# Ideal Hierarchical Secret Sharing Schemes [*]

Oriol Farràs, Carles Padró
Dep. de Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, Barcelona, Spain
{ofarras,cpadro}@ma4.upc.edu

**Abstract**

This paper deals with hierarchical secret sharing schemes, in which the participants are distributed into levels that are hierarchically ordered as, for instance, in a weighted threshold secret sharing scheme. Several particular constructions of ideal hierarchical secret sharing schemes have been given in the literature.

Here, we study hierarchical secret sharing in all generality by providing a natural definition for the family of the hierarchical access structures. We present a characterization of the ideal access structures in this family, that is, the ones admitting an ideal secret sharing scheme. In particular, we prove that every ideal hierarchical access structure admits an ideal *linear* secret sharing scheme.

**Key words.** Secret sharing, Ideal secret sharing schemes, Hierarchical secret sharing, Multipartite secret sharing, Multipartite matroids, Discrete polymatroids.

## 1 Introduction

A *secret sharing scheme* is a method to distribute *shares* of a *secret value* among a set of *participants*. Only the *qualified* subsets of participants can recover the secret value from their shares, while the *unqualified* subsets do not obtain any information about the secret value. The qualified subsets form the *access structure* of the scheme, which is a monotone increasing family of subsets of participants. Only *unconditionally secure perfect* secret sharing schemes are considered in this paper.

Secret sharing was independently introduced by Shamir [32] and Blakley [5] in 1979. They presented two different methods to construct secret sharing schemes for *threshold access structures*, whose qualified subsets are those with at least some given number of participants. These schemes are *ideal*, that is, the length of every share is the same as the length of the secret, which is the best possible situation [17].

There exist scenarios in which non-threshold secret sharing schemes are required because, for instance, some participants should be more powerful than others. The first attempt to overcome the limitation of threshold access structures was made by Shamir in his seminal work [32] by proposing a simple modification of the threshold scheme. Namely, every participant receives as its share a certain number of shares from a threshold scheme, according to its position in the hierarchy. In this way a scheme for a *weighted threshold access structure* is obtained. That is, every participant has

[*] The authors' work was partially supported by the Spanish Ministry of Education and Science under project TSI2006-02731.

a weight (a positive integer) and a set is qualified if and only if its weight sum is at least a given threshold. This new scheme is not ideal because the shares are in general larger than the secret.

Every access structure admits a secret sharing scheme [3, 15], but in general the shares must be larger than the secret [9, 11]. Very little is known about the optimal complexity of secret sharing schemes for general access structures, and there is a wide gap between the best known general lower and upper bounds. Because of that, the construction of ideal secret sharing schemes for particular families of access structures that may have interesting applications is worth considering.

Brickell [7] proposed a method, based on linear algebra, to construct ideal secret sharing schemes for access structures that are not necessarily threshold. This method was applied to the construction of ideal secret sharing schemes for *multilevel* and *compartmented* access structures, two families that had been proposed by Simmons [33]. These are *multipartite access structures*, which means that the participants are divided into several parts (levels or compartments) and all participants in the same part play an equivalent role in the structure. These parts are hierarchically ordered in the multilevel access structures, while this is not the case in the compartmented ones. Other constructions of ideal secret sharing schemes for access structures with hierarchical properties have been given in [4, 35, 36].

In this paper we begin the study of hierarchical secret sharing in all generality. We introduce a natural definition for the family of the *hierarchical access structures*. Basically, if a participant in a qualified subset is substituted by a *hierarchically superior* participant, the new subset must be still qualified. An access structure is *hierarchical* if, for any two given participants, one of them is hierarchically superior to the other. This family contains the multilevel access structures [7, 33], the hierarchical threshold access structures studied by Tassa [35] and by Tassa and Dyn [36], and also the weighted threshold access structures that were first considered by Shamir [32] and studied in [1, 2, 24, 29]. Similarly to multipartite and weighted threshold access structures, the family of the hierarchical access structures is closed by duality and minors.

Our main result is a characterization of the ideal hierarchical access structures. In addition, we prove that all ideal access structures in this family are *vector space access structures*, that is, they admit an ideal linear secret sharing scheme constructed by the method proposed by Brickell [7].

The proofs of our results strongly rely on the connection between matroids and ideal secret sharing schemes discovered by Brickell and Davenport [8]. Moreover, since hierarchical access structures are in particular multipartite, the results and techniques in [12] about the characterization of ideal multipartite access structures are extremely useful in achieving our results. In particular, discrete polymatroids play a fundamental role in our proofs. Another important tool is the geometrical representation introduced in [12, 29] for multipartite access structures, which has been adapted here to the hierarchical case by introducing the notion of access structures that are *stable* under some set of translations.

## 2 Related Work

The construction of ideal secret sharing schemes for families of access structures that can have interesting applications have attracted some attention. Simmons [33] conjectured that multilevel and compartmented access structures admit an ideal scheme, and this was proved by Brickell [7] by introducing a new method to construct ideal secret sharing schemes, which are called vector space secret sharing schemes. Multilevel access structures are a particular case of hierarchical access structures. Different methods to construct vector space secret sharing schemes for several families of multipartite access structures were given by Ng [26], by Tassa [35], and by Tassa and Dyn [36]. Among the access structures considered in [35, 36] we find the *hierarchical threshold* ones, which are hierarchical structures that generalize the multilevel access structures in [7, 33]. The constructions in [35, 36] are remarkable for their efficiency and also for the use of novel techniques in secret sharing as Birkhoff interpolation and interpolation of bivariate polynomials.

The characterization of the ideal access structures is an important and long-standing open problem in secret sharing. Brickell and Davenport [8] proved that every ideal secret sharing scheme defines a matroid. Actually, this matroid is univocally determined by the access structure of the scheme. This implies a necessary condition for an access structure to be ideal. Namely, every ideal access structure is a *matroid port*. A sufficient condition is obtained from the method to construct linear ideal secret sharing schemes by Brickell [7]: the ports of representable matroids are ideal access structures. Seymour [31] proved that the necessary condition is not sufficient, while the sufficient condition is not necessary because of the counterexample given by Simonis and Ashikhmin [34]. Martí-Farré and Padró [21] generalized the results in [8] by proving that, if all shares in a secret sharing scheme are shorter than 3/2 times the secret value, then its access structure is a matroid port. At this point, the remaining open question about the characterization of ideal access structures is determining the matroids that can be defined from ideal secret sharing schemes. Some important results, ideas and techniques to solve this question are given in [23].

In addition to the search of general results, several authors [1, 6, 9, 12, 16, 19, 20, 22, 29] studied this open problem for particular families of access structures. In most of these families, the ideal access structures coincide with the ports of representable matroids, and hence they admit a vector space secret sharing scheme.

Some of these works deal with families of multipartite access structures. Beimel, Tassa and Weinreb [1] presented a characterization of the ideal weighted threshold access structures that generalizes the partial results in [24, 29]. A complete characterization of ideal bipartite access structures was given in [29], and related results were given independently in [25, 27]. Partial results on the characterization of tripartite ideal access structures appeared in [10, 13], and this question was solved in [12]. In all these families, the ideal access structures are precisely the ports of representable matroids. The characterization of ideal tripartite access structures in [12] was obtained actually from the general results on the characterization of ideal multipartite access structures in that paper. One of the most remarkable contributions in [12] is the use for the first time in secret sharing of *discrete polymatroids*, a combinatorial object introduced by Herzog and Hibi [14].

Another important result about weighted threshold access structures have been obtained recently by Beimel and Weinreb [2]. They prove that all such access structures in admit secret sharing schemes in which the size of the shares is quasi-polynomial in the number of users.

## 3 Ideal Secret Sharing Schemes and Matroids

We recall in this section some facts about the connection between ideal secret sharing schemes and matroids that is derived from the results by Brickell [7] and by Brickell and Davenport [8].

We begin by describing the method by Brickell [7] to construct ideal secret sharing schemes. Consider a vector space $E$ with finite dimension over a finite field $\mathbb{K}$. Given a set $P$ of participants and a special participant $p_0 \notin P$, usually called *dealer*, consider, for every $i \in Q = P \cup \{p_0\}$, a nonzero linear form $\pi_i \colon E \to \mathbb{K}$, that is, a nonzero vector in the dual space $E^*$. A secret sharing scheme is constructed from these linear forms as follows. For every choice of a random vector $x \in E$, one obtains a collection of shares $s_i = \pi_i(x) \in \mathbb{K}$, where $i \in P$, for the secret value $s = \pi_{p_0}(x) \in \mathbb{K}$. A set $A \subseteq P$ is in the access structure of this scheme if and only if the vector $\pi_{p_0} \in E^*$ is a linear combination of the vectors $(\pi_i)_{i\in A}$. Let $\mathcal{P}(Q)$ denote the power set of $Q$. This access structure is actually determined by the *rank function* $r\colon \mathcal{P}(Q) \to \mathbb{Z}$ that is defined as follows: for every $X \subseteq Q$, the value $r(X)$ is the dimension of the subspace of $E^*$ spanned by the set $\{\pi_i : i \in X\}$. 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 following properties are satisfied by the rank function $r$.

1. $0 \le r(X) \le |X|$ for every $X \subseteq Q$.

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

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 [28, 37] for general references on matroid theory. One of the many possible equivalent definitions for this concept states 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 $\mathbb{K}$-*representable* if its rank function can be defined as before from a family of vectors in some vector space over $\mathbb{K}$.

For a (not necessarily representable) 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

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

Such access structures are said to be *matroid ports* or, more precisely, the access structure $\Gamma_{p_0}(\mathcal{M})$ is called the *port of the matroid* $\mathcal{M}$ *at the point* $p_0$.

Therefore, as a consequence of the construction by Brickell [7], we obtain a sufficient condition for an access structure to be ideal. Namely, the ports of representable matroids are ideal access structures. 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: every ideal access structure is a matroid port.

With a slightly different definition, matroid ports were introduced by Lehman [18] to solve the *Shannon switching game* in 1964, much before secret sharing was invented by Shamir [32] and Blakley [5] in 1979. A forbidden minor characterization of matroid ports was given by Seymour [30]. Even though the results in [7, 8] deal with matroid ports, this terminology was not used in those and many other subsequent works on secret sharing. The old results on matroid ports in [18, 30] were rediscovered for secret sharing by Martí-Farré and Padró [21], who used them to generalize the result by Brickell and Davenport by proving that, if all shares in a secret sharing scheme are shorter than 3/2 times the secret, then its access structure is a matroid port.

## 4 Hierarchical Access Structures

We present here a natural definition for the family of the *hierarchical access structures*, which embraces all possible situations in which there is a hierarchy on the set of participants. For instance, the weighted threshold access structures and the hierarchical threshold access structures [35] are contained in this new family. Hierarchical access structures are in particular multipartite. Therefore, we can take advantage of the results and techniques in [12] about the characterization of ideal multipartite access structures.

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

Let $\Pi = (P_1, \ldots, P_m)$ be a partition of $P$. An access structure $\Gamma$ is said to be $\Pi$-*partite* if every pair of participants in the same part $P_i$ are hierarchically equivalent. A different but equivalent definition for this concept is given in [12]. If $m$ is the number of parts in $\Pi$, such structures are called *$m$-partite access structures*. A $\Pi$-partite access structure is said to be $\Pi$-*hierarchical* if $q \preceq p$ for every pair of participants $p \in P_i$ and $q \in P_j$ with $i < j$. That is, the participants in the first level are hierarchically superior to those in the second level and so on. Obviously, an access structure is hierarchical if and only if it is $\Pi$-hierarchical for some partition $\Pi$ of the set of participants.

## 5 A Geometric Representation of Hierarchical Access Structures

In this section we recall the geometric representation for multipartite access structures that was introduced in [12, 29]. This representation is adapted to hierarchical access structures by introducing the new concept of *stabilizers* of multipartite access structures.

We notate $\mathbb{Z}_+$ and $\mathbb{Z}_-$ for the sets of the non-negative and the non-positive integers, respectively, while $\mathbb{Z}_+^*$ and $\mathbb{Z}_-^*$ denote, respectively, the sets of the positive and the negative integers. For any $u \in \mathbb{Z}^m$, we write $u_i$ for its $i$-th coordinate, that is, $u = (u_1, \ldots, u_m)$. If $u, v \in \mathbb{Z}^m$, we write $u \le v$ if $u_i \le v_i$ for every $1 \le i \le m$, and we write $u < v$ if $u \le v$ and $u \ne v$.

For each partition $\Pi = (P_1, \ldots, P_m)$ of the set $P$, we consider a mapping $\Pi \colon \mathcal{P}(P) \to \mathbb{Z}_+^m$ defined by $\Pi(A) = (|A \cap P_1|, \ldots, |A \cap P_m|) \in \mathbb{Z}_+^m$. We write $\mathbf{p} = \Pi(P) = (|P_1|, \ldots, |P_m|)$ and

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

For a $\Pi$-partite access structure $\Gamma \subseteq \mathcal{P}(P)$, consider $\Pi(\Gamma) = \{\Pi(A) \,:\, A \in \Gamma\} \subseteq \mathbf{P}$. Observe that $A \in \Gamma$ if and only if $\Pi(A) \in \Pi(\Gamma)$, so $\Gamma$ is univocally represented by the set of points $\Pi(\Gamma) \subseteq \mathbf{P}$. By an abuse of notation, we will use $\Gamma$ to denote both a $\Pi$-partite access structure on $P$ and the corresponding set of points $\Pi(\Gamma)$.

Let $\Gamma$ be a $\Pi$-partite access structure on $P$. If two points $u, v \in \mathbf{P}$ are such that $u \le v$ and $u \in \Gamma$, then $v \in \Gamma$. This is due to the fact that $\Gamma$ is a monotone increasing family of subsets. Therefore, $\Gamma \subseteq \mathbf{P}$ is determined by the family $\min \Gamma \subset \mathbf{P}$ of its minimal points. We are using here an abuse of notation as well, because $\min \Gamma$ denotes also the family of minimal subsets of the access structure $\Gamma$.

A set $V \subseteq \mathbb{Z}^m$ is called a *stabilizer* if $V$ is closed by sums, and $\mathbb{Z}_+^m \subseteq V$, and $V \cap (\mathbb{Z}_-^*)^m = \{0\}$. For a stabilizer $V \subseteq \mathbb{Z}^m$, we define the binary relation $\le_V$ in $\mathbb{Z}^m$ by $u \le_V v$ if and only if $v - u \in V$.

Since $0 \in V$ and $V$ is closed by sums, this binary relation is reflexive and transitive. It is an order if and only if $V \cap (-V) = \{0\}$.

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

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

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

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

The next lemma shows a characterization of the vectors in $H$. This result and the one in Lemma 5.2 will be very useful in our study of hierarchical access structures.

**Lemma 5.1.** *A vector $v \in \mathbb{Z}^m$ is in $H$ if and only if $\sum_{j=1}^{i} v_j \geq 0$ for all $i = 1, \dots, m$.*

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

**Lemma 5.2.** *If $x, y \in \mathbb{Z}_+^m$ are such that $y - x \in H$, then there exist $v \in H_0$ and $u \in \mathbb{Z}_+^m$ such that $y = x + v + u$ and $x + v \geq 0$. In particular, if $\Gamma$ is a $\Pi$-hierarchical access structure and $y \in \min \Gamma$, then there exists $x \in \min_H \Gamma$ such that $y - x \in H_0$.*

*Proof.* The proof is by induction on $m$. The result is trivial for $m = 1$. Assume that $m > 1$. For a vector $x \in \mathbb{Z}^m$, we notate $x = (\widetilde{x}, x_m)$ with $\widetilde{x} \in \mathbb{Z}^{m-1}$. If $x, y \in \mathbb{Z}_+^m$ are such that $y - x \in H$, then it is clear from Lemma 5.1 that $\widetilde{y} - \widetilde{x} \in H$. By the induction hypothesis, $\widetilde{y} = \widetilde{x} + \widetilde{v} + \widetilde{u}$, where $\widetilde{v} \in H_0$, and $\widetilde{u} \in \mathbb{Z}_+^{m-1}$, and $\widetilde{x} + \widetilde{v} \geq 0$. If $x_m \leq y_m$, then $y = (\widetilde{y}, y_m) = (\widetilde{x}, x_m) + (\widetilde{v}, 0) + (\widetilde{u}, y_m - x_m)$. So, we can take $v = (\widetilde{v}, 0)$ and $u = (\widetilde{u}, y_m - x_m)$. If $x_m > y_m$, then there exists $w = (\widetilde{w}, y_m - x_m) \in H_0$ such that $\widetilde{w} \geq 0$, and $x' = x + w \geq 0$, and $y - x' \in H$. Since $x'_m = y_m$, we have that $y = x' + v' + u'$ with $v' \in H_0$, and $u' \in \mathbb{Z}_+^m$, and $x' + v' \geq 0$. In this case we can take $v = v' + w$ and $u = u'$.

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

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

Duals and minors of access structures are important concepts in secret sharing, because several properties as being a matroid port or being a $\mathbb{K}$-vector space access structure have a good behavior under these operations. The *dual* of an access structure $\Gamma$ on a set $P$ is the access structure on the same set defined by $\Gamma^* = \{A \subset P \,:\, P \setminus A \notin \Gamma\}$. It is not difficult to prove that $\Gamma$ is $\Pi$-partite if and only if $\Gamma^*$ is so. For a subset $B \subset P$, we define the access structures $\Gamma \backslash B$ and $\Gamma / B$ on the set $P \setminus B$ by $\Gamma \backslash B = \{A \subset P \setminus B \,:\, A \in \Gamma\}$ and $\Gamma / B = \{A \subset P \setminus B : A \cup B \in \Gamma\}$. Every access structure that can be obtained from $\Gamma$ by repeatedly applying the operations $\backslash$ and $/$ is called a *minor* of $\Gamma$. If $\Pi = (P_1, \ldots, P_m)$ is a partition of $P$ and $\Gamma$ is a $\Pi$-partite access structure, then the minors $\Gamma \backslash B$ and $\Gamma / B$ are $(\Pi \backslash B)$-partite access structures, where $\Pi \backslash B = (P_1 \setminus B, \ldots, P_m \setminus B)$, a partition of $P \setminus B$. If $\Pi(B) = b$, then the geometric representations of these access structures are $\Gamma \backslash B = \{x \leq \mathbf{p} - b \,:\, x \in \Gamma\}$ and $\Gamma / B = \{x \leq \mathbf{p} - b \,:\, x + b \in \Gamma\}$.

**Proposition 5.3.** *Let $V \subset \mathbb{Z}^m$ be a stabilizer. Then the dual of a $V$-stable $m$-partite access structure is $V$-stable and all its minors are $V$-stable as well. In particular, this holds for hierarchical and weighted threshold access structures.*

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

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

Let $P'$ and $P''$ be two disjoint sets and let $\Gamma'$ and $\Gamma''$ be access structures on $P'$ and $P''$, respectively. The *composition of* $\Gamma'$ *and* $\Gamma''$ *over* $p \in P'$ is denoted by $\Gamma'[\Gamma''; p]$ and is defined as the access structure on the set of participants $P = P' \cup P'' \setminus \{p\}$ that is formed by all subsets $A \subseteq P$ such that $A \cap P' \in \Gamma'$ and all subsets $A \subseteq P$ such that $(A \cup \{p\}) \cap P' \in \Gamma'$ and $A \cap P'' \in \Gamma''$. The composition of matroid ports is a matroid port, and the same applies to $\mathbb{K}$-vector space access structures. A proof for these facts can be found in [22]. The access structures that can be expressed as the composition of two access structures on sets with at least two participants are called *decomposable*.

Suppose that $\Gamma'$ is $(P_1, \ldots, P_r)$-partite and $\Gamma''$ is $(P_{r+1}, \ldots, P_{r+s})$-partite, and take $p \in P_r$. Then the composition $\Gamma'[\Gamma''; p]$ is $(P'_1, \ldots, P'_{r+s})$-partite, where $P'_r = P_r \setminus \{p\}$ and $P'_i = P_i$ for $i \neq r$. If $\Gamma'$ and $\Gamma''$ are hierarchical and $p \in P_r$ then $\Gamma'[\Gamma''; p]$ is also hierarchical. Observe that the composition is made over a participant in the lowest level of $\Gamma'$.

**Example 5.4.** Brickell [7] showed how to construct ideal secret sharing schemes for the multilevel structures proposed by Simmons [33]. These structures are of the form

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

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

**Example 5.5.** Another hierarchical threshold access structure was proposed by Tassa [35]. Given integers $0 < t_1 < \ldots < t_m$, the access structure is defined as

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

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

# 6 Multipartite Access Structures and Discrete Polymatroids

The aim of this and the following sections is to present and to prove our main result, Theorem 9.2, which is a complete characterization of the ideal hierarchical access structures in terms of the properties of their $H$-minimal points. First we recall here some facts about discrete polymatroids and we show the connection between these combinatorial objects and multipartite matroids and their ports. Since all ideal access structures are matroid ports, we obtain in this way some necessary conditions for a hierarchical access structure to be ideal in Section 7. Finally, in Sections 8 and 9 we show that these necessary conditions are also sufficient.

Multipartite matroid ports are ports of *multipartite matroids*, and those matroids are closely related to *discrete polymatroids*, a combinatorial object that was introduced by Herzog and Hibi [14] to study some problems in commutative algebra. We recall here some definitions and basic facts about discrete polymatroids and multipartite matroids, the relation between these two combinatorial objects, and their connections to the characterization of multipartite access structures. More information about these concepts can be found in [12, 14].

We need to introduce some notation before defining discrete polymatroids. Consider a finite set $J$. For every two points $u = (u_i)_{i \in J}$ and $v = (v_i)_{i \in J}$ in $\mathbb{Z}^J$, the point $w = u \vee v$ is defined by $w_i = \max\{u_i, v_i\}$ for every $i \in J$. As before, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J$. The *modulus* of a point $u \in \mathbb{Z}^J$ is $|u| = \sum_{i \in J} u_i$. For every subset $X \subseteq J$, we notate $u(X) = (u_i)_{i \in X} \in \mathbb{Z}^X$ and $|u(X)| = \sum_{i \in X} u_i$. A *discrete polymatroid* with *ground set* $J$ is a nonempty finite set of points $\mathcal{D} \subset \mathbb{Z}_+^J$ satisfying the following properties.

1. If $u \in \mathcal{D}$ and $v \in \mathbb{Z}_+^J$ is such that $v \leq u$, then $v \in \mathcal{D}$, and
2. for every pair of points $u, v \in \mathcal{D}$ 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 point $u \in \mathcal{D}$ such that there does not exist any $v \in \mathcal{D}$ with $u < v$. Similarly to matroids, all bases have the same modulus, and discrete polymatroids are completely determined by their bases. Moreover, a nonempty set $\mathcal{B} \subset \mathbb{Z}_+^m$ 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 $j \in J$ such that $u_j < v_j$ and $u - \mathbf{e}^i + \mathbf{e}^j \in \mathcal{B}$, where $\mathbf{e}^i \in \mathbb{Z}^J$ is such that $\mathbf{e}^i_k = 0$ if $i \neq k$ and $\mathbf{e}^i_i = 1$.

The mapping $h \colon \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \max\{|u(X)| : u \in \mathcal{D}\}$ for every $X \subseteq J$ is called the *rank function* of the discrete polymatroid $\mathcal{D}$. A discrete polymatroid is completely determined by its rank function. So we will write $\mathcal{D} = (J, h)$ to denote the discrete polymatroid with ground set $J$ and rank function $h$. A mapping $h \colon \mathcal{P}(J) \to \mathbb{Z}$ is the rank function of a discrete polymatroid with ground set $J$ if and only if

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

We say that a discrete polymatroid $\mathcal{D}' = (J', h')$ is an extension of a discrete polymatroid $\mathcal{D} = (J, h)$ if $J \subset J'$ and $h'(A) = h(A)$ for all $A \subseteq J$. Since $h'$ is an extension of $h$, both will be usually denoted by $h$. For a discrete polymatroid $\mathcal{D}$ with ground set $J$ and a subset $X \subseteq J$, we define the discrete polymatroid $\mathcal{D}(X)$ with ground set $X$ by $\mathcal{D}(X) = \{u(X) : u \in \mathcal{D}\} \subset \mathbb{Z}_+^X$. We consider the set of points $\mathcal{B}(\mathcal{D}, X) \subset \mathbb{Z}_+^J$ such that $u \in \mathcal{B}(\mathcal{D}, X)$ if and only if $u(X)$ is a basis of $\mathcal{D}(X)$ and $u_i = 0$ for every $i \in J \smallsetminus X$. Observe that $\mathcal{D}$ is an extension of $\mathcal{D}(X)$ for all $X \subset J$.

For a partition $\Pi = (Q_1, \ldots, Q_m)$ of the ground set $Q$, a matroid $\mathcal{M} = (Q, r)$ is said to be $\Pi$-*partite* if every permutation $\sigma$ on $Q$ such that $\sigma(Q_i) = Q_i$ for $i = 1, \ldots, m$ is an automorphism of $\mathcal{M}$. Consider the set $J_m = \{1, \ldots, m\}$. Then the function $h \colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = r(\bigcup_{i \in X} Q_i)$ is the rank function of a discrete polymatroid $\mathcal{D}(\mathcal{M}) = (J_m, h)$. Reciprocally, for every discrete polymatroid $\mathcal{D} = (J_m, h)$ with $h(\{i\}) \leq |Q_i|$ for $i \in J_m$, there exists a unique $\Pi$-partite matroid $\mathcal{M}$ with $\mathcal{D}(\mathcal{M}) = \mathcal{D}$.

Consider a partition $\Pi = (P_1, \ldots, P_m)$ of a set $P$ and the partition $\Pi_0 = (\{p_0\}, P_1, \ldots, P_m)$ of the set $Q = P \cup \{p_0\}$. A connected matroid port $\Gamma = \Gamma_{p_0}(\mathcal{M})$ on $P$ is $\Pi$-partite if and only if the matroid $\mathcal{M}$ is $\Pi_0$-partite. Therefore, multipartite matroids, and hence discrete polymatroids, are fundamental in the characterization of ideal multipartite access structures. These connections are in the core of the results in [12]. In particular, we present next a characterization of multipartite matroid ports in terms of discrete polymatroids that was proved in [12] and will be extremely useful for our purposes.

From now on, we notate $J_m = \{1, \ldots, m\}$ and $J'_m = \{0, 1, \ldots, m\}$ for every positive integer $m$. Consider a $\Pi$-partite matroid port $\Gamma = \Gamma_{p_0}(\mathcal{M})$ and the associated discrete polymatroid $\mathcal{D}' = \mathcal{D}(\mathcal{M}) = (J'_m, h)$. The $\Pi$-partite matroid port $\Gamma$ is completely determined by the partition $\Pi$ and the discrete polymatroid $\mathcal{D}'$ and we write $\Gamma = \Gamma_0(\mathcal{D}')$. As a consequence of this fact, the following characterization of multipartite matroid ports is proved in [12].

**Theorem 6.1** ([12]). *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set $P$ and let $\Gamma$ be an $\Pi$-partite access structure on $P$. Then $\Gamma$ is a matroid port if and only if there exists a discrete polymatroid $\mathcal{D}' = (J'_m, h)$ with $h(\{0\}) = 1$ and $h(\{i\}) \leq |P_i|$ such that*

$$\min \Gamma = \min \{u \in \mathcal{B}(\mathcal{D}, X) \,:\, X \subseteq J_m \textit{ is such that } h(X) = h(X \cup \{0\})\},$$

*where $\mathcal{D} = \mathcal{D}'(J_m) = (J_m, h)$.*

Since every ideal access structure is a matroid port, Theorem 6.1 provides a necessary condition for a multipartite access structure to be ideal. Several necessary conditions for a hierarchical access structure to be ideal will be deduced from this result in Section 7.

On the other hand, sufficient conditions can be obtained from the fact that the ports of linearly representable matroids are ideal access structures. We present in Theorem 6.2 an interesting result from [12] connecting the linear representations of multipartite matroids to the ones of discrete polymatroids. This result is used in Section 8 to find sufficient conditions for a hierarchical access structure to be ideal.

Let $E$ be a vector space with finite dimension over a finite field $\mathbb{K}$ and, for every $i \in J$, consider a vector subspace $V_i \subseteq E$. It is not difficult to check that the mapping $h\colon \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i\in X} V_i)$ is the rank function of a discrete polymatroid $\mathcal{D} = (J, h)$. The discrete polymatroids that can be defined in this way are said to be $\mathbb{K}$*-linearly representable*.

**Theorem 6.2** ([12])**.** *For every large enough field $\mathbb{K}$, an $m$-partite matroid $\mathcal{M}$ is $\mathbb{K}$-linearly representable if and only if its associated discrete polymatroid $\mathcal{D}(\mathcal{M}) = (J_m, h)$ is $\mathbb{K}$-linearly representable.*

## 7 Hierarchical Matroid Ports

In this section, we use the connection between discrete polymatroids and multipartite matroid ports that is discussed in Section 6 to find necessary conditions for hierarchical access structures to be matroid ports. We prove first some technical lemmas that apply to every discrete polymatroid. Specifical results on discrete polymatroids associated to hierarchical matroid ports will be given afterwards.

**Lemma 7.1.** *Consider a discrete polymatroid $\mathcal{D} = (J_m, h)$, a subset $A \subseteq J_m$, and a point $y \in \mathbb{Z}_+^m$ that is $H$-minimal in $\mathcal{B}(\mathcal{D}, A)$. Then $y$ is the $H$-minimum point of $\mathcal{B}(\mathcal{D}, A)$, that is, $y \le_H x$ for every $x \in \mathcal{B}(\mathcal{D}, A)$.*

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

For every $i, j \in \mathbb{Z}$ we notate $[i, j] = \{i, i+1, \dots, j\}$ if $i < j$, while $[i, i] = \{i\}$ and $[i, j] = \emptyset$ if $i > j$. Let $\mathcal{D} = (J_m, h)$ be a discrete polymatroid. For every $i \in J_m$, consider the point $y^i = y^i(\mathcal{D}) \in \mathbb{Z}_+^m$ defined by $y^i_j = h([j, i]) - h([j + 1, i])$. Observe that $\sum_{j=s}^{i} y^i_j = h([s, i])$ for every $s \in [1, i]$.

**Lemma 7.2.** *For every $i = 1, \dots, m$, the point $y^i(\mathcal{D})$ is the $H$-minimum of $\mathcal{B}(\mathcal{D}, [1, i])$.*

*Proof.* By Lemma 7.1, it is enough to prove that $y^i(\mathcal{D})$ is an $H$-minimal point of $\mathcal{B}(\mathcal{D}, [1, i])$. We prove first that $y^i = y^i(\mathcal{D}) \in \mathcal{B}(\mathcal{D}, [1, i])$. Take $A \subseteq [1, i]$ and, for $j \in [1, i]$, consider $A_j = A \cap [j, i]$. Then

$$|y^i(A)| = \sum_{j\in A} y^i_j = \sum_{j\in A} (h([j, i]) - h([j + 1, i])) \le \sum_{j\in A} (h(A_j) - h(A_{j+1})) = h(A).$$

The inequality holds because $A_{j+1} = A_j \cap [j + 1, i]$ and $[j, i] = A_j \cup [j + 1, i]$. Since $y^i_j = 0$ for all $j > i$, this implies that $y^i \in \mathcal{D}$ for all $i \in J_m$. Moreover, $y^i \in \mathcal{B}(\mathcal{D}, [1, i])$ because $|y^i| = h([1, i])$. We prove next that $y^i$ is $H$-minimal in $\mathcal{B}(\mathcal{D}, [1, i])$. If not, there exists $v \in H_0 \smallsetminus \{0\}$ such that $u = y^i - v \in \mathcal{B}(\mathcal{D}, [1, i])$. Observe that $v_j = 0$ or all $j > i$. By Lemma 5.1, there exists $s \in [1, i]$ for which $\sum_{j=1}^{s-1} v_j > 0$, and hence $\sum_{j=s}^{i} v_j < 0$. Then $|u([s, i])| = \sum_{j=s}^{i} u_j > \sum_{j=s}^{i} y^i_j = h([s, i])$, a contradiction with the assumption that $u \in \mathcal{B}(\mathcal{D}, [1, i])$. □

**Lemma 7.3.** *If $1 \leq j \leq i < m$, then $y^i_j \geq y^{i+1}_j$.*

*Proof.* Since $h$ is submodular, $y^{i+1}_j = h([j, i+1]) - h([j+1, i+1]) \leq h([j, i]) - h([j+1, i]) = y^i_j$. □

For the remaining of this section, we assume that $\Gamma$ is a $\Pi$-hierarchical matroid port, where $\Pi = (P_1, \ldots, P_m)$ is an $m$-partition of the set of participants $P$. Recall that we notate $\mathbf{p} = \Pi(P)$ and $\mathbf{P} = \Pi(\mathcal{P}(P)) \subset \mathbb{Z}^m_+$. In addition, we assume that the access structure $\Gamma$ is *connected*, that is, that every participant is in a minimal qualified subset or, equivalently, for every $i \in J_m$, there is a minimal point $x \in \min \Gamma$ such that $x_i > 0$. Consider the discrete polymatroid $\mathcal{D}' = (J'_m, h)$ such that $\Gamma = \Gamma_0(\mathcal{D}')$, and the discrete polymatroid $\mathcal{D} = \mathcal{D}'(J_m) = (J_m, h)$. Since $\Gamma$ is connected, $h(\{i\}) > 0$ for all $i \in J_m$, and hence $y^i_i > 0$. Consider $\Delta(\Gamma) = \{\mathrm{supp}(x) : x \in \Gamma\} \subseteq \mathcal{P}(J_m)$. Observe that $\Delta(\Gamma) = \{A \subseteq J_m : h(A \cup \{0\}) = h(A)\}$ by Theorem 6.1. For every $x \in \mathbb{Z}^m_+$, we notate $\mathrm{supp}(x) = \{i \in J_m : x_i \neq 0\} \subseteq J_m$. Take $m(x) = \max(\mathrm{supp}(x))$ and $M(x) = \{1, \ldots, m(x)\}$.

**Lemma 7.4.** *If $x \in \mathbf{P}$ is a minimal point of $\Gamma$, then $x \in \mathcal{B}(\mathcal{D}, M(x))$.*

*Proof.* From Theorem 6.1, $x \in \mathcal{B}(\mathcal{D}, A)$ for some subset $A \subseteq M(x)$. We are going to prove that $x \in \mathcal{B}(\mathcal{D}, M(x))$ by checking that $h(A) = h(M(x))$. Specifically, we prove that $h(A \cup \{j\}) = h(A)$ for every $j \in M(x) \smallsetminus A$. Consider $j \in M(x) \smallsetminus A$ and the point $x' = x + \mathbf{e}^j - \mathbf{e}^{m(x)} \in \mathbf{P}$. Observe that $x' \in \Gamma$ because $x' - x \in H$. Applying Theorem 6.1 again, there exist $C \subseteq A \cup \{j\}$ with $C \in \Delta(\Gamma)$ and a point $u \in \mathcal{B}(\mathcal{D}, C)$ such that $x' \geq u$. If $u_j = 0$, then $u < x$, but this is not possible because $x \in \min \Gamma$. Thus, $u_j = 1$ and $j \in C$. Since $h$ is submodular, $h(A \cup \{j\}) + h(C \smallsetminus \{j\}) \leq h(A) + h(C)$. Therefore, $h(A \cup \{j\}) = h(A)$ if $h(C) = h(C \smallsetminus \{j\})$. Suppose now that $h(C \smallsetminus \{j\}) \leq h(C) - 1$. Observe that $h(C \smallsetminus \{j\}) \geq |u(C \smallsetminus \{j\})| = |u(C)| - 1 = h(C) - 1$ because $u \in \mathcal{B}(\mathcal{D}, C)$. Hence, $h(C \smallsetminus \{j\}) = h(C) - 1$ and $u - \mathbf{e}^j \in \mathcal{B}(\mathcal{D}, C \smallsetminus \{j\})$. Observe that $u - \mathbf{e}^j \notin \Gamma$ because $u - \mathbf{e}^j < x$ and $x \in \min \Gamma$. Thus, $C \smallsetminus \{j\} \notin \Delta(\Gamma)$ and $h((C \smallsetminus \{j\}) \cup \{0\}) = h(C \smallsetminus \{j\}) + 1 = h(C)$. The submodularity of $h$ implies that

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

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

**Lemma 7.5.** *If $x \in \mathbf{P}$ is an $H$-minimal point of $\Gamma$, then $x = y^{m(x)}(\mathcal{D})$.*

*Proof.* From Lemma 7.4, $x \in \mathcal{B}(\mathcal{D}, M(x))$ and, since $\mathcal{B}(\mathcal{D}, M(x)) \subseteq \Gamma$ by Theorem 6.1, $x$ is $H$-minimal in $\mathcal{B}(\mathcal{D}, M(x))$. By Lemmas 7.1 and 7.2, this implies that $x = y^{m(x)}(\mathcal{D})$. □

**Lemma 7.6.** *If $x, y \in \mathbf{P}$ are two different $H$-minimal points of $\Gamma$, then $m(x) \neq m(y)$. Moreover, if $m(x) < m(y)$, then $|x| < |y|$.*

*Proof.* It is obvious from Lemma 7.5 that $m(x) \neq m(y)$ if $x \neq y$. Observe that $|x| = h(M(x))$ and $|y| = h(M(y))$, and hence $|x| \leq |y|$ if $m(x) < m(y)$. If $|x| = |y|$, then $x \in \mathcal{B}(\mathcal{D}, M(y)) \subseteq y + H$ and $x - y \in H$, a contradiction. □

**Lemma 7.7.** *If $x, y \in \min_H \Gamma$ are such that $m(x) < m(y)$, then $x_i \geq y_i$ for all $i = 1, \ldots, m(x)$.*

*Proof.* A direct consequence of Lemmas 7.3 and 7.5 □

**Lemma 7.8.** *Let $x, y \in \mathbf{P}$ be two different $H$-minimal points of $\Gamma$ with $m(x) < m(y)$ such that there is not any $H$-minimal point $z$ with $m(x) < m(z) < m(y)$. If $x_i > y_i$ for some $i \in [1, m(x)-1]$, then $|P_j| = x_j$ for all $j \in [i+1, m(x)]$.*

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

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

Clearly $y' \in \Gamma$, but $y' \notin \min \Gamma$ because $|y([j, m(x)])| > |x([j, m(x)])| = h([j, m(x)])$, and hence $y' \notin \mathcal{D}$. Therefore, there exists $z' \in \min \Gamma$ such that $z' < y'$, and by Lemma 5.2 there exists $z \in \min_H \Gamma$ such that $z' - z \in H_0$. By Lemma 7.6, $m(z) < m(y)$ because $|z| = |z'| < |y'| = |y|$. Clearly, $m(z) \geq i$ because $z < y$ if $m(z) < i$. If $m(z) \leq m(x)$, then $z_k \geq x_k$ for all $k = 1, \dots, m(z)$ by Lemma 7.7, a contradiction with $z_i \leq y'_i = y_i < x_i$. Therefore, there exists an $H$-minimal point $z$ such that $m(x) < m(z) < m(y)$. □

## 8 A Family of Ideal Hierarchical Access Structures

Observe that Lemmas 7.6, 7.7, and 7.8 in previous section provide necessary conditions for a $\Pi$-hierarchical access structure to be a matroid port, and hence to be ideal, in terms of the properties of its $H$-minimal points. A sufficient condition is given in this section by constructing a new family of hierarchical vector space secret sharing schemes. Specifically, we present a family of linearly representable discrete polymatroids and we prove that the multipartite access structures that are obtained from them are actually hierarchical. In addition, they are vector space access structures by Theorem 6.2.

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

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

take $d = b_m$ and consider a basis $\{e^1, \dots, e^d\}$ of $\mathbb{K}^d$ and, for every $i = 1, \dots, m$, consider the subspace $V_i = \langle e^{a_i}, \dots, e^{b_i} \rangle \subseteq \mathbb{K}^d$. Let $\mathcal{D}' = \mathcal{D}'(\mathbf{a}, \mathbf{b}) = (J'_m, h)$ be the discrete polymatroid that is linearly represented by the subspaces $V_0, V_1, \dots, V_m$. Observe that the rank function $h$ of $\mathcal{D}'$ is such that $h(A) = |\cup_{i \in A} [a_i, b_i]|$ for all $A \subseteq J'_m$. In particular, $h([j, i]) = |[a_j, b_i]| = b_i - a_j + 1$ whenever $0 \leq j \leq i \leq m$, and hence $h(\{0\}) = 1$. Therefore, for every set of players $P$ and for every $m$-partition $\Pi = (P_1, \dots, P_m)$ of $P$ such that $|P_i| \geq h(\{i\}) = b_i - a_i + 1$, we can consider the $\Pi$-partite matroid port $\Gamma = \Gamma_0(\mathcal{D}')$ that is determined as in Theorem 6.1. Since $\mathcal{D}'$ is $\mathbb{K}$-linearly representable for every finite field $\mathbb{K}$, we have from Theorem 6.2 that $\Gamma$ is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. We prove in the following that $\Gamma$ is actually a $\Pi$-hierarchical access structure.

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

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

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

**Lemma 8.1.** *The points $y^1, \ldots, y^m \in \mathbb{Z}_+^m$ are of the form $y^i = y^i(\mathcal{D}(\mathbf{a}, \mathbf{b}))$ for some $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_+^{m+1}$ in the above conditions if and only if*

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

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

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

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

**Lemma 8.2.** *If $h(A) < h([\min(A), \max(A)])$, then there exists $s \in [\min(A), \max(A)] \smallsetminus A$ such that $h(A) = h(A \cap [1, s]) + h(A \cap [s+1, m])$.*

*Proof.* Consider $s \in [\min(A), \max(A)] \smallsetminus A$ such that $h(A \cup \{s\}) > h(A)$ and define $A_1 = A \cap [1, s]$, and $A_2 = A \cap [s+1, m]$, and $B = \cup_{i \in A} [a_i, b_i]$. Them there exists $t \in [a_s, b_s]$ such that $t \notin B$, and hence $h(A) = |B \cap [1, t-1]| + |B \cap [t+1, m]| = h(A_1) + h(A_2)$. □

**Lemma 8.3.** *If $x \in \min \Gamma$, then $x \in \mathcal{B}(\mathcal{D}, M(x))$.*

*Proof.* Take $A = \operatorname{supp}(x)$. Clearly, $x \in \mathcal{B}(\mathcal{D}, M(x))$ if $h(A) = h(M(x))$. Suppose that $h(A) < h(M(x))$. Observe that $h(A \cup \{0\}) = h(A)$ because $A \in \Delta(\Gamma)$, and hence $a_{\min(A)} = 1$. Then the subset $A' = A \cup [1, \min(A)]$ is such that $h(A') = h(A)$. By applying Lemma 8.2 to $A'$, there exists $s \in [1, M(x)] \smallsetminus A'$ such that $h(A') = h(A' \cap [1, s]) + h(A' \cap [s+1, m])$. Consider $A_1 = A' \cap [1, s]$. Since $|x(B)| \leq h(B)$ for all $B \subseteq J_m$ and $|x| = h(A) = h(A')$, we have that $|x(A_1)| = h(A_1)$, and hence $x' = \sum_{i \in A_1} x_i \mathbf{e}^i \in \mathcal{B}(\mathcal{D}, A_1)$. Then $x' \in \Gamma$ because $A_1 \in \Delta(\Gamma)$, a contradiction with $x \in \min \Gamma$. □

**Lemma 8.4.** *The access structure $\Gamma$ is $\Pi$-hierarchical.*

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

Let $x \in \min \Gamma$ be such that $y = x + \mathbf{v}^i \in \mathbf{P}$. Then $s = m(x) > i$ and $x \in \mathcal{B}(\mathcal{D}, [1, s])$. Clearly, $y \in \Gamma$ if $y \in \mathcal{B}(\mathcal{D}, [1, s])$. Suppose that $y \notin \mathcal{B}(\mathcal{D}, [1, s])$. We assert that, in this situation, there exists $t \in [1, i]$ such that $\sum_{j=t}^{i} y_j > h([t, i])$. Since $y \notin \mathcal{B}(\mathcal{D}, M(x))$, there exists $A \subseteq [1, s]$ such that $|y(A)| > h(A)$ and that is minimal with this property. It is clear that $i \in A$ and $i + 1 \notin A$. Take $t = \min(A)$ and $t' = \max(A)$. If $h(A) < h([t, t'])$, there exists by Lemma 8.2 a value $k \in [t, t'] \smallsetminus A$ such that $h(A) = h(A_1)+h(A_2)$, where $A_1 = A \cap [t, k]$ and $A_2 = A \cap [k+1, t']$. Then, $|y(A_\ell)| > h(A_\ell)$ if $i \in A_\ell$, a contradiction with the election of $A$. Therefore, $h(A) = h([t, t'])$ and $t' = i$ because $|y([t, t'])| > h([t, t'])$. This proves our assertion.

Observe that

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

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

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

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

**Lemma 8.5.** *A point $x \in \mathbf{P}$ is $H$-minimal in $\Gamma$ if and only if $x = y^i$ with $i = m$ or $i < m$ and $|y^i| < |y^{i+1}|$.*

*Proof.* From Lemma 7.5, $\min_H \Gamma \subseteq \{y^1, \ldots, y^m\}$, and hence $\min_H \Gamma = \min_H \{y^1, \ldots, y^m\}$. Take $i, j \in J_m$ with $i < j$. Then $s_k = \sum_{\ell=1}^{k}(y_\ell^i - y_\ell^j) = 0$ if $1 \leq k < i$, while $s_i = y_i^i - y_i^j > 0$, and $s_k \geq |y^i| - |y^j| = s_m$ if $i + 1 \leq k \leq m$. Therefore, by Lemma 5.1, $y^j - y^i \notin H$ while $y^i - y^j \in H$ if and only if $|y^i| = |y^j|$. □

The next proposition summarizes the results in this section.

**Proposition 8.6.** *Let $\Pi = (P_1, \ldots, P_m)$ be an $m$-partition of a set $P$ and let $\Gamma$ be a $\Pi$-hierarchical access structure on $P$. Let $x^1, \ldots, x^r \in \mathbb{Z}_+^m$ be the $H$-minimal points of $\Gamma$ and define $m_i =$ $\max(\operatorname{supp}(x^i))$. Suppose that the following properties are satisfied.*

1. *If $i < j$, then $m_i < m_j$ and $x_k^i = x_k^j$ for all $k = 1, \ldots, m_i - 1$.*
2. *If $m_{j-1} < i \leq m_j$, then $|P_i| \geq \sum_{\ell=i}^{m_j} x_\ell^j$.*

*Then $\Gamma$ is ideal and, moreover, it admits a $\mathbb{K}$-vector space secret sharing scheme for every large enough finite field $\mathbb{K}$.*

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

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

Observe that $x^j_{m_j} > x^{j+1}_{m_j}$ because $x^j \leq x^{j+1}$ otherwise. With that in mind, it is not difficult to check that the points $y^1, \ldots, y^m \in \mathbb{Z}^m_+$ satisfy the conditions in Lemma 8.1, and hence there exists a discrete polymatroid of the form $\mathcal{D} = \mathcal{D}(\mathbf{a}, \mathbf{b})$ such that $y^i = y^i(\mathcal{D})$ for every $i = 1, \ldots, m$. In addition, from the previous results, $\Gamma_0(\mathcal{D})$ is a $\Pi$-hierarchical access structure with $\min_H \Gamma_0(\mathcal{D}) = \min_H\{y^1, \ldots, y^m\} = \{x^1, \ldots, x^r\}$. Therefore, $\Gamma = \Gamma_0(\mathcal{D})$ and, since $\mathcal{D}$ is linearly representable over every finite field, $\Gamma$ is a $\mathbb{K}$-vector space access structure if $\mathbb{K}$ is large enough. $\square$

# 9 A Characterization of Ideal Hierarchical Access Structures

By using the results in Sections 7 and 8, we present here a complete characterization of ideal hierarchical access structures. Moreover, we prove that every ideal hierarchical access structure is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. The next result is a consequence of Proposition 8.6 and the necessary conditions for a hierarchical access structure to be ideal given in Section 7. It provides a characterization of hierarchical access structures in which the number of participants in every hierarchical level is large enough in relation to the $H$-minimal points.

**Theorem 9.1.** *Let $\Pi = (P_1, \ldots, P_m)$ be an $m$-partition of a set $P$ and let $\Gamma$ be a $\Pi$-hierarchical access structure on $P$ with $\min_H \Gamma = \{x^1, \ldots, x^r\}$. For $j = 1, \ldots, r$, consider $m_j = \max(\operatorname{supp}(x^j))$ and suppose that $|P_{m_j}| > x^j_{m_j}$. Then $\Gamma$ is ideal if and only if*

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

*Moreover, in this situation $\Gamma$ is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$.*

*Proof.* The conditions are necessary because of the results in Section 7. We prove now that they are also sufficient. Suppose that the $H$-minimal points of $\Gamma$ are ordered in such a way that $m_i < m_j$ if $i < j$. Consider a set $\widehat{P} \supseteq P$ and an $m$-partition $\widehat{\Pi} = (\widehat{P}_1, \ldots, \widehat{P}_m)$ of $\widehat{P}$ such that $\widehat{P}_i \supseteq P_i$ for all $i = 1, \ldots, m$ and $|\widehat{P}_i| \geq \sum_{\ell=i}^{m_j} x^j_\ell$ if $m_{j-1} < i \leq m_j$. Let $\widehat{\Gamma}$ be the $\widehat{\Pi}$-hierarchical access structure with $\min_H \widehat{\Gamma} = \{x^1, \ldots, x^r\}$. By Proposition 8.6, $\widehat{\Gamma}$ is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$. Observe that $((x^j + H) \cap \widehat{\mathbf{P}}) \cap \mathbf{P} = (x^j + H) \cap \mathbf{P}$ for every $j = 1, \ldots, r$. This implies that the access structure $\Gamma$ is a minor of $\widehat{\Gamma}$. Specifically, $\Gamma = \widehat{\Gamma} \backslash (\widehat{P} \smallsetminus P)$. $\square$

Finally, we present our complete characterization of ideal hierarchical access structures in terms of the properties of the $H$-minimal points. Actually, we prove that a hierarchical access structure is ideal if and only if it is a minor of an access structure in the family that is presented in Section 8. Therefore every ideal hierarchical access structure is a $\mathbb{K}$-vector access structure for all large enough finite fields $\mathbb{K}$.

**Theorem 9.2.** *Let $\Pi = (P_1, \dots, P_m)$ be an $m$-partition of a set $P$ and let $\Gamma$ be a $\Pi$-hierarchical access structure on $P$ with $\min_H \Gamma = \{x^1, \dots, x^r\}$. Consider $m_j = \max(\operatorname{supp}(x^j))$ and suppose that the $H$-minimal points are ordered in such a way that $m_j \le m_{j+1}$. Then $\Gamma$ is ideal if and only if*

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

*Proof.* As before, the results in Section 7 imply that the given conditions are necessary. Suppose that the conditions are satisfied. Take $\widehat{x}^r = x^r$, and for $j = 1, \dots, r-1$ consider the point $\widehat{x}^j \in \mathbb{Z}_+^m$ defined by

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

As we did in the proof of Theorem 9.1, we extend the set $P$ of participants to a larger one. Consider a set $\widehat{P} \supseteq P$ and an $m$-partition $\widehat{\Pi} = (\widehat{P}_1, \dots, \widehat{P}_m)$ of $\widehat{P}$ such that $\widehat{P}_i \supseteq P_i$ for all $i = 1, \dots, m$ and $|P_i| \ge \sum_{\ell=i}^{m_j} \widehat{x}_\ell^j$ if $m_{j-1} < i \le m_j$. Let $\widehat{\Gamma}$ be the $\widehat{\Pi}$-hierarchical access structure on $\widehat{P}$ with $\min_H \widehat{\Gamma} = \{\widehat{x}^1, \dots, \widehat{x}^r\}$. It is not difficult to check that $\widehat{\Gamma}$ satisfies the conditions in Proposition 8.6, and hence it is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$. Consider the discrete polymatroid $\widehat{\mathcal{D}}' = (J_m', \widehat{h})$ associated to $\widehat{\Gamma}$ and take $\widehat{\mathcal{D}} = \widehat{\mathcal{D}}'(J_m) = (J_m, \widehat{h})$.

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

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

which implies that $\Gamma = \widehat{\Gamma} \backslash (\widehat{P} \smallsetminus P)$. Observe that $x^j - \widehat{x}^j \in H_0$, and hence $\Gamma \subseteq \widehat{\Gamma} \cap \mathbf{P}$. For $j = 1, \dots, r$, consider $A_j = (\widehat{x}^j + H_0) \cap \mathbf{P}$. Clearly, it is enough to prove that $A_j \subseteq \Gamma$ for all $j = 1, \dots, r$. Suppose that, on the contrary, there exists $j = 1, \dots, r$ such that $A_j \not\subseteq \Gamma$ while $A_k \subseteq \Gamma$ for all $k = 1, \dots, j-1$.

Suppose that $x^j \notin \mathcal{B}(\widehat{\mathcal{D}}, [1, m_j])$. Then $x^j \notin \min \widehat{\Gamma}$ and, since $x^j \in \widehat{\Gamma}$, there exists $z \in \min \widehat{\Gamma}$ with $z < x^j$. By Lemma 5.2, there exists an $H$-minimal point $x$ of $\widehat{\Gamma}$ such that $z - x \in H_0$, and hence $|x| = |z| < |x^j|$. This is impossible if $j = 1$. If $j > 1$, then $x = \widehat{x}^k$ for some $k < j$, and hence $z \in A_k \subseteq \Gamma$. Clearly, $z \in \min \Gamma$ and, by applying Lemma 5.2 again, $z - x^k \in H_0$. This implies that $x^j - x^k = (x^j - z) + (z - x^k) \in H$, a contradiction. Therefore, $x^j \in \mathcal{B}(\widehat{\mathcal{D}}, [1, m_j])$.

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

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

By combining Theorem 9.2 with the results in previous sections and the ones in [21], the results in this paper can be summarized in the following corollary.

**Corollary 9.3.** *Let $\Gamma$ be a hierarchical access structure. The following properties are equivalent:*

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

**Example 9.4.** Let $\Gamma$ be the weighted theshold access structure defined by the vector of weights $w = (7, 5, 4, 3)$ and the threshold $T = 13$ on the set of participants $P = P_1 \cup P_2 \cup P_3 \cup P_4$ with $|P_i| = 4$ for all $i = 1, \ldots, 4$. The $H$-minimal points of $\Gamma$ are $x^1 = (2, 0, 0, 0)$, $x^2 = (0, 1, 2, 0)$, and $x^3 = (0, 0, 1, 3)$. Since $x^2_2 > x^3_2$ and $|P_3| > x^2_3$, it follows from Theorem 9.2 that $\Gamma$ is not ideal.

**Example 9.5.** Let $P = P_1 \cup P_2 \cup P_3 \cup P_4$ be a set of participants and $t_1 < t_2 < t_3 < t_4$ some positive integers. Consider a 4-partite hierarchical scheme on $P$ in which all authorized subsets must have at least one participant from $P_1$, and also must have $t_1$ participants in $P_1$, or $t_2$ in $P_1 \cup P_2$, or $t_3$ in $P_1 \cup P_2 \cup P_3$, or $t_4$ in $P$. The access structure of this scheme, $\Gamma$, is a minor of $\Gamma'$, the access structure whose $H$-minimal points are $(1, 0, 0, t_4)$, $(1, 0, t_3, 0)$, $(1, t_2, 0, 0)$ and $(t_1, 0, 0, 0)$. Since $\Gamma'$ is ideal by Proposition 8.6, $\Gamma$ is ideal.

The access structures described in Example 5.4 with and Example 5.5 are ideal. If $\Gamma$ is a hierarchical access structure with just one $H$-minimal point $(t_1, t_2 - t_1, \ldots, t_m - t_{m-1})$, it is ideal by Proposition 8.6. The vector subspaces $V_0, \ldots, V_m$ that represent the polymatroid associated to $\Gamma$ satisfy $V_m \subset \ldots \subset V_1$, $V_0 \subset V_1$, and $V_0 \not\subseteq V_i$ for $i \neq 1$. If $\Gamma$ is a hierarchical access structure with $\min_H \Gamma = \{t_1\mathbf{e}^1, \ldots t_m\mathbf{e}^m\}$, then $\Gamma$ is also ideal and the vector subspaces $V_0, \ldots, V_m$ satisfy $V_0 \subset V_1 \subset \ldots \subset V_m$.

## References

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

[2] A. Beimel, E. Weinreb. Monotone Circuits for Monotone Weighted Threshold Functions. *Information Processing Letters* **97** (2006) 12–18.

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

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

[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** 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] O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *Advances in Cryptology, EUROCRYPT 2007, Lecture Notes in Comput. Sci.* **4515** (2007) 448–465.

[13] J. Herranz, G. Sáez. New Results on Multipartite Access Structures. *IEE Proceedings of Information Security* **153** (2006) 153–162.

[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 with three or four minimal qualified subsets. *Des. Codes Cryptogr.* **34** (2005) 17–34.

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

[21] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Computer Science* **4392** (2007) 273–290.

[22] J.Martí-Farré, C. Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Des. Codes Cryptogr.* **52** (2009) 1–14.

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

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

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

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

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

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

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

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

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

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

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

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

[35] T. Tassa. Hierarchical Threshold Secret Sharing. *J. Cryptology* **20** (2007) 237–264.

[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.