Ideal Hierarchical Secret Sharing Schemes [*]

Oriol Farràs [†] Carles Padró [‡]

June 30, 2011

Abstract

Hierarchical secret sharing is among the most natural generalizations of threshold secret sharing, and it has attracted a lot of attention since the invention of secret sharing until nowadays. Several constructions of ideal hierarchical secret sharing schemes have been proposed, but it was not known what access structures admit such a scheme. We solve this problem by providing a natural definition for the family of the hierarchical access structures and, more importantly, by presenting a complete characterization of the ideal hierarchical access structures, that is, the ones admitting an ideal secret sharing scheme. Our characterization is based on the well known connection between ideal secret sharing schemes and matroids and, more specifically, on the connection between ideal multipartite secret sharing schemes and integer polymatroids. In particular, we prove that every hierarchical matroid port admits an ideal linear secret sharing scheme over every large enough finite field. Finally, we use our results to present a new proof for the existing characterization of the ideal weighted threshold access structures.

Key words. Secret sharing, Ideal secret sharing schemes, Hierarchical secret sharing, Weighted threshold secret sharing, Multipartite secret sharing, Integer polymatroids, Boolean 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. Such a scheme is said to be *perfect* if 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 [31] 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].

[*] A previous version of this paper appeared in *Seventh IACR Theory of Cryptography Conference, TCC 2010, Lecture Notes in Computer Science* **5978** (2010) 219–236.

[†] Universitat Rovira i Virgili, Tarragona, Spain (e-mail: oriol.farras@urv.cat). His research was partially supported by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia through grant 2009 SGR 1135. He is with the UNESCO Chair in Data Privacy, but the views expressed in this paper are his own and do not commit UNESCO.

[‡] Nanyang Technological University, Singapore (e-mail: carlespl@ntu.edu.sg). His research was partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

One can think on many situations 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 [31] by proposing a simple modification of the threshold scheme to be used in hierarchical organizations. Namely, every participant receives as its share a certain number of shares from a threshold scheme, according to its position in the hierarchy. In this way a scheme for a *weighted threshold access structure* is obtained. That is, every participant has a weight (a positive integer) and a set is qualified if and only if its weight sum is at least a given threshold. This scheme is not ideal because the shares have in general larger length than the secret.

Every access structure admits a secret sharing scheme [4, 16], but in general the shares must have larger length than the secret [8, 10]. Very little is known about the optimal length of the shares in secret sharing schemes for general access structures, and there is a wide gap between the best known general lower and upper bounds. Nevertheless, it seems clear that we cannot expect to find efficient secret sharing schemes for all access structures. The reader is referred to the recent survey by Beimel [1] on this topic. Because of that, the construction of ideal secret sharing schemes for families of access structures with interesting properties for the applications is worth considering. This line of work was initiated by Kothari [18], who presented some ideas to construct ideal hierarchical secret sharing schemes, and by Simmons [32], who introduced two families of access structures, the *multilevel* and the *compartmented* ones, and conjectured them to admit ideal secret sharing schemes. Those access structures are *multipartite*, 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. In addition, multilevel access structures are hierarchical, that is, the participants in higher levels are more powerful than the ones in lower levels. Multipartite and, in particular, hierarchical secret sharing are arguably among the most natural generalizations of threshold secret sharing.

Simmons' conjecture was proved by Brickell [6], who proposed a general method, based on linear algebra, to construct ideal secret sharing schemes, and showed how to apply it to find ideal schemes for the multilevel and compartmented access structures. By using different kinds of polynomial interpolation, Tassa [33], and Tassa and Dyn [34] proposed constructions of ideal secret sharing schemes for several families of multipartite access structures that contain the multilevel and compartmented ones. Other proposals of ideal multipartite secret sharing schemes have been given in [14, 26]. All these constructions are based as well on the general linear algebra method by Brickell [6].

In spite of all those constructions of ideal hierarchical secret sharing schemes, it was not known what access structures admit such a scheme. This natural question, which is solved in this paper, is related to the more general problem of determining what access structures admit an ideal secret sharing scheme, that is, the characterization of the *ideal access structures*. This is a very important and long-standing open problem in secret sharing. Brickell and Davenport [7] 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 ideal secret sharing schemes by Brickell [6]: the ports of representable matroids are ideal access structures. The results in [7] have been generalized in [20] 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 have been given by Matúš [21, 22].

In addition to the search of general results, several authors studied this open problem for particular families of access structures. Some of them dealt with families of multipartite access structures. Beimel, Tassa and Weinreb [2] presented a characterization of the ideal weighted threshold access structures that generalizes the partial results in [23, 29]. Another important result about weighted threshold access structures have been obtained recently by Beimel and Weinreb [3]. They prove that all such access structures admit secret sharing schemes in which the size of the shares is quasi-polynomial in the number of users. A complete characterization of the ideal bipartite access structures was given in [29], and related results were given independently in [25, 27]. Partial results on the characterization of the ideal tripartite access structures appeared in [9, 14], and this question was solved in [12]. In every one of these families, all matroid ports are ports of representable matroids, and hence, all ideal access structures are *vector space access structures*, that is, they admit an ideal linear secret sharing scheme constructed by the method proposed by Brickell [6].

The characterization of the ideal tripartite access structures in [12] was obtained actually from the much more general results about ideal multipartite access structures in that paper. Specifically, by elaborating on the connection between ideal secret sharing and matroids, integer polymatroids are introduced in [12] as a new powerful combinatorial tool to study ideal multipartite secret sharing schemes.

2 Our Results

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

First of all, we formalize the concept of *hierarchical access structure* by introducing in Section 4 a natural definition for it. Basically, if a participant in a qualified subset is substituted by a *hierarchically superior* participant, the new subset must be still qualified. An access structure is *hierarchical* if, for any two given participants, one of them is hierarchically superior to the other. According to this definition, the family of the hierarchical access structures contains the multilevel access structures [6, 32], the hierarchical threshold access structures studied by Tassa [33] and by Tassa and Dyn [34], and also the weighted threshold access structures that were first considered by Shamir [31] and studied in [2, 3, 23, 29]. Duality and minors are fundamental concepts in secret sharing, as they are in matroid theory. Several important classes of access structures are closed by duality and minors, as for instance, matroid ports or vector space access structures. Similarly to multipartite and weighted threshold access structures, the family of the hierarchical access structures is closed by duality and minors. This is discussed in Section 7.

Our main result is Theorem 10.2, which provides a complete characterization of the ideal hierarchical access structures. In particular, we prove that all hierarchical matroid ports are ports of representable matroids. By combining this with the results in [20], we obtain the following theorem.

Theorem 2.1. *Let Γ be a hierarchical access structure. The following properties are equivalent.*

1. *Γ admits a vector space secret sharing scheme over every large enough finite field.*

2. *Γ is ideal.*

3. *Γ admits a secret sharing scheme in which the length of every share is less than $3/2$ times the length of the secret value.*

4. Γ is a matroid port.

This generalizes the analogous statement that holds for weighted threshold access structures as a consequence of the results in [2, 20]. Actually, as an application of our results, we present in Section 11 a new proof for the characterization of the ideal weighted threshold access structures by Beimel, Tassa and Weinreb [2].

Our starting point is the observation that every hierarchical access structure is determined by its *hierarchically minimal sets*, which are the minimal qualified sets that become unqualified if any participant is replaced by another one in a lower level in the hierarchy. Our results strongly rely on the connection between matroids and ideal secret sharing schemes discovered by Brickell and Davenport [7]. Moreover, since hierarchical access structures are in particular multipartite, the results and techniques in [12] about the characterization of ideal multipartite access structures, which are recalled in Section 6, are extremely useful. In particular, integer polymatroids play a fundamental role. Another important tool is the geometric representation introduced in [12, 29] for multipartite access structures, which is adapted in Section 4 to the hierarchical case by introducing the *hierarchically minimal points* that represent the hierarchically minimal sets. Our characterization of the ideal hierarchical access structures is given in terms of some properties of the h-minimal points that can be efficiently checked. By using our results, given a hierarchical access structure that is described by its hierarchically minimal points, one can efficiently determine whether it is ideal or not.

3 Notation

Some notation and terminology are needed to describe in Section 4 the geometric representation of multipartite access structures introduced in [12, 29], and also to present in Section 6 the basic facts about integer polymatroids. This notation will be used all through the paper.

We notate $\mathbb{Z}_+$ and $\mathbb{R}_+$ for the sets of the non-negative integer and real numbers, respectively. For every $i, j \in \mathbb{Z}$ we write $[i, j] = \{i, i+1, \dots, j\}$ if $i < j$, while $[i, i] = \{i\}$ and $[i, j] = \emptyset$ if $i > j$. For a positive integer m, we put $J'_m = [0, m]$ and $J_m = [1, m]$. Consider a finite set J. The *modulus* $|u|$ of a vector $u = (u_i)_{i \in J} \in \mathbb{Z}_+^J$ is defined by $|u| = \sum_{i \in J} u_i$. For every subset $X \subseteq J$, we notate $u(X) = (u_i)_{i \in X} \in \mathbb{Z}^X$. Observe that $|u(X)| = \sum_{i \in X} u_i$. The *support of* $u \in \mathbb{Z}^J$ is defined as $\operatorname{supp}(u) = \{i \in J : u_i \neq 0\}$ and we notate $m(x) = \max(\operatorname{supp}(x))$ for every $x \in \mathbb{Z}_+^{J_m} = \mathbb{Z}_+^m$. Finally, we consider the vectors $\mathbf{e}^i \in \mathbb{Z}^J$ such that $\mathbf{e}^i_j = 1$ if $j = i$ and $\mathbf{e}^i_j = 0$ otherwise.

We need to introduce as well two order relations among vectors. Given $u, v \in \mathbb{R}^J$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J$. In addition, for two vectors $u, v \in \mathbb{Z}_+^{J_m} = \mathbb{Z}_+^m$, we put $u \preceq v$ if $\sum_{i=1}^j u_i \leq \sum_{i=1}^j v_i$ for every $j \in J_m$. In this situation, and for a reason that will be made apparent later, we say that the vector v is *hierarchically superior* to the vector u. The latter order relation was introduced in [34, Definition 4.2], also in the framework of hierarchical secret sharing.

We notate $\mathcal{P}(P)$ for the power set of P, that is, the set of all subsets of P. A sequence $\Pi = (\Pi_1, \dots, \Pi_m)$ of subsets of P is called here an *m-partition of P* if $P = \Pi_1 \cup \dots \cup \Pi_m$ and $\Pi_i \cap \Pi_j = \emptyset$ whenever $i \neq j$. Observe that some of the parts may be empty. For an m-partition Π of a set P, we consider the mapping $\Pi \colon \mathcal{P}(P) \to \mathbb{Z}_+^m$ defined by $\Pi(A) = (|A \cap \Pi_1|, \dots, |A \cap \Pi_m|)$. We write $\mathbf{p} = \Pi(P) = (|\Pi_1|, \dots, |\Pi_m|)$ and $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{u \in \mathbb{Z}_+^m : u \leq \mathbf{p}\}$.

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 as, for instance, the weighted threshold access structures, the multilevel access structures [6, 32] and the hierarchical threshold access structures [33].

An *access structure* on a finite set P of participants is a monotone increasing family $\Gamma \subseteq \mathcal{P}(P)$ of subsets of P. That is, if $A \subseteq B \subseteq P$ and $A \in \Gamma$, then $B \in \Gamma$. Given an access structure Γ, its members are called the *qualified subsets.* The participants that are not in any minimal qualified subset are called *redundant*. An access structure is *connected* if there is no redundant participant.

Let Γ be an access structure on 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 $A \subseteq P \backslash \{p, q\}$ 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*. Clearly, this is an equivalence relation, and the hierarchical relation $\preceq$ induces a partial order on the set of the equivalence classes. Observe that an access structure is hierarchical if and only if this is a total order.

For a partition Π of the set P, an access structure Γ on P is said to be Π-*partite* if every pair of participants in the same part Π_i are hierarchically equivalent. A different but equivalent definition for this concept is given in [12]. If m is the number of parts in Π, such structures are called *m-partite access structures*. An m-partite access structure is said to be *strictly m-partite* if all parts are nonempty and participants in different parts are not hierarchically equivalent.

A Π-partite access structure is said to be Π-*hierarchical* if $q \preceq p$ for every pair of participants $p \in \Pi_i$ and $q \in \Pi_j$ with $i < j$. That is, the participants in the first level are hierarchically superior to those in the second level and so on. Obviously, an access structure is hierarchical if and only if it is Π-hierarchical for some partition Π of the set of participants. The term *m-hierarchical access structure* applies to every Π-hierarchical access structure with $|\Pi| = m$.

We describe in the following the geometrical representation of multipartite access structures that was introduced in [12, 29]. Observe that a subset $A \subseteq P$ is in the Π-partite access structure Γ if and only if the vector $\Pi(A) \in \mathbb{Z}_+^m$ in is $\Pi(\Gamma)$. Then Γ is univocally represented by the set of vectors $\Pi(\Gamma) \subseteq \mathbf{P}$. By an abuse of notation, we will use Γ to denote both a Π-partite access structure on P and the corresponding set $\Pi(\Gamma)$ of vectors in $\mathbf{P}$. If two vectors $u, v \in \mathbf{P}$ are such that $u \leq v$ and $u \in \Gamma$, then $v \in \Gamma$. This is due to the fact that Γ is a monotone increasing family of subsets. Therefore, $\Gamma \subseteq \mathbf{P}$ is determined by the family $\min \Gamma \subseteq \mathbf{P}$ of its minimal vectors. We are using here an abuse of notation as well, because $\min \Gamma$ denotes also the family of minimal subsets of the access structure Γ.

Let Γ be a Π-hierarchical access structure. If a set $B \subseteq P$ is obtained from a set $A \subseteq P$ by replacing some participants by participants in superior levels, and $u = \Pi(A)$ and $v = \Pi(B)$, then $\sum_{i=1}^{j} u_i \leq \sum_{i=1}^{j} v_i$ for every $j \in J_m$, that is the vector v is hierarchically superior to the vector u. The vectors in $\mathbf{P}$ that are minimal according to this order are called the *hierarchically minimal vectors of* Γ, and the set of these vectors is denoted by $\operatorname{hmin} \Gamma$. Clearly, if $u, v \in \mathbf{P}$ are such that $u \in \Gamma$ and $u \preceq v$, then $v \in \Gamma$. This implies that every Π-hierarchical access structure is determined by the partition Π and its hierarchically minimal vectors. Since $u \preceq v$ if $u \leq v$, we have that $\operatorname{hmin} \Gamma \subseteq \min \Gamma$, and hence describing a hierarchical access structure by its hierarchically minimal vectors is more compact than doing so by its minimal vectors. The *hierarchically minimal sets of* Γ are the sets $A \subseteq P$ such that $\Pi(A)$ is a hierarchically minimal vector. Observe that a subset of participants is hierarchically minimal if and only if it is a minimal qualified subset such that it is impossible to replace a participant in it with another participant in an inferior level and still remain qualified.

We present next three examples of families of hierarchical access structures.

Example 4.1. *A* weighted threshold *access structure* Γ *is defined from a real* weight vector $w = (w_1, \dots, w_m) \in \mathbb{R}^m$ *with* $w_1 > w_2 > \cdots > w_m > 0$ *and a positive real* threshold $T > 0$. *Namely,* Γ *is the* Π*-partite access structure defined by*

$$\Gamma = \{u \in \mathbf{P} \,:\, u \cdot w = u_1 w_1 + \cdots + u_m w_m \geq T\}.$$

That is, every participant has a weight and a set is qualified if and only if its weight sum is at least the threshold. Clearly, such an access structure is Π*-hierarchical.*

Example 4.2. *Brickell [6] showed how to construct ideal schemes for the multilevel structures proposed by Simmons [32]. These are* Π*-partite access structures of the form*

$$\Gamma = \left\{ u \in \mathbf{P} \,:\, \sum_{j=1}^{i} u_j \geq t_i \text{ for some } i \in J_m \right\}$$

for some monotone increasing sequence of integers $0 < t_1 < \ldots < t_m$*. Clearly, such an access structure is* Π*-hierarchical and, if* $|\Pi_i| \geq t_i$ *for every* $i = 1, \dots, m$*, its hierarchically minimal vectors are* $\operatorname{hmin} \Gamma = \{t_1 \mathbf{e}^1, \dots, t_m \mathbf{e}^m\}$*.*

Example 4.3. *Tassa [33] presented a construction of ideal secret sharing schemes for another family of hierarchical threshold access structures. Namely, given integers* $0 < t_1 < \ldots < t_m$*, consider the* Π*-partite access structure*

$$\Gamma = \left\{ u \in \mathbf{P} \,:\, \sum_{j=1}^{i} u_j \geq t_i \text{ for every } i \in J_m \right\}.$$

Such an access structure is Π*-hierarchical and, if the number of participants in every level is large enough, its only hierarchically minimal vector is* $(t_1, t_2 - t_1, \dots, t_m - t_{m-1})$*.*

5 Polymatroids and Matroids

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

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

If the rank function h is integer-valued, we say that $\mathcal{S}$ is an *integer polymatroid*. An integer polymatroid such that $h(X) \leq |X|$ for every $X \subseteq J$ is called a *matroid*. Readers that are unfamiliar with Matroid Theory are referred to the textbooks [28, 35]. A detailed presentation about polymatroids can be found in [30, Chapter 44] or [15].

While matroids abstract some properties related to linear dependency of collections of vectors in a vector space, integer polymatroids do the same with collections of subspaces. Let V be a $\mathbb{K}$-vector space, and let $(V_i)_{i \in J}$ be a finite collection of subspaces of V. 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 an integer polymatroid. Integer polymatroids and, in particular, matroids that can be defined in this way are said to be $\mathbb{K}$ *-representable*. Observe that, in a representable matroid, $\dim V_i \leq 1$ for every $i \in J$, and hence representations of matroids are considered as collections of vectors in a vector space.

Example 5.1. *We present here a family of integer polymatroids that is specially useful for our purposes. Let B be a finite set and consider a family $(B_i)_{i\in J}$ of subsets of B. The mapping $h\colon \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \left|\bigcup_{i\in X} B_i\right|$ is clearly the rank function of an integer polymatroid. Integer polymatroids that can be defined in this way are called* Boolean polymatroids*. Such integer polymatroids are $\mathbb{K}$-representable over every field $\mathbb{K}$. This is proved by identifying the set B to a basis of $V = \mathbb{K}^{|B|}$ and considering the subspaces $V_i = \langle B_i \rangle \subseteq V$.*

A polymatroid $\mathcal{S}$ with ground set J is determined by its *independent vectors*, which are the elements in the convex polytope

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

Actually, the rank function h of $\mathcal{S}$ satisfies $h(X) = \max\{|u(X)| \,:\, u \in \mathcal{T}\}$ for every $X \subseteq J$. The maximal elements in $\mathcal{T}$, that is, the vectors $u \in \mathcal{T}$ such that there does not exist any $v \in \mathcal{T}$ with $u < v$, are the *bases of the polymatroid* $\mathcal{S}$. All bases of a polymatroid have the same modulus, which equals $h(J)$, the *rank of the polymatroid* $\mathcal{S}$. More details about these concepts can be found in [35] or [30, Chapter 44].

By formalizing known results from combinatorial optimization [13, 30] and discrete convex analysis [24], Herzog and Hibi [15] presented two characterizations of integer polymatroids, one in terms of the integer independent vectors and another one in terms of the integer bases. Complete proofs for the facts that are stated in the following are given in [15]. Let $\mathcal{Z}$ be an integer polymatroid with ground set J. Consider the set $\mathcal{D}$ of the *integer independent vectors* of $\mathcal{Z}$. That is, if $\mathcal{T} \subseteq \mathbb{R}_+^J$is the set of independent vectors of $\mathcal{Z}$, then

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

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

1. $\mathcal{D}$ is nonempty and finite.

2. If $u \in \mathcal{D}$ and $v \in \mathbb{Z}_+^J$ are such that $v \leq u$, then $v \in \mathcal{D}$.

3. For every pair of vectors $u, v \in \mathcal{D}$ with $|u| < |v|$, there exists $i \in J$ with $u_i < v_i$ such that $u + \mathbf{e}^i \in \mathcal{D}$.

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

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

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

As it happened with the integer independent vectors, every integer polymatroid is univocally determined by the family $\mathcal{B} \subseteq \mathbb{Z}_+^J$ of their integer bases.

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

If $\mathcal{D}$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}$ on J, then, for every $X \subseteq J$, the set $\mathcal{D}|X = \{u(X) : u \in \mathcal{D}\} \subseteq \mathbb{Z}_+^X$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}|X$ with ground set X. Clearly, the rank function $h|X$ of this polymatroid satisfies $(h|X)(Y) = h(Y)$ for every $Y \subseteq X$. Because of that, we will use the same symbol to denote both rank functions.

For an integer polymatroid $\mathcal{Z}$ and a subset $X \subseteq J$ of the ground set, we write $\mathcal{B}(\mathcal{Z}, X)$ to denote the family of the independent vectors $u \in \mathcal{D}$ such that $\operatorname{supp}(u) \subseteq X$ and $|u| = h(X)$. Observe that there is a natural bijection between $\mathcal{B}(\mathcal{Z}, X)$ and the family of bases of the integer polymatroid $\mathcal{Z}|X$.

6 Integer Polymatroids and Multipartite Matroid Ports

The aim of this section is to summarize the results in [12] about ideal multipartite secret sharing schemes, which play a central role in our characterization of the ideal hierarchical access structures.

For a polymatroid $\mathcal{S}$ and an element $p_0 \in J$ in the ground set, the family

$$\Gamma_{p_0}(\mathcal{S}) = \{A \subseteq J \setminus \{p_0\} : h(A \cup \{p_0\}) = h(A)\}$$

of subsets of $J \setminus \{p_0\}$ is monotone increasing, and hence it is an access structure on $J \setminus \{p_0\}$. If $\mathcal{S}$ is a matroid, then the access structure $\Gamma_{p_0}(\mathcal{S})$ is called the *port of the matroid $\mathcal{S}$ at the point p_0*. As a consequence of the results by Brickell [6] and by Brickell and Davenport [7], matroid ports play a very important role in secret sharing. Ports of $\mathbb{K}$-representable matroids are called *$\mathbb{K}$-vector space access structures*. Such an access structure admits an ideal scheme that is constructed according to the method given by Brickell [6]. In addition, Brickell and Davenport [7] proved that the access structure of every ideal secret sharing scheme is a matroid port. This result was generalized in [20] by proving that the access structure of a secret sharing scheme is a matroid port if the length of every share is less than $3/2$ times the length of the secret.

We introduce next a class of multipartite access structures that are defined by integer polymatroids. The interest of such access structures is due to the results from [12], which are summarized in Theorem 6.2.

Definition 6.1. *Let Π be an m-partition of a set P of participants. Consider an integer polymatroid $\mathcal{Z}'$ on J'_m with $h(\{0\}) = 1$ and $h(\{i\}) \le |\Pi_i|$ for every $i \in J_m$, and take $\mathcal{Z} = \mathcal{Z}'|J_m$. The Π-partite access structure $\Gamma_0(\mathcal{Z}', \Pi)$ is defined in the following way: a vector $u \in \mathbf{P} \subseteq \mathbb{Z}_+^m = \mathbb{Z}_+^{J_m}$ is in $\Gamma_0(\mathcal{Z}', \Pi)$ if and only if there exist a subset $X \subseteq J_m$ and a vector $v \in \mathcal{B}(\mathcal{Z}, X)$ such that $v \le u$ and $h(X \cup \{0\}) = h(X)$ (that is, X is in the access structure $\Gamma_0(\mathcal{Z}')$).*

Theorem 6.2 ([12])**.** *Let Π be an m-partition of a set P. A Π-partite access structure Γ on P is a matroid port if and only if it is of the form $\Gamma_0(\mathcal{Z}', \Pi)$ for some integer polymatroid $\mathcal{Z}'$ on J'_m with $h(\{0\}) = 1$ and $h(\{i\}) \le |\Pi_i|$ for every $i \in J_m$. Moreover, in this situation the integer polymatroid $\mathcal{Z}'$ is univocally determined by Γ if this access structure is connected. In addition, if $\mathcal{Z}'$ is $\mathbb{K}$-representable, then $\Gamma_0(\mathcal{Z}', \Pi)$ is an $\mathbb{L}$-vector space access structure for every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$.*

Example 6.3. *Given integers $1 = t_0 \le t_1 < \cdots < t_m$, consider the Boolean polymatroid $\mathcal{Z}'$ with ground set J'_m defined by the subsets $B_i = [1, t_i] \subseteq B = [1, t_m]$. We affirm that the Π-partite access structures $\Gamma_0(\mathcal{Z}', \Pi)$ defined by such polymatroids coincide with the ones introduced in Example 4.2. That is, $\Gamma_0(\mathcal{Z}', \Pi)$ is equal to the hierarchical access structure*

$$\Gamma = \left\{ u \in \mathbf{P} \, : \, \sum_{j=1}^{i} u_j \ge t_i \text{ for some } i \in J_m \right\}.$$

Observe that the access structure $\Gamma_0(\mathcal{Z}')$ contains all nonempty subsets of J_m. In addition, $v \in \mathbb{Z}_+^{J'_m}$ is an independent vector of $\mathcal{Z}'$ if and only if $\sum_{j=0}^{i} v_j \le t_i$ for all $i \in J'_m$. Consider a vector $u \in \mathbf{P}$ that is in Γ and let i_0 be the smallest element in J_m such that $\sum_{j=1}^{i_0} u_j \ge t_{i_0}$. Clearly, there exists a vector $v \in \mathcal{B}(\mathcal{Z}, [1, i_0])$, where $\mathcal{Z} = \mathcal{Z}'|J_m$, such that $v_j = u_j$ for $j \in [1, i_0 - 1]$, which implies that $u \in \Gamma_0(\mathcal{Z}', \Pi)$. Conversely, consider $v \in \mathcal{B}(\mathcal{Z}, X)$, where $\emptyset \ne X \subseteq J_m$. Observe that $h(X) = t_{i_0}$, where $i_0 = \max X$. Therefore $\sum_{j=1}^{i_0} v_j = |v| = t_{i_0}$, and hence $v \in \Gamma$. This concludes the proof of our affirmation. Since $\mathcal{Z}'$ is a Boolean polymatroid, it is representable over every finite field. Therefore, Γ is a vector space access structure over every large enough finite field. Actually, this fact was constructively proved by Brickell [6].

Example 6.4. *Given integers $0 = t_0 < t_1 < \cdots < t_m$, consider now the set $B = [1, t_m]$ and the subsets $B_0 = \{1\}$ and $B_i = [t_{i-1} + 1, t_m]$ for $i \in J_m$. If $\mathcal{Z}'$ is the Boolean polymatroid on J'_m defined by those sets, then the Π-partite access structure $\Gamma_0(\mathcal{Z}', \Pi)$ is one of the Π-hierarchical access structures introduced in Example 4.3. Specifically, $\Gamma_0(\mathcal{Z}', \Pi) = \Gamma$, where*

$$\Gamma = \left\{ u \in \mathbf{P} \, : \, \sum_{j=1}^{i} u_j \ge t_i \text{ for every } i \in J_m \right\}.$$

We prove this assertion in the following. Observe that $X \subseteq J_m$ is in the access structure $\Gamma_0(\mathcal{Z}')$ if and only if $1 \in X$. Clearly, $h(X) = t_m - t_{i_0 - 1}$ if $X \subseteq J_m$ and $i_0 = \min X$. In particular, $h(X) = t_m$ if $1 \in X$, and hence $|u| = t_m$ if $u \in \min \Gamma_0(\mathcal{Z}', \Pi)$. Obviously, the same applies to the vectors in $\min \Gamma$. Consider a vector $u \in \mathbf{P}$ with $|u| = t_m$ and a subset $X \subseteq J_m$, and take $i_0 = \min X$. Then

$$|u(X)| \le \sum_{j=i_0}^{m} u_j = t_m - \sum_{j=1}^{i_0 - 1} u_j,$$

and hence $|u(X)| \le h(X)$ if and only if $\sum_{j=1}^{i_0 - 1} u_j \ge t_{i_0 - 1}$. Clearly, this proves our assertion. Therefore, each of these Π-hierarchical access structures is a vector space access structure over every large enough finite field. A constructive proof of this fact was given by Tassa [33].

7 Operations on Hierarchical Access Structures

Duality and minors are fundamental concepts in matroid theory, and they have their counterpart in secret sharing. Several important classes of access structures are closed by duality and minors, as for instance, matroid ports and $\mathbb{K}$-vector space access structures. The *dual* of an access structure Γ on a set P is the access structure Γ^* on the same set defined by $\Gamma^* = \{A \subseteq P \, : \, P \backslash A \notin \Gamma\}$. It is not difficult to prove that Γ is Π-partite if and only if Γ^* is so. For a subset $B \subseteq P$, we define the access structures $\Gamma \backslash B$ and Γ / B on the set $P \backslash B$ by $\Gamma \backslash B = \{A \subseteq P \backslash B \, : \, A \in \Gamma\}$ and $\Gamma / B = \{A \subseteq P \backslash B \, : \, A \cup B \in \Gamma\}$. Every access structure that can be obtained from Γ by repeatedly applying the operations $\backslash$ and $/$ is called a *minor* of Γ. If Γ is a Π-partite access structure, then the minors $\Gamma\backslash B$ and Γ/B are $(\Pi\backslash B)$-partite access structures, where $\Pi\backslash B = (\Pi_1\backslash B, \dots, \Pi_m\backslash B)$, a partition of $P\backslash B$. If $\Pi(B) = b$, then the geometric representations of these access structures are $\Gamma\backslash B = \{x \in \mathbb{Z}_+^m : x \le \mathbf{p} - b \text{ and } x \in \Gamma\}$ and $\Gamma/B = \{x \in \mathbb{Z}_+^m : x \le \mathbf{p} - b \text{ and } x + b \in \Gamma\}$.

Proposition 7.1. *The class of the hierarchical access structures is minor-closed and duality-closed. The same applies to the class of the weighted threshold access structures.*

Proof. Let Γ be a hierarchical access structure. Consider $u \in \Gamma^*$ and $v \in \mathbf{P}$ such that $u \preceq v$. Observe that $\mathbf{p} - v \preceq \mathbf{p} - u \notin \Gamma$, and hence $\mathbf{p} - v \notin \Gamma$ and $v \in \Gamma^*$. Consider now the minors $\Gamma\backslash B$ and Γ/B for some $B \subseteq P$, and take $b = \Pi(B)$. Consider vectors $0 \le u, v \le \mathbf{p} - b$ with $u \preceq v$. If $u \in \Gamma\backslash B$, then $u \in \Gamma$. This implies that $v \in \Gamma$ and hence $v \in \Gamma\backslash B$. If $u \in \Gamma/B$, then $u + b \in \Gamma$ and hence $v + b \in \Gamma$ because $u + b \preceq v + b$. Therefore, $v \in \Gamma/B$.

Let Γ be the weighted threshold access structure defined by the weight vector w and the threshold T and take $W = \sum_{i=1}^m n_i w_i$, where $n_i = |\Pi_i|$, that is, W is the weight sum of all participants in P. Let W' be the maximum weight sum of all unqualified subsets and take $\epsilon > 0$ such that $W' + \epsilon < T$. Then Γ^* is the weighted threshold access structure given by the same weights as Γ but with threshold $T^* = W - W' - \epsilon$. The access structure $\Gamma\backslash B$ is defined by the same weights and threshold as Γ, while the threshold of Γ/B is $T - |w(B)|$. □

Let P' and P'' be two disjoint sets and let Γ' and Γ'' be access structures on P' and P'', respectively. The *composition of* Γ' *and* Γ'' *over* $p \in P'$, which is denoted by $\Gamma'[\Gamma''; p]$, is the access structure on the set of participants $P = P' \cup P''\backslash\{p\}$ that is defined as follows a subset $A \subseteq P$ is in $\Gamma'[\Gamma''; p]$ if and only if

- $A \cap P' \in \Gamma'$, or
- $(A \cup \{p\}) \cap P' \in \Gamma'$ 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 [19]. 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 Γ' is $(P_1, \dots, P_r)$-partite and Γ'' is $(P_{r+1}, \dots, P_{r+s})$-partite, and take $p \in P_r$. Then the composition $\Gamma'[\Gamma''; p]$ is $(P_1', \dots, P_{r+s}')$-partite, where $P_r' = P_r\backslash\{p\}$ and $P_i' = P_i$ for $i \ne r$. If Γ' and Γ'' are hierarchical and $p \in P_r$ then $\Gamma'[\Gamma''; p]$ is also hierarchical, and the same applies to weighted threshold access structures. Observe that the composition is made over a participant in the lowest level of Γ'.

8 Hierarchical Matroid Ports

We explain in the following how the hierarchically minimal vectors of an m-hierarchical matroid port can be determined from its associated integer polymatroid. We prove first some technical lemmas that apply to every integer polymatroid. Specifical results on integer polymatroids that define hierarchical matroid ports will be given afterwards.

Lemma 8.1. *Consider an integer polymatroid $\mathcal{Z}$ on J_m, a subset $X \subseteq J_m$, and a vector $y \in \mathcal{B}(\mathcal{Z}, X)$ that is hierarchically minimal in $\mathcal{B}(\mathcal{Z}, X)$. Then y is the hierarchically minimum vector of $\mathcal{B}(\mathcal{Z}, X)$, that is $y \preceq x$ for every $x \in \mathcal{B}(\mathcal{Z}, X)$.*

Proof. Suppose that the set $R = \mathcal{B}(\mathcal{Z}, X) \setminus \{x \in \mathcal{B}(\mathcal{Z}, X) : y \preceq x\}$ is nonempty and consider a vector $x \in R$ that is hierarchically minimal in R. Let $i \in X$ be the smallest index with $x_i \neq y_i$. If $x_i < y_i$, there exists $j \in X$ with $j > i$ such that $x_j > y_j$ and $z = y + \mathbf{e}^j - \mathbf{e}^i \in \mathcal{B}(\mathcal{Z}, X)$. Observe that $z \prec y$, a contradiction with the fact that y is hierarchically minimal in $\mathcal{B}(\mathcal{Z}, X)$. If $x_i > y_i$, there exists $j \in X$ with $j > i$ such that $x_j < y_j$ and $u = x + \mathbf{e}^j - \mathbf{e}^i \in \mathcal{B}(\mathcal{Z}, X)$. Then $u \notin R$ because x is hierarchically minimal in R and $u \prec x$. This implies that $y \preceq u \prec x$, a contradiction again. □

Let $\mathcal{Z}$ be an integer polymatroid on J_m. For every $i \in J_m$, consider the vector $y^i = y^i(\mathcal{Z}) \in \mathbb{Z}_+^m$ defined by $y^i_j = h([j, i]) - h([j+1, i])$. Observe that $|y^i([s, i])| = \sum_{j=s}^{i} y^i_j = h([s, i])$ for every $s \in [1, i]$. Actually, these vectors are vertices of the polytope $\mathcal{T} \subseteq \mathbb{R}_+^m$ formed by the (real) independent vectors of $\mathcal{Z}$. A description of all vertices of $\mathcal{T}$ can be found, for instance, in [11, Theorem 22] and [15, Proposition 1.3].

Lemma 8.2. *If $1 \le j \le i < m$, then $y^i_j \ge y^{i+1}_j$.*

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

Lemma 8.3. *For every $i \in J_m$, the vector y^i is the hierarchically minimum vector of $\mathcal{B}(\mathcal{Z}, [1, i])$.*

Proof. By Lemma 8.1, it is enough to prove that y^i is a hierarchically minimal vector of $\mathcal{B}(\mathcal{Z}, [1, i])$. We prove first that $y^i \in \mathcal{B}(\mathcal{Z}, [1, i])$. Take $X \subseteq [1, i]$ and, for $j \in [1, i+1]$, consider $X_j = X \cap [j, i]$. Then

$$\begin{aligned} |y^i(X)| &= \sum_{j \in X} y^i_j = \sum_{j \in X} (h([j, i]) - h([j+1, i])) \\ &\le \sum_{j \in X} (h(X_j) - h(X_{j+1})) = h(X). \end{aligned}$$

The inequality holds because $X_{j+1} = X_j \cap [j+1, i]$ and $[j, i] = X_j \cup [j+1, i]$. Since $y^i_j = 0$ for all $j > i$, this implies that y^i is an independent vector of $\mathcal{Z}$ and, moreover, $y^i \in \mathcal{B}(\mathcal{Z}, [1, i])$ because $|y^i| = h([1, i])$. We prove next that y^i is hierarchically minimal in $\mathcal{B}(\mathcal{Z}, [1, i])$. If not, there exists $z \in \mathcal{B}(\mathcal{Z}, [1, i])$ with $z \prec y^i$. Since $|z| = |y^i|$, there exists $s \in [1, i]$ for which $\sum_{j=1}^{s-1} (y^i_j - z_j) > 0$ and $\sum_{j=s}^{i} (y^i_j - z_j) < 0$. Then $|z([s, i])| = \sum_{j=s}^{i} z_j > \sum_{j=s}^{i} y^i_j = h([s, i])$, a contradiction because $z \in \mathcal{B}(\mathcal{Z}, [1, i])$. □

For the remaining of this section, we assume that $\mathcal{Z}'$ is an integer polymatroid on J'_m with $h(\{0\}) = 1$ such that, for an m-partition Π of a set P with $|\Pi_i| \ge h(\{i\})$ for every $i \in J_m$, the access structure $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ is Π-hierarchical. We consider the integer polymatroid $\mathcal{Z} = \mathcal{Z}' | J_m$ and the vectors $y^i = y^i(\mathcal{Z})$. Recall the notation $m(x) = \max(\operatorname{supp}(x))$.

Lemma 8.4. *If $x \in \mathbf{P}$ is a minimal vector of Γ, then $x \in \mathcal{B}(\mathcal{Z}, [1, m(x)])$.*

Proof. Take $X = \operatorname{supp}(x)$. Since $x \in \mathcal{B}(\mathcal{Z}, X)$, it is enough to prove that $h(X) = h([1, m(x)])$. Specifically, we are going to prove that $h(X \cup \{j\}) = h(X)$ for every $j \in [1, m(x)] \setminus X$. Clearly this is the case if $\Pi_j = \emptyset$. In any other case, consider the vector $x' = x + \mathbf{e}^j - \mathbf{e}^{m(x)} \in \mathbf{P}$. Since Γ is Π-hierarchical, $x' \in \Gamma$, and hence there exists $Y \subseteq X \cup \{j\}$ with $Y \in \Gamma_0(\mathcal{Z}')$ and a vector $y \in \mathcal{B}(\mathcal{Z}, Y)$ with $y \le x'$. Clearly, $y_j \neq 0$ because $x \in \min \Gamma$. Thus, $y_j = 1$ and $j \in Y$. Since h is submodular, $h(X \cup \{j\}) + h(Y \setminus \{j\}) \le h(X) + h(Y)$. Therefore, $h(X \cup \{j\}) = h(X)$ if $h(Y) = h(Y \setminus \{j\})$. Suppose now that $h(Y \setminus \{j\}) \le h(Y) - 1$. Observe that $h(Y \setminus \{j\}) \ge |y(Y \setminus \{j\})| = |y(Y)| - 1 = h(Y) - 1$ because $y \in \mathcal{B}(\mathcal{Z}, Y)$. Hence, $h(Y \setminus \{j\}) = h(Y) - 1$ and

$y - \mathbf{e}^j \in \mathcal{B}(\mathcal{Z}, Y\backslash\{j\})$. Observe that $y - \mathbf{e}^j \notin \Gamma$ because $y - \mathbf{e}^j < x$. Thus, $Y\backslash\{j\} \notin \Gamma_0(\mathcal{Z})$, and hence

$$h((Y\backslash\{j\}) \cup \{0\}) = h(Y\backslash\{j\}) + 1 = h(Y).$$

The submodularity of h implies inequality (1) in the following calculation.

$$\begin{aligned} h(X \cup \{j, 0\}) + h(Y) &= h(X \cup \{j, 0\}) + h((Y\backslash\{j\}) \cup \{0\}) \\ &\le h(X \cup \{0\}) + h(Y \cup \{0\}) \qquad (1) \\ &= h(X) + h(Y). \end{aligned}$$

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

Let $t_0 = t_0(\mathcal{Z}')$ be the minimum value $t \in J_m$ with $h([0, t]) = h([1, t])$, that is, the minimum value $t \in J_m$ such that $[1, t] \in \Gamma_0(\mathcal{Z}')$. The following result describes how the hierarchically minimal vectors of a hierarchical matroid port are determined from its associated integer polymatroid. Its proof is straightforward from the previous lemmas in this section.

Lemma 8.5. *If $x \in \mathbf{P}$ is a hierarchically minimal vector of Γ, then $x = y^{m(x)}$. As a consequence,* $\operatorname{hmin}\Gamma = \operatorname{hmin}\{y^{t_0}(\mathcal{Z}), \dots, y^m(\mathcal{Z})\}$.

We need to prove some more technical results before concluding this section with Proposition 8.10. The first one describes some hierarchical properties of the vectors $y^i = y^i(\mathcal{Z})$.

Lemma 8.6. *The following properties hold whenever $1 \le i < j \le m$.*

1. *$y^j \preceq y^i$ if and only if $|y^j| = |y^i|$.*
2. *$y^i \preceq y^j$ if and only if $y^i_\ell = y^j_\ell$ for all $\ell \in [1, i]$. In this situation, $y^i \le y^k$ for every $k \in [i + 1, j]$.*
3. *$y^i \preceq y^j$ if and only if $h([1, j]) = h([1, i]) + h([i + 1, j])$.*

Proof. Properties 1 and 2 are straightforward. We prove Property 3. By Property 2, $y^i \preceq y^j$ if and only if

$$\begin{aligned} h([s, i]) &= \sum_{k=s}^{i} y^i_k = \sum_{k=s}^{i} y^j_k = \sum_{k=s}^{i} (h([k, j]) - h([k + 1, j])) \\ &= h([s, j]) - h([i + 1, j]) \end{aligned}$$

for every $s \le i$. Moreover, if $h([i + 1, j]) = h([1, j]) - h([1, i])$, then

$$h([i + 1, j]) = h([1, j]) - h([1, i]) \le h([s, j]) - h([s, i]) \le h([i + 1, j])$$

for every $s \le i$. □

Lemma 8.7. *For every $z \in \min\Gamma$ there exists a unique $x \in \operatorname{hmin}\Gamma$ such that $x \preceq z$ and $|x| = |z|$.*

Proof. Let $i \in [m(z), m]$ be the maximum value with $|y^i| = |y^{m(z)}|$. Clearly, $y^i \preceq z$ and $|y^i| = |z|$. We only have to prove that y^i is hierarchically minimal in $\{y^{t_0}, \dots, y^m\}$. If $j \in [i + 1, m]$, then $|y^j| > |y^i|$, and hence $y^j \not\preceq y^i$ by Lemma 8.6 (1). Suppose that there exists $j \in [t_0, i - 1]$ such that $y^j \preceq y^i$. By Lemma 8.6 (2), $|y^j| < |y^i| = |y^{m(z)}|$, and hence $j < m(z)$ and $y^j \le y^{m(z)}$. This implies that $h([1, m(z)]) = h([1, j]) + h([j+1, m(z)])$ by Lemma 8.6 (3). Since $z \in \mathcal{B}(\mathcal{Z}, [1, m(z)])$, we have that $|z| = h([1, m(z)])$, while $|z([1, j])| \le h([1, j])$ and $|z([j+1, m(z)])| \le h([j+1, m(z)])$. Therefore, $|z([1, j])| = h([1, j])$, and hence $z' = \sum_{\ell=1}^{j} z_\ell \, \mathbf{e}^\ell \in \Gamma$, a contradiction with $z' < z$ and $z \in \min\Gamma$. □

Lemma 8.8. *Let $x, y \in \mathbf{P}$ be two different hierarchically minimal vectors of Γ with $m(x) < m(y)$ such that there is not any hierarchically minimal vector z with $m(x) < m(z) < m(y)$. If $x_i > y_i$ for some $i \in [1, m(x) - 1]$, then $|\Pi_j| = x_j$ for all $j \in [i + 1, m(x)]$.*

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

- $y \preceq y'$ and $|y'| = |y|$, and
- $y'_k = y_k$ for all $k \in [1, j - 1]$, and
- $y'_j = x_j + 1$, and
- $y'_k = x_k$ for all $k \in [j + 1, m(x)]$.

Observe that y' is not an independent vector of $\mathscr{Z}'$ because $|y'([j, m(x)])| > |x([j, m(x)])| = h([j, m(x)])$. The last equality is due to the fact that $x = y^{m(x)}$. Therefore, $y' \in \Gamma$ but $y' \notin \min \Gamma$. Consider $z' \in \min \Gamma$ with $z' < y'$ and the only hierarchically minimal vector $z = y^{m(z)} \in \operatorname{hmin} \Gamma$ such that $z \preceq z'$ and $|z| = |z'|$. Clearly, $m(z) < m(y)$ because $|z| = |z'| < |y'| = |y|$, and $m(z) \ge i$ because $z \preceq y$ otherwise. Observe that $\sum_{k=1}^{i} y_k = \sum_{k=1}^{i} y'_k \ge \sum_{k=1}^{i} z_k$ because $z \preceq y'$. Since $z_k \ge y_k$ for all $k \in [1, m(z)]$, we have that $z_k = y_k$ for all $k \in [1, i]$. If $m(z) \le m(x)$, then $z_k \ge x_k$ for all $k \in [1, m(z)]$, a contradiction with $z_i = y_i < x_i$. Therefore, there exists a hierarchically minimal vector z with $m(x) < m(z) < m(y)$. □

Several properties of the hierarchically minimal vectors of a hierarchical matroid port that can be inferred from Lemma 8.8 and the others results in this section are summarized in the next proposition. Of course, these properties are necessary conditions for a hierarchical access structure to be ideal. We prove in Section 10 that these conditions are also sufficient.

Notation 8.9. *From now on, the hierarchically minimal vectors of a Π-hierarchical access structure Γ are denoted by $\operatorname{hmin} \Gamma = \{x^1, \dots, x^r\}$, we write $m_i = m(x^i)$ for $i = 1, \dots, r$ and we put $m_0 = 0$. In addition, we assume that the hierarchically minimal vectors are ordered in such a way that $m_i \le m_{i+1}$ for all $i = 1, \dots, r - 1$.*

Proposition 8.10. *Let $\Gamma = \Gamma_0(\mathscr{Z}', \Pi)$ be a Π-hierarchical matroid port with $\operatorname{hmin} \Gamma = \{x^1, \dots, x^r\}$. Then the following properties are satisfied.*

1. *If $1 \le i < r$, then $m_i < m_{i+1}$. In particular, Γ has at most as many hierarchically minimal vectors as levels in the hierarchy.*
2. *If $1 \le i < r$, then $x^i_k \ge x^{i+1}_k$ for all $k \in [1, m_i]$ and $x^i_k > x^{i+1}_k$ for some $k \in [1, m_i]$.*
3. *If $x^i_k > x^r_k$ for some $1 \le i \le r - 1$ and $k \in [1, m_i - 1]$, then $|\Pi_\ell| = x^i_\ell$ for all $\ell \in [k + 1, m_i]$.*

Proof. The first property is straightforward from Lemma 8.5. By Lemmas 8.2 and 8.5, $x^i_k \ge x^{i+1}_k$ for all $k \in [1, m_i]$. Observe that $x^i \le x^{i+1}$ if $x^i_k = x^{i+1}_k$ for all $k \in [1, m_i]$. This implies that $x^i_k > x^{i+1}_k$ for some $k \in [1, m_i]$. We prove now the third property. Since $x^i_k \ge x^{i+1}_k \ge \dots \ge x^r_k$, there exists $j \in \{i, \dots, r - 1\}$ such that $x^j_k > x^{j+1}_k$. Then $|\Pi_\ell| = x^j_\ell$ for all $\ell \in [k + 1, m_j]$ by Lemma 8.8. Therefore, $|\Pi_\ell| = x^j_\ell \le x^i_\ell \le |\Pi_\ell|$ for all $\ell \in [k + 1, m_i]$. □

9 A Family of Ideal Hierarchical Access Structures

We introduce in Definition 9.1 a family of hierarchical access structures that generalizes the ones in Examples 6.3 and 6.4. This section is devoted to prove that these access structures are ideal. Actually, they can be constructed from a class of Boolean polymatroids that contains the ones used in those examples. Moreover, we prove in Section 10 that every ideal hierarchical access structure is a member of this family.

Definition 9.1. *Consider two integer vectors $\mathbf{a} = (a_0, \ldots, a_m)$ and $\mathbf{b} = (b_0, \ldots, b_m)$ with $a_0 = a_1 = b_0 = 1$ and $a_i \le a_{i+1} \le b_i \le b_{i+1}$ for every $i \in [0, m-1]$, and consider as well an m-partition Π of the set P of participants. The Π-partite access structure $\Gamma(\mathbf{a}, \mathbf{b}, \Pi)$ is defined as follows: a vector $u \in \mathbf{P}$ is in $\Gamma(\mathbf{a}, \mathbf{b}, \Pi)$ if and only if there exists $i \in J_m$ such that $\sum_{k=1}^{i} u_k \ge b_i$ and $\sum_{k=1}^{j} u_k \ge a_{j+1} - 1$ for all $j \in [1, i-1]$. Clearly, these access structures are Π-hierarchical.*

The access structures $\Gamma(\mathbf{a}, \mathbf{b}, \Pi)$ with $a_i = 1$ for all $i \in J'_m$ and $1 = b_0 \le b_1 < \cdots < b_m$ coincide with the hierarchical matroid ports in Example 6.3. We obtain the hierarchical matroid ports in Example 6.4 by taking $1 = a_0 = a_1 < \cdots < a_m$ and $1 = b_0 < b_1 = \cdots = b_m$.

Given two integer vectors $\mathbf{a} = (a_0, \ldots, a_m)$ and $\mathbf{b} = (b_0, \ldots, b_m)$ such that $a_0 = a_1 = b_0 = 1$ and $a_i \le a_{i+1} \le b_i \le b_{i+1}$ for every $i \in [0, m-1]$, consider the subsets $B_i = [a_i, b_i]$ of the set $B = [1, b_m]$ and the Boolean polymatroid $\mathcal{Z}' = \mathcal{Z}'(\mathbf{a}, \mathbf{b})$ with ground set J'_m defined from them. Observe that $h([j, i]) = |[a_j, b_i]| = b_i - a_j + 1$ whenever $0 \le j \le i \le m$ and, in particular, $h(\{0\}) = 1$. Therefore, for every m-partition Π of a set P with $|\Pi_i| \ge h(\{i\}) = b_i - a_i + 1$, we can consider the Π-partite matroid port $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$. Since $\mathcal{Z}'$ is representable over every field, we have that Γ is a vector space access structure over every large enough finite field.

We analyze first the properties of the vectors $y^i = y^i(\mathcal{Z})$, where $\mathcal{Z} = \mathcal{Z}(\mathbf{a}, \mathbf{b}) = \mathcal{Z}'(\mathbf{a}, \mathbf{b}) | J_m$. Observe that $y^i_j = h([j, i]) - h([j+1, i]) = a_{j+1} - a_j$ if $j < i$ while $y^i_i = b_i - a_i + 1$. Therefore,

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

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

Lemma 9.2. *Given vectors $y^1, \ldots, y^m \in \mathbb{Z}^m_+$, there exists a Boolean polymatroid of the form $\mathcal{Z}(\mathbf{a}, \mathbf{b})$ with $y^i = y^i(\mathcal{Z}(\mathbf{a}, \mathbf{b}))$ if and only if the following conditions are satisfied.*

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

Proof. Clearly, the vectors of the form $y^i = y^i(\mathcal{Z}(\mathbf{a}, \mathbf{b}))$ satisfy the required conditions. The converse is proved by considering $\mathbf{a} = (a_0, \ldots, a_m)$ 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 $i \in J_m$,
- $b_i = \sum_{j=1}^{i} y^i_j$ for all $i \in J_m$.

Clearly and $a_{i+1} - a_i = y^{i+1}_i \ge 0$ and $b_i = |y^i| \le |y^{i+1}| = b_{i+1}$. In addition, $b_i - a_{i+1} = y^i_i - y^{i+1}_i - 1 \ge 0$. Finally, observe that $y^i = (a_2 - a_1, \ldots, a_i - a_{i-1}, b_i - a_i + 1, 0, \ldots, 0)$ for every $i \in J_m$. □

We prove in Proposition 9.5 that $\Gamma_0(\mathcal{Z}'(\mathbf{a},\mathbf{b}),\Pi)=\Gamma(\mathbf{a},\mathbf{b},\Pi)$. Two technical lemmas about the properties of the integer polymatroid $\mathcal{Z}'=\mathcal{Z}'(\mathbf{a},\mathbf{b})$ and its associated multipartite matroid port $\Gamma=\Gamma_0(\mathcal{Z}'(\mathbf{a},\mathbf{b}),\Pi)$ are needed. Observe that a subset $X\subseteq J_m$ is in $\Gamma_0(\mathcal{Z}')$ if and only if $a_{\min X}=1$.

Lemma 9.3. *If $X\subseteq J'_m$ is such that $h(X)<h([\min X,\max X])$, then*

$$h(X)=h(X\cap[1,j-1])+h(X\cap[j+1,m])$$

for some $j\in[\min X,\max X]\backslash X$.

Proof. Take $C=\bigcup_{i\in X}[a_i,b_i]$ and consider $j\in[\min X,\max X]\backslash X$ such that $h(X\cup\{j\})>h(X)$. Then there exists $c\in[a_j,b_j]$ such that $c\notin C$. We claim that $b_k<c$ if $k\in X\cap[1,j-1]$. Otherwise, $a_k\leq a_j\leq c\leq b_k$ and $c\in[a_k,b_k]\subseteq C$. Analogously, $a_\ell>c$ if $\ell\in X\cap[j+1,m]$. Therefore, $h(X)=|C\cap[1,c-1]|+|C\cap[c+1,m]|=h(X\cap[1,j-1])+h(X\cap[j+1,m])$. □

Lemma 9.4. *If $x\in\min\Gamma$, then $x\in\mathcal{B}(\mathcal{Z},[1,m(x)])$.*

Proof. We have to prove that $h(\operatorname{supp}(x))=h([1,m(x)])$. Take $X=\operatorname{supp}(x)$ and $i_0=\min X$, and suppose that $h(X)<h([1,m(x)])$. Since $X\in\Gamma_0(\mathcal{Z}')$, it holds that $a_{i_0}=1$, which implies that $h([i_0,m(x)])=h([1,m(x)])$. Therefore, $h(X)<h([\min X,\max X])$ and, by Lemma 9.3, there exists $j\in[i_0,m(x)]\backslash X$ such that $h(X)=h(X\cap[1,j-1])+h(X\cap[j+1,m])$. Consider $Z=X\cap[1,j-1]$ and $z=\sum_{i\in Z}x_i\,\mathbf{e}^i$. Clearly, z is an independent vector of $\mathcal{Z}'$ with $|x(Z)|=h(Z)$, which implies that $z\in\Gamma$ because $Z\in\Gamma_0(\mathcal{Z}')$. Since $z<x$, this is a contradiction with $x\in\min\Gamma$. □

Proposition 9.5. *Consider two integer vectors $\mathbf{a}=(a_0,\dots,a_m)$ and $\mathbf{b}=(b_0,\dots,b_m)$ 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 $i\in[0,m-1]$, and let Π be an m-partition of a set P with $|\Pi_i|\geq h(\{i\})=b_i-a_i+1$. Then $\Gamma_0(\mathcal{Z}'(\mathbf{a},\mathbf{b}),\Pi)=\Gamma(\mathbf{a},\mathbf{b},\Pi)$.*

Proof. Put $\Gamma=\Gamma_0(\mathcal{Z}'(\mathbf{a},\mathbf{b}),\Pi)$ and $\mathcal{Z}=\mathcal{Z}'(\mathbf{a},\mathbf{b})|J_m$. Consider a vector $x\in\min\Gamma$. Then $x\in\mathcal{B}(\mathcal{Z},[1,m(x)])$ by Lemma 9.4, and hence $|x|=\sum_{k=1}^{m(x)}x_k=h([1,m(x)])=b_{m(x)}$. In addition, $|x([j+1,m(x)])|\leq h([j+1,m(x)])=b_{m(x)}-a_{j+1}+1$ for all $j\in[1,m(x)-1]$. Therefore, $|x([1,j])|=\sum_{k=1}^{j}x_k\geq a_{j+1}-1$ for all $j\in[1,m(x)-1]$.

Consider now a vector $u\in\mathbf{P}$ such that there exists $i\in J_m$ with $\sum_{k=1}^{i}u_k\geq b_i$ and $\sum_{k=1}^{j}u_k\geq a_{j+1}-1$ for all $j\in[1,i-1]$. We can assume that i is the mininum index for which the vector u satisfies this condition, which implies that $a_{j+1}-1\leq\sum_{k=1}^{j}u_k<b_j$ for all $j\in[1,i-1]$. Let $v\in\mathbf{P}$ be the vector given by $v_j=u_j$ if $j\in[1,i-1]$, and $\sum_{k=1}^{i}v_k=b_i$, and $v_j=0$ if $j\in[i+1,m]$. Obviously, $v\leq u$. The proof is concluded by checking that $v\in\mathcal{B}(\mathcal{Z},[1,i])$. Since $|v|=b_i=h([1,i])$, we only have to check that $|v(X)|\leq h(X)$ for every $X\subseteq[1,i]$. If $X=[j_0,j_1]\subseteq[1,i]$, then

$$|v(X)|=\sum_{k=j_0}^{j_1}v_k=\sum_{k=1}^{j_1}v_k-\sum_{k=1}^{j_0-1}v_k\leq b_{j_1}-a_{j_0}+1=h(X).$$

By Lemma 9.3, for every $X\subseteq[1,i]$, there exist disjoint subsets $Y_1,\dots,Y_s\subseteq[1,i]$ such that $Y_\ell=[\alpha_\ell,\beta_\ell]$, and $X\subseteq Y_1\cup\cdots\cup Y_s$, and $h(X)=h(Y_1)+\cdots+h(Y_s)$. □

As a direct consequence of Proposition 9.5, we prove next that every access structure of the form $\Gamma(\mathbf{a},\mathbf{b},\Pi)$ is ideal. Finally, Proposition 9.7 provides a sufficient condition for a hierarchical access structure to be ideal in terms of the properties of its hierarchically minimal vectors.

Proposition 9.6. *Every access structure of the form $\Gamma(\mathbf{a},\mathbf{b},\Pi)$ admits a $\mathbb{K}$-vector space secret sharing scheme for every large enough finite field $\mathbb{K}$.*

Proof. Consider a set $\widetilde{P} \supseteq P$ and an m-partition $\widetilde{\Pi}$ of $\widetilde{P}$ such that $\widetilde{\Pi}_i \supseteq \Pi_i$ and $|\widetilde{\Pi}_i| \geq b_i - a_i + 1$ for all $i \in J_m$. Then $\widetilde{\Gamma} = \Gamma(\mathbf{a},\mathbf{b},\widetilde{\Pi}) = \Gamma_0(\mathcal{Z}'(\mathbf{a},\mathbf{b}),\widetilde{\Pi})$ by Proposition 9.5, and hence $\widetilde{\Gamma}$ is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. Finally, it is easy to prove that $\Gamma = \Gamma(\mathbf{a},\mathbf{b},\Pi)$ is a minor of $\widetilde{\Gamma}$. Specifically, $\Gamma = \widetilde{\Gamma} \backslash (\widetilde{P} \backslash P)$. □

Proposition 9.7. *Let Π be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P. Consider the family $\operatorname{hmin}\Gamma = \{x^1,\dots,x^r\}$ of its hierarchically minimal points. Suppose that the following properties are satisfied.*

1. *If $1 \leq i < r$, then $m_i < m_{i+1}$ and $x^i_k = x^{i+1}_k$ for all $k \in [1, m_i - 1]$.*
2. *If $m_{i-1} < j \leq m_i$, then $|\Pi_j| \geq \sum_{\ell=j}^{m_i} x^i_\ell$.*

Then Γ 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 $y^1,\dots,y^m \in \mathbf{P}$ defined as follows: if $m_{i-1} < j \leq m_i$, then

- $y^j_k = x^i_k$ for every $k \in [1, j-1]$, and
- $y^j_j = \sum_{\ell=j}^{m_i} x^i_\ell$, and
- $y^j_k = 0$ for every $k \in [j+1, m]$.

Observe that $x^i_{m_i} > x^{i+1}_{m_i}$ because $x^i \not\preceq x^{i+1}$. In addition, $|x^i| < |x^{i+1}|$ because $x^{i+1} \preceq x^i$ otherwise. With that in mind, it is not difficult to check that the points $y^1,\dots,y^m \in \mathbb{Z}_+^m$ satisfy the conditions in Lemma 9.2, and hence there exists a Boolean polymatroid of the form $\mathcal{Z}' = \mathcal{Z}'(\mathbf{a},\mathbf{b})$ such that $y^j = y^j(\mathcal{Z}'|J_m)$ for every $j \in J_m$. Moreover, $h(\{j\}) = y^j_j \leq |\Pi_j|$ for every $j \in J_m$, and hence we can consider the access structure $\Gamma_0(\mathcal{Z}',\Pi)$, which is Π-hierarchical with $\operatorname{hmin}\Gamma_0(\mathcal{Z}',\Pi) = \operatorname{hmin}\{y^1,\dots,y^m\} = \{x^1,\dots,x^r\}$. Therefore, $\Gamma = \Gamma_0(\mathcal{Z}',\Pi)$ and this concludes the proof. □

10 A Characterization of Ideal Hierarchical Access Structures

By using the results in Sections 8 and 9, we present here a complete characterization of the ideal hierarchical access structures. Moreover, we prove that every hierarchical matroid port is ideal and, moreover, it is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. In particular, the results in this section prove Theorem 2.1. The next result is a consequence of Proposition 9.7 and the necessary conditions for a hierarchical access structure to be ideal given in Section 8. It provides a characterization of the ideal hierarchical access structures in which the number of participants in every hierarchical level is large enough in relation to the hierarchically minimal points.

Proposition 10.1. *Let Π be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P with $\operatorname{hmin}\Gamma = \{x^1,\dots,x^r\}$. Suppose that $|\Pi_{m_i}| > x^i_{m_i}$ for all $i \in \{1,\dots,r\}$. Then Γ is ideal if and only if $m_i < m_{i+1}$ and $x^i_k = x^{i+1}_k$ for all $i \in \{1,\dots,r-1\}$ and $k \in [1, m_i - 1]$. Moreover, in this situation Γ is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$.*

Proof. The condition is necessary because of Proposition 8.10. We prove now that it is also sufficient. Consider a set $\widetilde{P} \supseteq P$ and an m-partition $\widetilde{\Pi}$ of $\widetilde{P}$ such that $\widetilde{\Pi}_j \supseteq \Pi_j$ for all $j \in J_m$ and $|\widetilde{\Pi}_j| \ge \sum_{\ell=j}^{m_i} x_\ell^i$ if $m_{i-1} < j \le m_i$. Let $\widetilde{\Gamma}$ be the $\widetilde{\Pi}$-hierarchical access structure with the same hierarchically minimal vectors as Γ. By Proposition 9.7, $\widetilde{\Gamma}$ is a $\mathbb{K}$-vector space access structure for every large enough field $\mathbb{K}$. Clearly, the access structure Γ is a minor of $\widetilde{\Gamma}$. Specifically, $\Gamma = \widetilde{\Gamma} \backslash (\widetilde{P} \backslash P)$. □

Finally, we present our complete characterization of ideal hierarchical access structures in terms of the properties of the hierarchically minimal vectors. Specifically, an access structure is ideal if and only if it satisfies the conditions in Proposition 8.10.

Theorem 10.2. *Let Π be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P with $\operatorname{hmin}\Gamma = \{x^1, \dots, x^r\}$. Then Γ is ideal if and only if the following conditions are satisfied.*

1. *If $1 \le i < r$, then $m_i < m_{i+1}$.*
2. *If $1 \le i < r$, then $x_k^i \ge x_k^{i+1}$ for all $k \in [1, m_i]$.*
3. *If $x_k^i > x_k^r$ for some $i \in [1, r-1]$ and $k \in [1, m_i - 1]$, then $|\Pi_\ell| = x_\ell^i$ for all $\ell \in [k+1, m_i]$.*

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

Proof. As before, Proposition 8.10 implies that the given conditions are necessary. Suppose that the conditions are satisfied. Take $\widetilde{x}^r = x^r$ and for $i \in [1, r-1]$ consider the vectors $\widetilde{x}^i \in \mathbb{Z}_+^m$ defined by

- $\widetilde{x}_k^i = x_k^r$ if $k \in [1, m_i - 1]$, and
- $\widetilde{x}_{m_i}^i = x_{m_i}^i + \sum_{\ell=1}^{m_i-1} (x_\ell^i - x_\ell^r)$, and
- $\widetilde{x}_k^i = 0$ if $k \in [m_i + 1, m]$.

As we did in the proof of Proposition 10.1, we extend the set P of participants to a larger one. Consider a set $\widetilde{P} \supseteq P$ and an m-partition $\widetilde{\Pi}$ of $\widetilde{P}$ such that $\widetilde{\Pi}_j \supseteq \Pi_j$ for all $j \in J_m$ and $|\widetilde{\Pi}_j| \ge \sum_{\ell=j}^{m_i} \widetilde{x}_\ell^i$ if $m_{i-1} < j \le m_i$. Let $\widetilde{\Gamma}$ be the $\widetilde{\Pi}$-hierarchical access structure on $\widetilde{P}$ with $\operatorname{hmin}\widetilde{\Gamma} = \{\widetilde{x}^1, \dots, \widetilde{x}^r\}$. It is not difficult to check that $\widetilde{\Gamma}$ satisfies the conditions in Proposition 9.7, and hence it is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. In particular, $\widetilde{\Gamma} = \Gamma_0(\widetilde{\mathcal{Z}}', \widetilde{\Pi})$ for some integer polymatroid $\widetilde{\mathcal{Z}}'$ on J'_m. Consider $\widetilde{\mathcal{Z}} = \widetilde{\mathcal{Z}}' | J_m$.

The proof is concluded by checking that Γ is a minor of $\widetilde{\Gamma}$. Specifically, we prove that $\Gamma = \widetilde{\Gamma} \cap \mathbf{P}$, which implies that $\Gamma = \widetilde{\Gamma} \backslash (\widetilde{P} \backslash P)$. Since $\widetilde{x}^i \preceq x^i$ for all $i \in [1, r]$, it is clear that $\Gamma \subseteq \widetilde{\Gamma} \cap \mathbf{P}$. Since every minimal vector of $\widetilde{\Gamma}$ is in $\mathcal{B}(\widetilde{\mathcal{Z}}, [1, m_i])$ for some $i \in [1, r]$, it is enough to prove that $\Omega_i = \mathcal{B}(\widetilde{\mathcal{Z}}, [1, m_i]) \cap \mathbf{P} \subseteq \Gamma$ for all $i \in [1, r]$. Suppose that this is false and take the smallest $i \in [1, r]$ such that $\Omega_i \not\subseteq \Gamma$.

We affirm that, in this situation, $x^i \in \Omega_i$. If not, $x^i \notin \min \widetilde{\Gamma}$ by Lemma 8.4 and, since $x^i \in \widetilde{\Gamma}$, there exists $z \in \min \widetilde{\Gamma}$ with $z < x^i$. Applying Lemma 8.4 again, $z \in \mathcal{B}(\widetilde{\mathcal{Z}}, [1, m_j])$ for some $j \in [1, r]$ and, since $|z| < |x^i| = |\widetilde{x}^i|$, we have that $j < i$. Therefore, $z \in \Omega_j \subseteq \Gamma$, a contradiction with the fact that x^i is a minimal vector of Γ. This proves our affirmation.

Consider $R = \Omega_i \backslash \Gamma$ and consider a vector $y \in R$ that is hierarchically minimal in R. Let $k \in [1, m_i - 1]$ be the smallest value such that $y_k \ne x_k^i$. If $y_k < x_k^i$, there exists $\ell \in [k+1, m_i]$ such that $y_\ell > x_\ell^i$. Since $\widetilde{x}^i \preceq y$, it follows that $|\widetilde{x}^i([1,k])| \le |y([1,k])| < |x^i([1,k])|$, and hence

$x^r_s = \widetilde{x}^i_s < x^i_s$ for some $s \in [1,k]$. This implies that $x^i_\ell = |\Pi_\ell|$ and $y_\ell \le x^i_\ell$ because $y \in \mathbf{P}$, a contradiction. If $y_k > x^i_k$, then $y_\ell < x^i_\ell$ and $y' = y - \mathbf{e}^k + \mathbf{e}^\ell \in \mathcal{B}(\widetilde{\mathcal{Z}}, [1, m_i]) \cap \mathbf{P}$ for some $\ell \in [k+1, m_i]$. Since $y' \preceq y$ and and y is a hierarchically minimal vector in R, it follows that $y' \notin R$, and hence $y' \in \Gamma$, a contradiction with $y \notin \Gamma$. □

Actually, we have proved that a hierarchical access structure Γ is ideal if and only if $\Gamma = \widetilde{\Gamma} \backslash (\widetilde{P} \backslash P)$ for some matroid port $\widetilde{\Gamma} = \Gamma_0(\mathcal{Z}'(\mathbf{a}, \mathbf{b}), \widetilde{\Pi})$. By combining this fact with Propositions 9.5 and 9.6, another characterization of the ideal hierarchical access structures is obtained.

Theorem 10.3. *Let Γ be an m-partite access structure. Then Γ is an ideal hierarchical access structure if and only if it coincides with one of the access structures $\Gamma(\mathbf{a}, \mathbf{b}, \Pi)$ described in Definition 9.1.*

Example 10.4. *Let Π be a 4-partition of a set P with $|\Pi_i| = 4$ for all $i \in J_4$, and let Γ be the weighted threshold access structure defined by the vector of weights $w = (7, 5, 4, 3)$ and the threshold $T = 13$. The hierarchically minimal points of Γ are $x^1 = (2, 0, 0, 0)$, $x^2 = (0, 1, 2, 0)$, and $x^3 = (0, 0, 1, 3)$. Since $x^2_2 > x^3_2$ and $|\Pi_3| > x^2_3$, it follows from Theorem 10.2 that Γ is not ideal.*

Example 10.5. *Given positive integers $t_1 < t_2 < t_3 < t_4$, consider a 4-hierarchical access structures in which the qualified subsets are those with at least one participant from the first level, and at least t_i participants in the first i levels for some $i \in J_4$. This access structure is ideal because it is a minor of a 4-hierarchical access structure with hierarchically minimal points $(t_1, 0, 0, 0)$, $(1, t_2, 0, 0)$, $(1, 0, t_3, 0)$, and $(1, 0, 0, t_4)$.*

Tassa [33] proposed an open problem on hierarchical access structures that can be solved by using our results. Given integers $0 < t_1 < \cdots < t_m$ and $\ell \in J_m$, consider the Π-hierarchical access structure

$$\Gamma_\ell = \bigcup_{X \subseteq J_m,\, |X| = \ell} \left\{ x \in \mathbf{P} \,:\, \sum_{j=1}^{i} x_j \ge t_i \text{ for all } i \in X \right\}$$

Observe that the access structures Γ_ℓ for $\ell = 1$ and $\ell = m$ are, respectively, the ones in Examples 4.2 and 4.3, and hence they are ideal. The open problem proposed in [33] is to find out whether the other access structures of this form are ideal or not.

We solve this open problem by proving a negative answer for this question. Consider an access structure of the form Γ_ℓ with $\ell \neq 1, m$, and suppose that $|\Pi_i| \ge t_i$ for every $i \in J_m$. For every $X = \{i_1, \ldots, i_\ell\} \subseteq J_m$ with $i_1 < \cdots < i_\ell$, consider the vector $v^X \in \mathbb{Z}^m_+$ with $\operatorname{supp}(v^X) = X$ determined by $v^X_{i_1} = t_{i_1}$ and $v^X_{i_k} = t_{i_k} - t_{i_{k-1}}$ for $k = 2, \ldots, \ell$. Clearly, $v^X \in \Gamma_\ell$ and $u \notin \Gamma_\ell$ if $u \in \mathbf{P}$ and $u \prec v^X$. Therefore, v^X is a hierarchically minimal vector of this access structure. Consider the sets $X = [2, \ell+1]$ and $Y = \{1\} \cup [3, \ell+1]$. Then v^X and v^Y are two different hierarchically minimal vectors of Γ_ℓ with $m(v^X) = m(v^Y)$. By Theorem 10.2, this implies that Γ_ℓ is not ideal.

11 Ideal Weighted Threshold Access Structures

By using our characterization of ideal hierarchical access structures, we present in this section an alternative proof for the characterization of ideal weighted threshold access structures that was given by Beimel, Tassa and Weinreb [2]. First, we describe several families of ideal weighted threshold access structures, and then we prove in Theorem 11.1 that every indecomposable ideal weighted threshold access structure must be in one of these families. As was noticed in [2], an ideal weighted threshold access structure can be the composition of smaller such structures.

The (t,n)-threshold access structures form the first of those families. Of course, they are ideal weighted threshold access structures. We consider as well two families of ideal bipartite hierarchical access structures, that is, ideal Π-hierarchical access structures for some bipartition $\Pi = (\Pi_1, \Pi_2)$ of the set of participants.

B$_1$ This family consists of the access structures such that $\operatorname{hmin}\Gamma = \{(x_1, x_2)\}$ with $x_1 > 0$ and $0 < x_2 = |\Pi_2| - 1$. We affirm that every member of $\mathbf{B}_1$ is a weighted threshold access structure with weight vector $(w_1, w_2) = (1, 1-\delta)$, where $0 < \delta < 1/x_2$, and threshold $T = x_1 + x_2(1-\delta)$. This is proved by checking that $(x_1, x_2) \cdot w \geq T$ while $(x_1 - 1, x_2 + 1) \cdot w < T$ and $(x_1 + x_2 - 1, 0) \cdot w < T$.

B$_2$ This is the family of the access structures with $\operatorname{hmin}\Gamma = \{(y_1 + y_2 - 1, 0), (y_1, y_2)\}$, where $y_2 > 2$, and $|\Pi_2| \leq y_2 + 1$ if $y_1 > 0$. They are weighted threshold access structures with $w = (w_1, w_2) = (1, 1 - 1/y_2)$ and $T = y_1 + y_2 - 1$.

In addition we consider two families of ideal tripartite hierarchical access structures. Similarly to the previous families of bipartite access structures, all their members are weighted threshold access structures. In this case we also describe the hierarchically maximal non-authorized vectors. The computation of these vectors is straightforward. If Γ is a hierarchical tripartite access structure with $\operatorname{hmin}\Gamma = \{x^1, x^2\}$, then $u \in \mathbb{Z}_+^3$ is not in Γ if there exist $1 \leq i, j \leq 3$ such that $|x^1([1,i])| > |u([1,i])|$ and $|x^2([1,j])| > |u([1,j])|$.

T$_1$ We consider in this case the structures with $\operatorname{hmin}\Gamma = \{(x_1, 0, 0), (y_1, y_2, y_3)\}$ such that $y_2 = |\Pi_2|$ if $y_1 \neq 0$, and $y_2 > 0$, and $1 < y_3 = |\Pi_3| - 1$, and $x_1 = y_1 + y_2 + y_3 - 1$. The hierarchically maximal non-authorized vectors of such an access structure are $u = (x_1 - 1, 1, 0)$ and $u' = (y_1 + y_2 - 1, 0, y_3 + 1)$. Consider real numbers $0 < \delta_2 < \delta_3 < 1$ such that

$$\frac{1}{y_3 + 1} < \delta_3 \leq \frac{1 - y_2 \delta_2}{y_3}.$$

We affirm that Γ is the weighted threshold access structure with weight vector $w = (1, 1 - \delta_2, 1 - \delta_3)$ and threshold $T = x_1$. This is proved by checking that $u \cdot w < T$ and $u' \cdot w < T$ while $v \cdot w \geq T$ if $v \in \operatorname{hmin}\Gamma$.

T$_2$ This family contains the access structures with $\operatorname{hmin}\Gamma = \{(x_1, x_2, 0), (y_1, y_2, y_3)\}$, where $0 < y_1 < x_1$, and $1 < y_3 = |\Pi_3|$, and $0 < x_2 = y_2 + 1 = |\Pi_2|$, and $x_1 + x_2 = y_1 + y_2 + y_3 - 1$. In this case, the hierarchically maximal non-authorized vectors are $u = (x_1 + x_2 - 1, 0, 1)$ and $u' = (y_1 - 1, y_2 + 1, y_3)$. Consider real numbers $0 < \delta_2 < \delta_3 < 1$ such that

$$\max\left\{\delta_2 x_2, \frac{1}{y_3}\right\} < \delta_3 \leq \frac{1 + \delta_2}{y_3}.$$

Then Γ is the weighted threshold access structure determined by $w = (1, 1 - \delta_2, 1 - \delta_3)$ and $T = x_1 + (1 - \delta_2) x_2$.

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

Theorem 11.1. *A weighted threshold access structure without redundant participants is ideal if and only if*

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

The remaining of this section is devoted to the proof of this theorem, which is divided into several partial results. We prove first a technical result about ideal hierarchical access structures that are indecomposable and strictly m-partite.

Lemma 11.2. *Let* Π *be an* m*-partition of the set* P *of participants and let* Γ *be an ideal* Π*-hierarchical access structure with* $\operatorname{hmin}\Gamma = \{x^1, \dots, x^r\}$*. Assume that* Γ *is indecomposable and strictly* m*-partite. Then the following properties hold.*

1. *For every* $j \in J_m$*, there exists* $i \in \{1, \dots, r\}$ *such that* $x^i_j \neq 0$*.*
2. *If* $j \in J_m$ *is such that* $m_{i-1} + 1 < j \le m_i$ *for some* $i \in \{1, \dots, r\}$*, then* $x^r_j < |\Pi_j|$ *(remember that* $m_0 = 1$*).*
3. *If* $r \ge 2$*, then* $x^i([1, m_i]) \neq x^r([1, m_i]) + \mathbf{e}^j$ *for every* $i \in \{1, \dots, r-1\}$ *and* $j \in [1, m_i]$*.*
4. *If* $m \ge 2$*, then* $x^i_1 < |\Pi_1|$ *for some* $i = 1, \dots, r$*.*
5. *If* $m \ge 2$*, then* $x^r_m > 1$*.*
6. *If* $r = 2$*, then* $x^2_j > 0$ *for all* $j \in [1, m_1 - 1]$*.*

Proof. Suppose that there exists $j \in J_m$ such that $x^i_j = 0$ for all $i = 1, \dots, r$. Clearly, the participants in Π_m are redundant if $j = m$. We prove that the participants in Π_j are hierarchically equivalent to the ones in Π_{j+1} if $j < m$. Consider $u \in \Gamma$ such that $v = u - \mathbf{e}^j + \mathbf{e}^{j+1} \in \mathbf{P}$, and take $x \in \operatorname{hmin}\Gamma$ with $x \preceq u$. If $m(x) \le j - 1$, then clearly $x \preceq v$. If $m(x) \ge j + 1$, then $\sum_{\ell=1}^{j}(v_\ell - x_\ell) \ge \sum_{\ell=1}^{j-1}(v_\ell - x_\ell) \ge 0$ because $x_j = 0$ and $x \preceq u$. Therefore, $x \preceq v$. This proves Property 1.

Assume that there exist $i \in \{1, \dots, r\}$ and $j \in J_m$ such that $m_{i-1} + 1 < j \le m_i$ and $x^r_j = |\Pi_j|$. Property 2 is proved by checking that, in this situation, the participants in Π_{j-1} are hierarchically equivalent to those in Π_j. By Theorem 10.2, $x^k_j = |\Pi_j|$ for all $k = i, \dots, r$. Consider $u \in \Gamma$ such that $v = u - \mathbf{e}^{j-1} + \mathbf{e}^j \in \mathbf{P}$, and take $x^k \in \operatorname{hmin}\Gamma$ with $x^k \preceq u$. Clearly, $x^k \preceq v$ if $k < i$. If $k \ge i$, then $u_j - x^k_j = u_j - |\Pi_j| \le -1$, and hence $\sum_{\ell=1}^{j-1}(u_\ell - x^k_\ell) \ge 1$. This implies that $x^k \preceq v$.

Property 3 is proved in the following. Suppose that $r \ge 2$ and there exist $i \in \{1, \dots, r-1\}$ and $j \in [1, m_i]$ such that $x^i([1, m_i]) = x^r([1, m_i]) + \mathbf{e}^j$. Observe that Proposition 8.10 (2) implies that $x^i([1, m_i]) = x^k([1, m_i]) + \mathbf{e}^j$ for all $k = i+1, \dots, r$. In addition, $x^i_\ell = |\Pi_\ell|$ for all $\ell \in [j+1, m_i]$ by Theorem 10.2. Consider $p \notin P$ and the m-partition Π' of $P' = P \cup \{p\}$ obtained by modifying Π with $\Pi'_{m_i} = \Pi_{m_i} \cup \{p\}$. Consider as well the vectors $y^i = x^i([1, m_i]) + \mathbf{e}^{m_i} - \mathbf{e}^j$, and $y^k = x^k([1, m_i])$ for all $1 \le k < i$, and $z^k = x^k([m_i + 1, m])$ for all $i < k \le r$. Let Γ_1 be the $(\Pi_1, \dots, \Pi_{m_i - 1}, \Pi'_{m_i})$-hierarchical access structure with $\operatorname{hmin}\Gamma_1 = \{y^1, \dots, y^i\}$, and let Γ_2 be the $(\Pi_{m_i+1}, \dots, \Pi_m)$-hierarchical access structure with $\operatorname{hmin}\Gamma_2 = \{z^{i+1}, \dots, z^r\}$. We prove next that $\Gamma = \Gamma_1[\Gamma_2; p]$. If $k \le i$, then $y^k \preceq x^k([1, m_i])$, and hence $x^k \in \Gamma_1[\Gamma_2; p]$ because $x^k([1, m_i]) \in \Gamma_1$. If $k > i$, then $x^k([1, m_i]) + \mathbf{e}^{m_i} = x^i([1, m_i]) - \mathbf{e}^j + \mathbf{e}^{m_i} = y^i \in \Gamma_1$, and $x^k([m_i + 1, m]) = z^k \in \Gamma_2$. This implies that $x^k \in \Gamma_1[\Gamma_2; p]$. Therefore, $\Gamma \subseteq \Gamma_1[\Gamma_2; p]$ because all hierarchically minimal vectors of Γ are in $\Gamma_1[\Gamma_2; p]$, which is Π-hierarchical. If $u \in \Gamma_1[\Gamma_2; p]$, then either $u([1,m_i]) \in \Gamma_1$ or $u([1,m_i]) + \mathbf{e}^{m_1} \in \Gamma_1$ and $u([m_i+1,m]) \in \Gamma_2$. In both cases, it is clear that $u \in \Gamma$.

Suppose that $m \geq 2$ and $x^i_1 = |\Pi_1|$ for all $i = 1, \ldots, r$. Consider $p \notin P$ and $\Pi'_1 = \Pi_1 \cup \{p\}$, and the points $z^i = x^i([2,m])$ for all $i = 1, \ldots, r$. Let Γ_1 be the $(|\Pi'_1|, |\Pi'_1|)$-threshold access structure on Π'_1 and let Γ_2 be the $(\Pi_2, \ldots, \Pi_m)$-hierarchical access structure with $\operatorname{hmin} \Gamma_2 = \{z^1, \ldots, z^r\}$. Then $\Gamma = \Gamma_1[\Gamma_2; p]$. This proves Property 4.

We prove next Property 5. If $m_{r-1} = m-1$, then $x^r_m > 1$ by Theorem 10.2. Suppose that $m_{r-1} < m-1$ and $x^r_m = 1$. Then $|\Pi_m| > x^r_m = 1$ by Property 2. Consider $p \notin P$ and $\Pi'_{m-1} = \Pi_{m-1} \cup \{p\}$, and the vectors $y^i = x^i([1,m-1])$ for $1 \leq i \leq r-1$ and $y^r = x^r([1,m-1]) + \mathbf{e}^{m-1}$. Let Γ_1 be the $(\Pi_1, \ldots, \Pi_{m-2}, \Pi'_{m-1})$-hierarchical access structure with $\operatorname{hmin} \Gamma_1 = \{y^1, \ldots, y^r\}$ and let Γ_2 the $(1, |\Pi_m|)$-threshold access structure on P_m. One can check that $\Gamma = \Gamma_1[\Gamma_2; p]$.

Finally, we prove Property 6. Suppose that $x^2_j = 0$ for some $j \in [1, m_1 - 1]$. By Property 1, $x^1_j > 0$ and, as consequence of Theorem 10.2, $x^1_\ell = |\Pi_\ell|$ for all $\ell = j+1, \ldots, m_1$. Then the participants in Π_j are hierarchically equivalent to those in Π_{j+1}. Let $u \in \Gamma$ be such that $v = u - \mathbf{e}^j + \mathbf{e}^{j+1} \in \mathbf{P}$. If $x^1 \preceq u$, then $\sum_{\ell=1}^{j}(u_\ell - x^1_\ell) \geq 1$ because $u_{j+1} - x^1_{j+1} \leq -1$. Therefore, $x^1 \preceq v$. If $x^2 \preceq u$, then $\sum_{\ell=1}^{j}(u_\ell - x^1_\ell) = \sum_{\ell=1}^{j-1}(u_\ell - x^1_\ell) + u_j \geq 1$, and hence $x^1 \preceq v$. □

We can now proceed to prove Theorem 11.1. We assume in the following that Γ is an ideal weighted threshold access structure. That is, Γ is an ideal m-hierarchical access structure with

$$\Gamma = \{u \in \mathbf{P} \,:\, u \cdot w = u_1 w_1 + \cdots + u_m w_m \geq T\}$$

for some weight vector $w \in \mathbb{R}^m$ with $w_1 > \cdots > w_m > 0$ and some threshold $T > 0$. We suppose as well that Γ is indecomposable and strictly m-partite. Several cases are considered depending on the number m of levels in the structure. The case $m = 1$ clearly corresponds to the threshold access structures. We discuss in Lemma 11.4 the case $m = 2$, while the case $m \geq 3$ is analyzed in Lemmas 11.5, 11.6 and 11.7. We begin with an obvious fact that will be used several times in the following.

Lemma 11.3. *Consider $u \in \mathbf{P}$ and $v \in \mathbb{Z}^m$ such that $u + v \in \mathbf{P}$. If $u \in \Gamma$ and $u + v \notin \Gamma$, then $v \cdot w < 0$. On the other hand, if $u \notin \Gamma$ and $u + v \in \Gamma$, then $v \cdot w > 0$.*

Lemma 11.4. *If $m = 2$, then Γ belongs to one of the families $\mathbf{B}_1$ or $\mathbf{B}_2$.*

Proof. Suppose first that $\operatorname{hmin} \Gamma = \{(x_1, x_2)\}$. By Lemma 11.2, it is clear that $0 < x_1 < |\Pi_1|$ and $1 < x_2 < |\Pi_2|$. If $|\Pi_2| \geq x_2 + 2$, then $(x_1, x_2) + (-1, 2) \in \mathbf{P} \backslash \Gamma$ and $(x_1, x_2) + (1, -2) \in \mathbf{P} \backslash \Gamma$, a contradiction by Lemma 11.3 implying that $|\Pi_2| = x_2 + 1$. Therefore, $\Gamma \in \mathbf{B}_1$ in this case. Suppose now that $\operatorname{hmin} \Gamma = \{(x_1, 0), (y_1, y_2)\}$. Since $y_2 \geq 2$ and $x_1 - y_1 \geq 2$ by Lemma 11.2, $(y_1, y_2) + (1, -2) \in \mathbf{P} \backslash \Gamma$, so $w_1 < 2w_2$. In addition, $w_1 > (y_2 + y_1 - x_1) w_2$ because $(x_1, 0) + (-1, y_2 + y_1 - x_1) \in \mathbf{P} \backslash \Gamma$. This implies that $x_1 = y_2 + y_1 - 1$. If $y_1 = 0$ then $y_2 = x_1 + 1$, and hence $\Gamma \in \mathbf{B}_2$. Suppose that $y_1 > 0$. If $|\Pi_2| \geq y_2 + 2$, then both $(y_1, y_2) + (-1, 2)$ and $(y_1, y_2) + (1, -2)$ are in $\mathbf{P} \backslash \Gamma$, which is impossible. Therefore, $|\Pi_2| \leq y_2 + 1$ and $\Gamma \in \mathbf{B}_2$ as well. This concludes the proof because, by Theorem 10.2, all possible cases for ideal 2-hierarchical access structures have been analyzed. □

Lemma 11.5. *If $m \geq 3$, then Γ has exactly 2 hierarchically minimal vectors.*

Proof. Suppose that Γ has only one hierarchically minimal vector, that is, $\operatorname{hmin} \Gamma = \{x\}$. From Lemma 11.2, $0 < x_j < |\Pi_j|$ for all $j \in J_m$. This implies that the vectors $x + (\mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^3)$ and $x - (\mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^3)$ are in $\mathbf{P} \backslash \Gamma$, a contradiction.

Suppose that Γ has $r \geq 3$ hierarchically minimal vectors. Consider the vector

$$u = x^{r-2} - \mathbf{e}^{m_{r-2}} + \mathbf{e}^{m_{r-1}} + \mathbf{e}^{m}.$$

By using Theorem 10.2, it is not difficult to check that $|u([1, m_i])| < |x^i|$ for all $i = 1, \ldots, r$, and hence $u \in \mathbf{P} \backslash \Gamma$. This implies that $(-\mathbf{e}^{m_{r-2}} + \mathbf{e}^{m_{r-1}} + \mathbf{e}^{m}) \cdot w = -w_{m_{r-2}} + w_{m_{r-1}} + w_m < 0$, and hence $w_{m_{r-2}} > 2w_m$. Let j be the maximum element in $[1, m_{r-2}]$ such that $x_j^{r-2} > x_j^r$. Such a value exists by Proposition 8.10 and, in addition, $|\Pi_\ell| = x_\ell^r = x_\ell^{r-2}$ for all $\ell \in [j+1, m_{r-2}]$. Consider $v = x^r + \mathbf{e}^j - 2\mathbf{e}^m$, which is in $\mathbf{P}$ by Lemma 11.2 (5). At this point, it is enough to prove that $v \notin \Gamma$, because this implies that $w_{m_{r-2}} \leq w_j < 2w_m$, a contradiction.

Clearly, $|x^{r-2}([1, \ell])| \geq |v([1, \ell])|$ for all $\ell \in [1, m_{r-2}]$ and, by Theorem 10.2, $|x^i([1, m_i])| > |x^{r-2}([1, m_i])|$ if $1 \leq i < r-2$. This implies that $x^i \not\preceq v$ if $1 \leq i < r-2$. In addition, $x^r \not\preceq v$ because $|x^r| > |v|$. Suppose that $x^{r-2} \preceq v$. Then $|x^{r-2}([1, m_{r-2}])| = |v([1, m_{r-2}])|$, which implies that $x^{r-2}([1, m_{r-2}]) = x^r([1, m_{r-2}]) + \mathbf{e}^j$, a contradiction by Lemma 11.2 (3). This proves that $x^{r-2} \not\preceq v$, and one can prove analogously that $x^{r-1} \not\preceq v$. Therefore, $v \notin \Gamma$. □

Lemma 11.6. *If $m = 3$, then Γ is in one of the families $\mathbf{T}_1$ or $\mathbf{T}_2$.*

Proof. Suppose that $\operatorname{hmin} \Gamma = \{x, y\} = \{(x_1, 0, 0), (y_1, y_2, y_3)\}$. Taking into account Lemma 11.2, it is clear that $y_2 > 0$, and $1 < y_3 < |\Pi_3|$, and $x_1 > y_1 + 1$, which implies that $y + (1, 0, -2) \in \mathbf{P} \backslash \Gamma$, and hence $w_1 < 2w_3$. If $|x| < |y| - 1$, then $x + (-1, 0, 2) \in \mathbf{P} \backslash \Gamma$ and $w_1 > 2w_3$, a contradiction. Therefore, $|x| = |y| - 1$. If $|\Pi_3| > y_3 + 1$, then $y + (0, -1, 2) \in \mathbf{P} \backslash \Gamma$ and $w_2 > 2w_3$, a contradiction because $w_1 < 2w_3$. Therefore, $|\Pi_3| = y_3 + 1$. Now suppose that $y_2 < |\Pi_2|$ and $y_1 > 0$. Then $y + (-1, 1, 1) \in \mathbf{P} \backslash \Gamma$, and hence $w_1 > w_2 + w_3$, a contradiction with $w_1 < 2w_3$. Therefore, Γ is in $\mathbf{T}_1$.

Suppose that $\operatorname{hmin} \Gamma = \{x, y\} = \{(x_1, x_2, 0), (y_1, y_2, y_3)\}$ with $x_2 > 0$. Observe that $y_3 \geq 2$ by Lemma 11.2. Suppose, for the sake of contradiction, that $x_1 = y_1$. Taking into account Lemma 11.2 again, it is clear that $x_2 \geq y_2 + 2$ and $x_1 < |\Pi_1|$. In this case, both $y + (1, 0, -2)$ and $y + (-1, 2, 0)$ are in $\mathbf{P} \backslash \Gamma$, a contradiction. Hence $x_1 > y_1$ and, as a consequence of Theorem 10.2, $x_2 = |\Pi_2|$, and so $x_2 > y_2$ by Lemma 11.2 (2). If $|x| < |y| - 1$, then $x + (-1, 0, 2) \in \mathbf{P} \backslash \Gamma$, a contradiction because $y + (1, 0, -2) \in \mathbf{P} \backslash \Gamma$. Therefore, $|x| = |y| - 1$. We claim that $y_1 > 0$. Indeed, if $y_1 = 0$, then $x_1 > 0$, and hence $x_2 = |\Pi_2|$, but this is impossible by Lemma 11.2 (6). If $y_3 < |\Pi_3|$ then $y + (-1, 1, 1) \in \mathbf{P} \backslash \Gamma$ and so $w_1 > w_2 + w_3$, a contradiction implying $y_3 = |\Pi_3|$. Observe that $x_2 = y_2 + 1$, because if $x_2 > y_2 + 1$ then $y + (-1, 2, 0) \in \mathbf{P} \backslash \Gamma$ and hence $w_1 > 2w_2$, a contradiction. Therefore, Γ is in $\mathbf{T}_2$.

This concludes the proof because, by Theorem 10.2, all possible tripartite hierarchical ideal access structures with exactly two hierarchically minimal points have been analyzed. □

Lemma 11.7. $m \leq 3$.

Proof. Suppose that $m > 3$ and take $\operatorname{hmin} \Gamma = \{x^1, x^2\}$.

Suppose that $m_1 = m - 1$ and $x_1^1 = x_1^2$. Since $m_1 \geq 3$, by Lemma 11.2 we obtain that $x_j^1 > 0$ and $x_j^2 < |\Pi_j|$ for all $j = 1, 2, 3$. Thus both $x^1 + \mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^3$ and $x^2 - \mathbf{e}^1 + \mathbf{e}^2 + \mathbf{e}^3$ are in $\mathbf{P} \backslash \Gamma$, a contradiction. Now suppose that $x_1^1 > x_1^2$. By Theorem 10.2, $x_j^1 = |\Pi_j|$ for all $j \in [2, m_1]$, and by Lemma 11.2 (2), $x_j^2 < |\Pi_j|$ for $j = 2, 3$. As a consequence of Lemma 11.2 (6) we obtain that $x_1^2 > 0$ and $x_2^2 > 0$. Hence both $x^2 - \mathbf{e}^1 + \mathbf{e}^2 + \mathbf{e}^3$ and $x^2 + \mathbf{e}^1 - \mathbf{e}^2 - \mathbf{e}^m$ are in $\mathbf{P} \backslash \Gamma$, which implies that $w_3 < w_m$, a contradiction. Therefore $m_1 < m - 1$.

Now suppose that $1 < m_1 \leq m - 2$. Then $x_2^2 < |\Pi_2|$ and $1 < x_m^2 < |\Pi_m|$. Moreover, $|x^1([1, m_1])| > |x^2([1, m_1])| + 1$ by Lemma 11.2. Suppose that $x_1^1 = x_1^2$. Then $x_1^2 > 0$ and both $x^2 + \mathbf{e}^1 - 2\mathbf{e}^m$ and $x^2 - \mathbf{e}^1 + \mathbf{e}^2 + \mathbf{e}^m$ are in $\mathbf{P} \backslash \Gamma$, a contradiction. Now suppose that $x_1^1 > x_1^2$. In this case, $x_1^2 > 0$ by Lemma 11.2 (6). Now both $x^2 + \mathbf{e}^1 - \mathbf{e}^{m-1} - \mathbf{e}^m$ and $x^2 - \mathbf{e}^1 + \mathbf{e}^{m-1} + \mathbf{e}^m$ are in $\mathbf{P}\backslash\Gamma$, a contradiction.

Finally, suppose that $m_1 = 1$. Then $x_1^1 - x_1^2 \geq 2$, and $x_j^2 > 0$ for $j \in [m-2, m]$, and $x_j^2 < |\Pi_j|$ for $j \in [m-1, m]$. Both $x^2 + \mathbf{e}^1 - \mathbf{e}^{m-1} - \mathbf{e}^m$ and $x^2 - \mathbf{e}^{m-2} + \mathbf{e}^{m-1} + \mathbf{e}^m$ are in $\mathbf{P}\backslash\Gamma$, a contradiction. □

References

[1] A. Beimel, “Secret-Sharing Schemes: A Survey,” *Coding and Cryptology, Third International Workshop IWCC 2011, Lecture Notes in Comput. Sci.* **6639** 2011, pp. 11–46.

[2] A. Beimel and T. Tassa and E. Weinreb, “Characterizing Ideal Weighted Threshold Secret Sharing,” *SIAM J. Discrete Math.* **22** 2008, pp. 360–397.

[3] A. Beimel and E. Weinreb, “Monotone Circuits for Monotone Weighted Threshold Functions,” *Information Processing Letters* **97** 2006, pp. 12–18.

[4] J. Benaloh and J. Leichter, “Generalized secret sharing and monotone functions,” *Advances in Cryptology – CRYPTO ’88*, Lecture Notes in Comput. Sci., no. 403(1990), pp. 27–35.

[5] G. R. Blakley, “Safeguarding cryptographic keys,” *AFIPS Conference Proceedings*, no. 48(1979), pp. 313–317.

[6] E.F. Brickell, “Some ideal secret sharing schemes,” *J. Combin. Math. Combin. Comput.* **6** (1989), pp. 105–113.

[7] E.F. Brickell and D.M. Davenport, “On the classification of ideal secret sharing schemes,” *J. Cryptology* **4** (1991), pp. 123–134.

[8] R. M. Capocelli and A. De Santis and L. Gargano and U. Vaccaro, “On the size of shares of secret sharing schemes,” *J. Cryptology*, no. 6(1993), pp. 157–168.

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

[10] L. Csirmaz, “The size of a share must be large,” *J. Cryptology*, no. 10(1997), pp. 223–231.

[11] J. Edmonds. “Submodular Functions, Matroids, and Certain Polyhedra,” *Combinatorial Optimization — Eureka, You Shrink!, Lecture Notes in Comput. Sci.* **2570** (2003), pp. 11–26.

[12] O. Farràs and J. Martí-Farré and C. Padró, “Ideal Multipartite Secret Sharing Schemes,” *J. Cryptology*, Online First (2011).

[13] S. Fujishige, *Submodular Functions and Optimization*. Annals of Discrete Mathematics **47**, North-Holland Elsevier, Amsterdam, 1991.

[14] J. Herranz and G. Sáez, “New Results on Multipartite Access Structures,” *IEE Proceedings of Information Security*, no. 153(2006), pp. 153–162.

[15] J. Herzog and T. Hibi, “Discrete polymatroids,” *J. Algebraic Combin.* **16** (2002), pp. 239–268.

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

[17] E.D. Karnin and J.W. Greene and M.E. Hellman, "On secret sharing systems," *IEEE Trans. Inform. Theory*, no. 29(1983), pp. 35–41.

[18] S. C. Kothari, "Generalized Linear Threshold Scheme," *Advances in Cryptology – CRYPTO 84*, LNCS, no. 196(1985), pp. 231–241.

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

[20] J. Martí-Farré and C. Padró, "On Secret Sharing Schemes, Matroids and Polymatroids," *J. Math. Cryptol.* **4** (2010), pp. 95–120.

[21] F. Matúš, "Matroid representations by partitions," *Discrete Math.*, no. 203(1999), pp. 169–194.

[22] F. Matúš, "Two Constructions on Limits of Entropy Functions," *IEEE Trans. Inform. Theory* **53** (2007), pp. 320–330.

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

[24] K. Murota, *Discrete convex analysis*. SIAM Monographs on Discrete Mathematics and Applications. SIAM, Philadelphia, USA, 2003.

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

[26] S.-L. Ng, "Ideal secret sharing schemes with multipartite access structures," *IEE Proc.-Commun.*, no. 153(2006), pp. 165–168.

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

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

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

[30] A. Schrijver. *Combinatorial optimization. Polyhedra and efficiency.* Springer-Verlag, Berlin, 2003.

[31] A. Shamir, "How to share a secret," *Commun. of the ACM*, no. 22(1979), pp. 612–613.

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

[33] T. Tassa, "Hierarchical Threshold Secret Sharing," *J. Cryptology* **20** (2007), pp. 237–264.

[34] T. Tassa and N. Dyn, "Multipartite Secret Sharing by Bivariate Interpolation," *J. Cryptology* **22** (2009), pp. 227–258.

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