideal.

8.1 Characterizing Matroid-Related Bipartite and Tripartite Access Structures

By applying Theorem 6.2 to the particular cases $m = 2$ and $m = 3$, we characterize the matroid-related bipartite and tripartite access structures.

Let Γ be a bipartite access structure, that is, Γ is Π-partite for some partition $\Pi = (P_1, P_2)$ of the set P of participants. From Theorem 6.2, Γ is matroid-related if and only if there exists a discrete polymatroid $\mathcal{D}$ with ground set J_2 and a $\mathcal{D}$-compatible family $\Delta \subseteq \mathcal{P}(J_2)$ such that $\Gamma = \{A \subseteq P : \Pi(A) \geq u \text{ for some vector } u \in \mathcal{G}(\Delta)\}$, where $\mathcal{G}(\Delta) = \bigcup_{X \in \Delta} \mathcal{B}(X)$ and

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

Given integers r_1, r_2, s and a family of subsets $\Delta \subseteq \mathcal{P}(J_2)$, there exists a discrete polymatroid $\mathcal{D}$ with ground set J_2 and $r_i = h(\{i\})$, for $i = 1, 2$, and $s = h(\{1,2\})$ such that Δ is $\mathcal{D}$-compatible if and only if the following conditions are satisfied.

1. $s > 0$ and $0 \leq r_i \leq s \leq r_1 + r_2$.
2. Δ is monotone increasing, $\emptyset \notin \Delta$, and $J_2 \in \Delta$.
3. $r_i > 0$ if $\{i\} \in \Delta$, and $s > r_i$ if $\{i\} \notin \Delta$.
4. $r_1 + r_2 > s$ if $\{\{1\}, \{2\}\} \subset \Delta$.

Summarizing, a bipartite access structure is matroid-related if and only if it is determined in that way by some $\Delta \subseteq \mathcal{P}(J_2)$ and some integers r_1, r_2, s in the above conditions.

The characterization of the matroid-related tripartite access structure is more involved. We begin by introducing some notation. 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 $s = h(J_3)$. The integer values r_i, s_i, and s 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 6.1, 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 6.2, 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

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

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

8.2 All Matroid-Related Bipartite and 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, $\max\{0, s - \sum s_i + \sum r_i\} \leq t \leq \min\{t_1, t_2, t_3\}$.

Proposition 8.1. *Let $\mathcal{D}$ be a discrete 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 $\mathcal{D}$ given by subspaces $V_1, V_2, V_3 \subseteq E = \mathbb{K}^s$ with $\dim(V_1 \cap V_2 \cap V_3) = t$.*

Proof. Consider two subspaces $V, W \subseteq E$ such that $\dim V = s_3$ and $E = V \oplus W$. Given a basis $\{v_1, \ldots, v_{s_3}\}$ of V, consider the mapping $\mathbf{v}\colon \mathbb{K} \to V$ defined by $\mathbf{v}(x) = \sum_{i=1}^{s_3} x^{i-1} v_i$. Observe that the vectors $\mathbf{v}(x)$ have Vandermonde coordinates with respect to the given basis of V. This implies that every set of at most s_3 vectors of the form $\mathbf{v}(x)$ is independent. Consider three disjoint sets $T_3, R_1, R_2 \subseteq \{\mathbf{v}(x) : x \in \mathbb{K}\} \subset V$ 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 $V_3 \subset E$ to complete the representation of $\mathcal{D}$. 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 a consequence of this result, we obtain Corollary 8.2. This and Theorem 7.1 prove Corollary 8.3.

Corollary 8.2. *Every discrete polymatroid with ground set J_m with $m \leq 3$ is representable over fields of all characteristics.*

Corollary 8.3. *Every m-partite matroid with $m \leq 3$ is representable over fields of all characteristics.*

Corollary 8.4. *Every matroid-related bipartite access structure is ideal.*

Proof. If $\Gamma_{p_0}(\mathcal{M})$ is a matroid-related bipartite access structure, then the matroid $\mathcal{M}$ is tripartite and, from Corollary 8.3, it is representable. □

The next lemma is a well known result of linear algebra. It will be used in the proof of Theorem 8.6.

Lemma 8.5. *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 $V \not\subset W_i$ for every $i = 1, \ldots, n$. Then $V \not\subset \bigcup_{i=1}^{n} W_i$.*

Theorem 8.6. *Every matroid-related tripartite access structure is ideal. More specifically, every matroid-related tripartite access structure admits ideal linear secret sharing schemes over fields of all characteristics.*

Proof. Let $\Gamma = \Gamma_{p_0}(\mathcal{M})$ be a matroid-related tripartite access structure. Then there exist partitions $\Pi = \{P_1, P_2, P_3\}$ of the set P of participants and $\Pi_0 = \{\{p_0\}, P_1, P_2, P_3\}$ of the set $Q = P \cup \{p_0\}$ such that Γ is Π-partite and the matroid $\mathcal{M} = (Q, \mathcal{I})$ is Π_0-partite. From Theorem 7.1, we only have to prove that the discrete polymatroid $\mathcal{D}' = \Pi_0(\mathcal{M})$ is representable over finite fields of every characteristic. Remember that $\mathcal{D}'$ is a completion of the discrete polymatroid $\mathcal{D} = \mathcal{D}'(J_3)$. Therefore, $\mathcal{D}'$ is determined by the integers r_i, s_i, s that define the rank function of $\mathcal{D}$ and the family $\Delta = \Delta(\mathcal{D}')$. For every i, j, k with $\{i, j, k\} = J_3$, consider $t_i = r_j + r_k - s_i$. From the proof of Proposition 8.1, 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 $\mathcal{D}$ 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 $\mathcal{D}'$. We distinguish several cases, depending on the family Δ. Clearly, the cases that are not considered here are solved by symmetry. Remember that the values r_i, s_i, and s and the family Δ must satisfy the conditions in Section 8.1.

Case 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, $s_1 < s$.

Case 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 $\mathcal{D}$ such that $V_1 \cap V_2 \not\subset V_3$. Now, we only have to take a vector $x_0 \in V_1 \cap V_2$ such that $x_0 \notin V_3$.

Case 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, hence, there exists a representation of $\mathcal{D}$ with $V_1 \cap V_2 \cap V_3 \neq \{0\}$.

Case 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 $V_1 \cap (V_2 + V_3) \not\subset V_i$ 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 $x_0 \notin V_3$.

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

Case 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, $V \not\subset V_2$. 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 $x_0 \notin V_2$.

Case 7 $\min\Delta = \{\{1,2\},\{2,3\},\{3,1\}\}$. Consider $W = (V_1+V_2)\cap(V_2+V_3)\cap(V_3+V_1)$. Because of Equation (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 $W \not\subset V_i$ for every $i \in J_3$. Therefore, there exists a vector $x_0 \in W$ such that $x_0 \notin V_i$ for every $i \in J_3$.

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

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

[4] 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.

[5] 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** 148–167.

[6] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.

[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] E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology* **5** (1992), 153–166.

[10] 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.

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

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

[13] J. Herranz, G. Sáez. New Results on Multipartite Access Structures. *Cryptology ePrint Archive*, Report **2006/048**, `http://eprint.iacr.org/2006/048`.

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

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

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

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

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

[19] J.Martí-Farré, C. Padró. Secret sharing schemes on sparse homogeneous access structures with rank three. *Electronic Journal of Combinatorics* **11(1)** (2004) Research Paper 72, 16 pp. (electronic).

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

[21] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics* **154** (2006) 552–563.

[22] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *Cryptology ePrint Archive*, Report **2006/077**, `http://eprint.iacr.org/2006/077`.

[23] 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.*, to appear.

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

[25] P. Morillo, C. Padró, G. Sáez, J. L. Villar. Weighted Threshold Secret Sharing Schemes. *Inf. Process. Lett.* **70** (1999) 211-216.

[26] S.-L. Ng. A Representation of a Family of Secret Sharing Matroids. *Des. Codes Cryptogr.* **30** (2003) 5-19.

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

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

[29] J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

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

[31] P.D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.

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

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

[34] G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO '88, Lecture Notes in Comput. Sci.* **403** (1990) 390–448.

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

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

[37] T. Tassa. Hierarchical Threshold Secret Sharing. *First Theory of Cryptography Conference, TCC 2004, Lecture Notes in Comput. Sci.* **2951** (2004) 473–490.

[38] 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.

[39] D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.