Ideal Hierarchical Secret Sharing Schemes*

Oriol Farràs and Carles Padró

Universitat Politècnica de Catalunya, Barcelona, Spain

Abstract. Hierarchical secret sharing is among the most natural generalizations of threshold secret sharing, and it has attracted a lot of attention from 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 deals with the properties of the hierarchically minimal sets of the access structure, which are the minimal qualified sets whose participants are in the lowest possible levels in the hierarchy. By using our characterization, it can be efficiently checked whether any given hierarchical access structure that is defined by its hierarchically minimal sets is ideal. We use the well known connection between ideal secret sharing and matroids and, in particular, the fact that every ideal access structure is a matroid port. In addition, we use recent results on ideal multipartite access structures and the connection between multipartite matroids and integer polymatroids. We prove that every ideal hierarchical access structure is the port of a representable matroid and, more specifically, we prove that every ideal structure in this family admits ideal *linear* secret sharing schemes over fields of all characteristics. In addition, methods to construct such ideal schemes can be derived from the results in this paper and the aforementioned ones on ideal multipartite secret sharing. Finally, we use our results to find a new proof for the characterization of the ideal weighted threshold access structures that is simpler than the existing one.

Keywords: Secret sharing, Ideal secret sharing schemes, Hierarchical secret sharing, Weighted threshold secret sharing, Multipartite secret sharing, Multipartite matroids, Integer polymatroids.

1 Introduction

A *secret sharing scheme* is a method to distribute *shares* of a *secret value* among a set of *participants*. Only the *qualified* subsets of participants can recover the secret value from their shares, while the *unqualified* subsets do not obtain any information about the secret value. The qualified subsets form the *access structure*

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-11799-2_36

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

D. Micciancio (Ed.): TCC 2010, LNCS 5978, pp. 219–236, 2010.

of the scheme, which is a monotone increasing family of subsets of participants. Only *unconditionally secure perfect* secret sharing schemes are considered in this paper.

Secret sharing was independently introduced by Shamir [32] and Blakley [4] 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 [14].

There exist scenarios in which non-threshold secret sharing schemes are required because, for instance, some participants should be more powerful than others. The first attempt to overcome the limitation of threshold access structures was made by Shamir in his seminal work [32] by proposing a simple modification of the threshold scheme. Namely, every participant receives as its share a certain number of shares from a threshold scheme, according to its position in the hierarchy. In this way a scheme for a *weighted threshold access structure* is obtained. That is, every participant has a weight (a positive integer) and a set is qualified if and only if its weight sum is at least a given threshold. This new scheme is not ideal because the shares are in general larger than the secret.

Every access structure admits a secret sharing scheme [3,13], but in general the shares must be larger than the secret [7,9]. 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.

Because of the difficulty (presumably, impossibility) of finding efficient secret sharing schemes for general access structures, the construction of ideal secret sharing schemes for families of access structures with interesting properties for the applications of secret sharing is worth considering. This line of work was initiated by Simmons [33], who proposed two families of access structures, the *multilevel* and the *compartmented* ones, and conjectured them to admit ideal secret sharing schemes. The multilevel and compartmented 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, in a multilevel access structure, the participants are hierarchically ordered, and the participants in higher levels are more powerful than the ones in lower levels. Multipartite and, in particular, hierarchical secret sharing are the most natural generalization of threshold secret sharing.

Brickell [5] proposed a general method, based on linear algebra, to construct ideal secret sharing schemes for access structures that are not necessarily threshold, and he applied it to the construction of particular ideal secret sharing schemes proving the conjecture by Simmons. By using different kinds of polynomial interpolation, Tassa [35], and Tassa and Dyn [36] proposed constructions of ideal secret sharing schemes for several families of multipartite access structures, some of them with hierarchical properties. These constructions are based on the general linear algebra method by Brickell [5], but they provide schemes for the multilevel and compartmented access structures that are simpler and more

efficient than the particular ones proposed in [5] for those structures. Other constructions of ideal multipartite secret sharing schemes have been presented in [11,26].

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 [6] 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 [5]: the ports of representable matroids are ideal access structures. The results in [6] have been generalized in [16] 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 [20,21].

In addition to the search of general results, several authors studied this open problem for particular families of access structures. Some of them deal with families of multipartite access structures. Beimel, Tassa and Weinreb [1] presented a characterization of the ideal weighted threshold access structures that generalizes the partial results in [22,29]. Another important result about weighted threshold access structures have been obtained recently by Beimel and Weinreb [2]. 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 [8,11], and this question was solved in [10]. 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 [5].

The characterization of the ideal tripartite access structures in [10] was obtained actually from the much more general results about ideal multipartite access structures in that paper. Pointing out the close connection between multipartite matroids and integer polymatroids, specially the characterization of this combinatorial object given by Herzog and Hibi [12], and the use for the first time in secret sharing of these concepts are among the main contributions in [10]. The basic definitions and facts about integer polymatroids and the main results in [10] are recalled in Section 4.

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 3 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 [5,33], the hierarchical threshold access structures studied by Tassa [35] and by Tassa and Dyn [36], and also the weighted threshold access structures that were first considered by Shamir [32] and studied in [1,2,22,29]. Duality and minors of access structures 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 $\mathbb{K}$-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 3.

Our main result is Theorem 16, 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 [16], we obtain the following theorem.

Theorem 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 [1,16]. Actually, as an application of our results, we present in Section 8 a new proof of the characterization of the ideal weighted threshold access structures that simplifies the complicated proof given by Beimel, Tassa and Weinreb [1].

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 [6]. Moreover, since hierarchical access structures are in particular multipartite, the results and techniques in [10] about the characterization of ideal

multipartite access structures, which are recalled in Section 4, are extremely useful. In particular, integer polymatroids play a fundamental role. Another important tool is the geometric representation introduced in [10,29] for multipartite access structures, which is adapted in Section 3 to the hierarchical case by introducing the *hierarchically minimal points* (or *h-minimal points* for short) 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 h-minimal points, one can efficiently determine whether it is ideal or not. If the access structure is described by its minimal qualified subsets, it is easy to determine the h-minimal points. If the access structure is described in another way, one has to find the h-minimal points, but this can be done efficiently most of the times. This is the case, for instance, of weighted threshold access structures that are determined by the weights and the threshold. Moreover, by combining the results in this paper with the ones on ideal multipartite secret sharing in [10], a method to construct an ideal linear secret sharing scheme for every given ideal hierarchical access structure can be obtained. A more detailed study of this method and the analysis of its efficiency is deferred to future work.

2 Ideal Secret Sharing Schemes and Matroids

We recall in this section some facts about the connection between ideal secret sharing schemes and matroids that is derived from the results by Brickell [5] and by Brickell and Davenport [6]. See [16], for instance, for more information on these topics.

We begin by presenting the method by Brickell [5] to construct ideal secret sharing schemes as described by Massey [18,19] in terms of linear codes. Let C be an $[n+1,k]$-linear code over a finite field $\mathbb{K}$ and let M be a generator matrix of C, that is, a $k \times (n+1)$ matrix over $\mathbb{K}$ whose rows span C. Such a code defines an ideal secret sharing scheme on a set $P = \{p_1, \ldots, p_n\}$ of participants. Specifically, every random choice of a codeword $(s_0, s_1, \ldots, s_n) \in C$ corresponds to a distribution of shares for the secret value $s_0 \in \mathbb{K}$, in which $s_i \in \mathbb{K}$ is the share of the participant p_i. Such an ideal scheme is called a $\mathbb{K}$-*vector space secret sharing scheme* and its access structures is called a $\mathbb{K}$-*vector space access structure*. It is easy to check that a set $A \subseteq P$ is in the access structure Γ of this scheme if and only if the column of M with index 0 is a linear combination of the columns whose indices correspond to the players in A. Therefore, if $Q = P \cup \{p_0\}$ and $\mathcal{M}$ is the representable matroid with ground set Q and rank function r that is defined by the columns of the matrix M, then $\Gamma = \Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : r(A \cup \{p_0\}) = r(A)\}$. That is, Γ is the *port of the matroid* $\mathcal{M}$ *at the point* p_0. Consequently, a sufficient condition for an access structure to be ideal is obtained. Namely, the ports of representable matroids are ideal access structures. Actually, they coincide with the vector space access structures.

As a consequence the results by Brickell and Davenport [6], this sufficient condition is not very far from being necessary. Specifically, they proved that every ideal access structure is a matroid port.

With a slightly different definition, matroid ports were introduced in 1964 by Lehman [15] to solve the *Shannon switching game*, much before secret sharing was invented by Shamir [32] and Blakley [4] in 1979. A forbidden minor characterization of matroid ports was given by Seymour [31]. Even though the results in [5,6] deal with matroid ports, this terminology was not used in those and many other subsequent works on secret sharing. The old results on matroid ports in [15,31] were rediscovered for secret sharing by Martí-Farré and Padró [16], who used them to generalize the result by Brickell and Davenport by proving that, if all shares in a secret sharing scheme are shorter than 3/2 times the secret, then its access structure is a matroid port.

3 Hierarchical Access Structures

We present here a natural definition for the family of the *hierarchical access structures*, which embraces all possible situations in which there is a hierarchy on the set of participants. For instance, the weighted threshold access structures and the hierarchical threshold access structures [35] are contained in this new family. Hierarchical access structures are in particular multipartite. Therefore, we can take advantage of the results and techniques in [10] about the characterization of ideal multipartite access structures. Moreover, the geometric representation for multipartite access structures that was introduced in [10,29] will be very useful as well for our purposes. This representation is adapted here to hierarchical access structures by introducing the *hierarchically minimal* points.

Let Γ be an access structure on a set P of participants. 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 $A \subseteq P \setminus \{p, q\}$ 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 an 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 set P, a sequence $\Pi = (P_1, \ldots, P_m)$ of subsets of P is called here a *partition* of P if $P = P_1 \cup \cdots \cup P_m$ and $P_i \cap P_j = \emptyset$ whenever $i \neq j$. Observe that some of the parts may be empty. An access structure Γ is said to be *Π-partite* if every pair of participants in the same part P_i are hierarchically equivalent. A different but equivalent definition for this concept is given in [10]. If m is the number of parts in Π, such structures are called *m-partite access structures*. The participants that are not in any minimal qualified subset are called *redundant*. An m-partite access structure is said to be *strictly m-partite* if there are no redundant participants, 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 $p \in P_i$ and $q \in P_j$ with $i < j$. That is, the participants in the first level are hierarchically superior to those in the second level and so on. Obviously, an access structure is hierarchical if and only if it is 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 $|\Pi| = m$.

Some notation is needed to recall the geometric representation of multipartite access structures introduced in [10,29]. This notation will be used as well to present in Section 4 the basic facts about integer polymatroids and, because of that, all through the paper. Consider a finite set J. For every two points $u = (u_i)_{i\in J}$ and $v = (v_i)_{i\in J}$ in $\mathbb{Z}^J$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J$. The point $w = u \vee v$ is defined by $w_i = \max\{u_i, v_i\}$ for every $i \in J$. The *modulus* of a point $u \in \mathbb{Z}^J$ is $|u| = \sum_{i\in J} u_i$. For every subset $X \subseteq J$, we notate $u(X) = (u_i)_{i\in X} \in \mathbb{Z}^X$ and $|u(X)| = \sum_{i\in X} u_i$. We notate $\mathbb{Z}_+$ and $\mathbb{Z}_-$ for the sets of the non-negative and the non-positive integers, respectively.

For each partition $\Pi = (P_1, \ldots, P_m)$ of the set P, we consider a mapping $\Pi\colon \mathcal{P}(P) \to \mathbb{Z}_+^m$ defined by $\Pi(A) = (|A \cap P_1|, \ldots, |A \cap P_m|) \in \mathbb{Z}_+^m$. We write $\mathbf{p} = \Pi(P) = (|P_1|, \ldots, |P_m|)$ and $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{u \in \mathbb{Z}_+^m : u \leq \mathbf{p}\}$. For a Π-partite access structure $\Gamma \subseteq \mathcal{P}(P)$, consider $\Pi(\Gamma) = \{\Pi(A) : A \in \Gamma\} \subseteq \mathbf{P}$. Observe that $A \in \Gamma$ if and only if $\Pi(A) \in \Pi(\Gamma)$, so Γ is univocally represented by the set of points $\Pi(\Gamma) \subseteq \mathbf{P}$. 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 points in $\mathbf{P}$.

Let Γ be a Π-partite access structure on P. If two points $u, v \in \mathbf{P}$ 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 points. We are using here an abuse of notation as well, because $\min\Gamma$ denotes also the family of minimal subsets of the access structure 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 $j = 1, \ldots, m$. This motivates the following order relation, which was introduced in [36, Definition 4.2], also in the framework of hierarchical secret sharing. We say that the point $v \in \mathbb{Z}_+^m$ is *hierarchically superior* to the point $u \in \mathbb{Z}_+^m$, and we write $u \preceq v$, if $\sum_{i=1}^{j} u_i \leq \sum_{i=1}^{j} v_i$ for every $j = 1, \ldots, m$. The points in $\mathbf{P}$ that are minimal according to this order are called the *hierarchically minimal points* (or *h-minimal points* for short) of Γ, and the set of these points is denoted by $\operatorname{hmin}\Gamma$. The *hierarchically minimal sets of* Γ are the sets $A \subseteq P$ such that $\Pi(A)$ is a hierarchically minimal point. 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 h-minimal points. 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 h-minimal points is more compact than doing so by its minimal points. 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. For all of them, we consider the same m-partition $\Pi = (P_1, \ldots, P_m)$ of the set p of participants.

Example 2. A *weighted threshold* access structure Γ is defined from a real *weight vector* $w = (w_1, \ldots, w_m) \in \mathbb{R}^m$ 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 $\Gamma = \{u \in \mathbf{P} : u_1 w_1 + \cdots + u_m w_m \geq T\} \subseteq \mathbf{P}$. 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 3. Brickell [5] showed how to construct ideal schemes for the multilevel structures proposed by Simmons [33]. These access structures are of the form $\Gamma = \{A \subseteq P : |A \cap (\cup_{j=1}^{i} P_j)| \geq t_i \text{ for some } i = 1, \ldots, m\}$ for some monotone increasing sequence of integers $0 < t_1 < \ldots < t_m$. Clearly, such an access structure is Π-hierarchical and, if the number of participants in each level is large enough, its h-minimal points are $\operatorname{hmin} \Gamma = \{t_1 \mathbf{e}^1, \ldots, t_m \mathbf{e}^m\}$, where $\mathbf{e}^i$ is the i-th vector of the canonical basis of $\mathbb{R}^m$.

Example 4. Another family of hierarchical threshold access structures was proposed by Tassa [35]. Given integers $0 < t_1 < \ldots < t_m$, they are defined by $\Gamma = \{A \subseteq P : |A \cap (\cup_{j=1}^{i} P_j)| \geq t_i \text{ for every } i = 1, \ldots, m\}$. Such an access structure is Π-hierarchical and, if the number of participants in every level is large enough, its only h-minimal point is $(t_1, t_2 - t_1, \ldots, t_m - t_{m-1})$.

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 $\mathbb{K}$-vector space access structures. More information about these operations on access structures and their relevance in secret sharing can be found in [16]. The *dual* of an access structure Γ on a set P is the access structure on the same set defined by $\Gamma^* = \{A \subseteq P : P \setminus A \notin \Gamma\}$. For a subset $B \subseteq P$, we define the access structures $\Gamma \backslash B$ and Γ / B on the set $P \setminus B$ by $\Gamma \backslash B = \{A \subseteq P \setminus B : A \in \Gamma\}$ and $\Gamma / B = \{A \subseteq P \setminus B : A \cup B \in \Gamma\}$. Every access structure that can be obtained from Γ by repeatedly applying the operations $\backslash$ and $/$ is called a *minor* of Γ. The proof of the following proposition is straightforward.

Proposition 5. *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.*

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 $p \in P'$* is denoted by $\Gamma'[\Gamma''; p]$ and is defined as the access structure on the set of participants $P = P' \cup P'' \setminus \{p\}$ that is formed by all subsets $A \subseteq P$ such that $A \cap P' \in \Gamma'$ and all subsets $A \subseteq P$ such that $(A \cup \{p\}) \cap P' \in \Gamma'$ and $A \cap P'' \in \Gamma''$. The

composition of matroid ports is a matroid port, and the same applies to $\mathbb{K}$-vector space access structures. A proof for these facts can be found in [17]. 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 $(P_1, \ldots, P_r)$-partite and Γ'' is $(P_{r+1}, \ldots, P_{r+s})$-partite, and take $p \in P_r$. Then the composition $\Gamma'[\Gamma''; p]$ is $(P'_1, \ldots, P'_{r+s})$-partite with $P'_r = P_r \setminus \{p\}$ and $P'_i = P_i$ if $i \neq r$. If Γ' and Γ'' are hierarchical, then $\Gamma'[\Gamma''; p]$ is also hierarchical. Observe that the composition is made over a participant in the lowest level of Γ'.

4 Multipartite Matroid Ports and Integer Polymatroids

The aim of this and the following sections is to present our main result, Theorem 16, which is a complete characterization of the ideal hierarchical access structures in terms of the properties of their h-minimal points. First we recall here some facts about integer polymatroids and we show the connection between these combinatorial objects and multipartite matroids and their ports. Since all ideal access structures are matroid ports, we obtain in this way some necessary conditions for a hierarchical access structure to be ideal in Section 5. Finally, in Sections 6 and 7 we show that these necessary conditions are also sufficient.

Multipartite matroid ports are ports of *multipartite matroids*, and those matroids are closely related to *integer polymatroids*. We recall here some definitions and basic facts about integer polymatroids and multipartite matroids, the relation between these two combinatorial objects, and their connections to the characterization of multipartite access structures. We use in the following the notation for integer vectors that was introduced in Section 3. More information about these concepts can be found in [10,12].

Similarly to matroids, integer polymatroids can be defined in many different but equivalent ways. We present next the three of those definitions that are needed to present our results. The first one is in terms of an integer submodular rank function. The second one considers an integer polymatroid as a set of integer vectors with certain properties. Finally, the third one is given in terms of the integer bases, which are the maximal elements in that set of integer vectors. The equivalence between these definitions is a consequence of results on submodular functions that are well known in the areas of combinatorial optimization and discrete convex analysis (see, for instance, the works by Murota [23,24]). A full proof of this equivalence has been presented by Herzog and Hibi [12], who used integer polymatroids in commutative algebra. The formalization of these combinatorial concepts presented in [12] has been very useful for our purposes. Actually, a new term (*discrete polymatroid*) was introduced in [12] to denote the set of integer vectors defining an integer polymatroid. In our opinion, this new term is not needed because these sets should be considered as an alternative way to define integer polymatroids, and not as a new combinatorial object. Actually, they are formed by the integer points in the convex polytope associated to the integer polymatroid. See [37], for instance, for more information about polymatroids and their associated polytopes.

We notate $\mathcal{P}(J)$ for the power set of a set J. An *integer polymatroid* is an ordered pair $\mathcal{Z} = (J, h)$, where J is a finite set, the *ground set*, and h, the *rank function*, is a mapping $h\colon \mathcal{P}(J) \to \mathbb{Z}$ satisfying the following properties

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

An integer polymatroid with ground set J can be defined as well as a nonempty finite set $\mathcal{D} \subseteq \mathbb{Z}_+^J$ of integer points satisfying the following properties.

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

The equivalence between these two definitions can be proved as follows. On the one hand, one has to check that, given an integer polymatroid $\mathcal{Z} = (J, h)$, such a set of integer points is univocally determined by the rank function by $\mathcal{D} = \mathcal{D}(\mathcal{Z}) = \{u \in \mathbb{Z}_+^J : |u(X)| \leq h(X) \text{ for every } X \subseteq J\}$. On the other hand, it can be proved that, given a set $\mathcal{D} \subseteq \mathbb{Z}_+^J$ satisfying the properties above, there is a unique integer polymatroid $\mathcal{Z} = (J, h)$ with $\mathcal{D} = \mathcal{D}(\mathcal{Z})$, and its rank function is defined by $h(X) = \max\{|u(X)| : u \in \mathcal{D}\}$ for every $X \subseteq J$.

An *integer basis* of an integer polymatroid $\mathcal{Z}$ is a maximal element in $\mathcal{D}(\mathcal{Z})$, that is, a point $u \in \mathcal{D}$ such that there does not exist any $v \in \mathcal{D}$ with $u < v$. Since we are not going to consider here any other kind of bases of integer polymatroids, from now on integer bases will be called simply bases. Similarly to matroids, all bases have the same modulus, and integer polymatroids are completely determined by their bases. Moreover, a nonempty set $\mathcal{B} \subseteq \mathbb{Z}_+^J$ is the family of 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 $u - \mathbf{e}^i + \mathbf{e}^j \in \mathcal{B}$, where $\mathbf{e}^i \in \mathbb{Z}^J$ is such that $\mathbf{e}^i_k = 0$ if $i \neq k$ and $\mathbf{e}^i_i = 1$.

Because of that, this can be seen as another definition of integer polymatroid.

For an integer polymatroid $\mathcal{Z} = (J, h)$ and a subset $X \subseteq J$, we consider the integer polymatroid $\mathcal{Z}(X) = (X, h')$ defined by $h'(Y) = h(Y)$ for every $Y \subseteq X$. Since h' is a restriction of h, both will be usually denoted by h. Clearly, $\mathcal{D}(\mathcal{Z}(X)) = \{u(X) : u \in \mathcal{D}(\mathcal{Z})\} \subseteq \mathbb{Z}_+^X$. We consider as well the set of points $\mathcal{B}(\mathcal{Z}, X) \subseteq \mathbb{Z}_+^J$ such that $u \in \mathcal{B}(\mathcal{Z}, X)$ if and only if $u(X)$ is a basis of $\mathcal{Z}(X)$ and $u_i = 0$ for every $i \in J \setminus X$.

For a partition $\Pi = (Q_1, \ldots, Q_m)$ of the ground set Q, a matroid $\mathcal{M} = (Q, r)$ is said to be *Π-partite* if every permutation σ on Q such that $\sigma(Q_i) = Q_i$ for $i = 1, \ldots, m$ is an automorphism of $\mathcal{M}$. From now on, we notate $J_m = \{1, \ldots, m\}$ and $J'_m = \{0, 1, \ldots, m\}$ for every positive integer m. Then the function $h\colon \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = r(\bigcup_{i \in X} Q_i)$ is the rank function of an integer polymatroid $\mathcal{Z}(\mathcal{M}) = (J_m, h)$. Reciprocally, for every integer polymatroid $\mathcal{Z} = (J_m, h)$ with $h(\{i\}) \leq |Q_i|$ for $i \in J_m$, there exists a unique Π-partite matroid $\mathcal{M}$ with $\mathcal{Z}(\mathcal{M}) = \mathcal{Z}$.

Consider a partition $\Pi = (P_1, \ldots, P_m)$ of a set P and the partition $\Pi_0 = (\{p_0\}, P_1, \ldots, P_m)$ of the set $Q = P \cup \{p_0\}$. A connected matroid port $\Gamma = \Gamma_{p_0}(\mathcal{M})$ on P is Π-partite if and only if the matroid $\mathcal{M}$ is Π_0-partite. Therefore, multipartite matroids, and hence integer polymatroids, are fundamental in the characterization of ideal multipartite access structures. These connections are in the core of the results in [10]. In particular, we present next a characterization of multipartite matroid ports in terms of integer polymatroids that was proved in [10] and will be extremely useful for our purposes.

Consider a Π-partite matroid port $\Gamma = \Gamma_{p_0}(\mathcal{M})$ and the associated integer polymatroid $\mathcal{Z}' = \mathcal{Z}(\mathcal{M}) = (J'_m, h)$. The Π-partite matroid port Γ is completely determined by the partition Π and the integer polymatroid $\mathcal{Z}'$ and we write $\Gamma = \Gamma_0(\mathcal{Z}')$. As a consequence of this fact, the following characterization of multipartite matroid ports is proved in [10].

Theorem 6 ([10]). *Let $\Pi = (P_1, \ldots, P_m)$ be a partition of a set P and let Γ be an Π-partite access structure on P. Then Γ is a matroid port if and only if there exists an integer polymatroid $\mathcal{Z}' = (J'_m, h)$ with $h(\{0\}) = 1$ and $h(\{i\}) \leq |P_i|$ such that*

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

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

Since every ideal access structure is a matroid port, Theorem 6 provides a necessary condition for a multipartite access structure to be ideal. Several necessary conditions for a hierarchical access structure to be ideal will be deduced from this result in Section 5.

On the other hand, sufficient conditions can be obtained from the fact that the ports of linearly representable matroids are ideal access structures. We present in Theorem 7 an interesting result from [10] connecting the linear representations of multipartite matroids to the ones of integer polymatroids. This result is used in Section 6 to find sufficient conditions for a hierarchical access structure to be ideal.

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

Theorem 7 ([10]). *For every large enough field $\mathbb{K}$, an m-partite matroid $\mathcal{M}$ is $\mathbb{K}$-linearly representable if and only if its associated integer polymatroid $\mathcal{Z}(\mathcal{M}) = (J_m, h)$ is $\mathbb{K}$-linearly representable.*

5 Hierarchical Matroid Ports

In this section, we use the connection between integer polymatroids and multipartite matroid ports that is discussed in Section 4 to find necessary conditions

for hierarchical access structures to be matroid ports. Of course, these will be as well necessary conditions for hierarchical access structures to be ideal.

We present first a technical lemma that apply to every integer polymatroid. Specifical results on integer polymatroids associated to hierarchical matroid ports will be given afterwards. Due to space constraints, the proofs of most of these results are omitted.

For every $i, j \in \mathbb{Z}$ we notate $[i, j] = \{i, i+1, \ldots, j\}$ if $i < j$, while $[i, i] = \{i\}$ and $[i, j] = \emptyset$ if $i > j$. Let $\mathcal{Z} = (J_m, h)$ be an integer polymatroid. For every $i \in J_m$, consider the point $y^i(\mathcal{Z}) \in \mathbb{Z}_+^m$ defined by $y^i_j(\mathcal{Z}) = h([j, i]) - h([j+1, i])$. Observe that $\sum_{j=s}^{i} y^i_j(\mathcal{Z}) = h([s, i])$ for every $s \in [1, i]$. In addition, by the submodularity of the rank function, $y^i_j(\mathcal{Z}) \geq y^{i+1}_j(\mathcal{Z})$ if $1 \leq j \leq i < m$.

Lemma 8. *For every $i = 1, \ldots, m$, the point $y^i(\mathcal{Z})$ is the hierarchically minimum point of $\mathcal{B}(\mathcal{Z}, [1, i])$, that is, $y \in \mathcal{B}(\mathcal{Z}, [1, i])$ and $y \preceq x$ for every $x \in \mathcal{B}(\mathcal{Z}, [1, i])$.*

For the remaining of this section, we assume that Γ is a Π-hierarchical matroid port, where $\Pi = (P_1, \ldots, P_m)$ is an m-partition of the set of participants P. Recall that we notate $\mathbf{P} = \Pi(\mathcal{P}(P)) \subseteq \mathbb{Z}_+^m$. In addition, we assume that the access structure Γ is *connected*, that is, that every participant is in a minimal qualified subset or, equivalently, for every $i \in J_m$, there is a minimal point $x \in \min \Gamma$ such that $x_i > 0$. Consider the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $\Gamma = \Gamma_0(\mathcal{Z}')$, and the integer polymatroid $\mathcal{Z} = \mathcal{Z}'(J_m) = (J_m, h)$. Since Γ is connected, $h(\{i\}) > 0$ for all $i \in J_m$, and hence $y^i_i(\mathcal{Z}) > 0$. For every $x \in \mathbb{Z}_+^m$, we notate $\mathrm{supp}(x) = \{i \in J_m : x_i \neq 0\} \subseteq J_m$ and $s(x) = \max(\mathrm{supp}(x))$. Observe that $s(x)$ is the index of the most inferior hierarchical level represented in the sets $A \subseteq P$ with $\Pi(A) = x$.

Lemma 9. *If $x \in \mathbf{P}$ is a minimal point of Γ, then $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$.*

Lemma 10. *If $x \in \mathbf{P}$ is an h-minimal point of Γ, then $x = y^{s(x)}(\mathcal{Z})$.*

Proof. From Lemma 9, $x \in \mathcal{B}(\mathcal{Z}, [1, s(x)])$ and, since $\mathcal{B}(\mathcal{Z}, [1, s(x)]) \subseteq \Gamma$ by Theorem 6, x is h-minimal in $\mathcal{B}(\mathcal{Z}, [1, s(x)])$. By Lemma 8, this implies that $x = y^{s(x)}(\mathcal{Z})$. □

At this point, we have identified the h-minimal points of the hierarchical matroid port Γ. Namely, they are the h-minimal elements in $\{y^1(\mathcal{Z}), \ldots, y^m(\mathcal{Z})\}$.

Lemma 11. *If $x, y \in \mathbf{P}$ are two different h-minimal points of Γ, then $s(x) \neq s(y)$. Moreover, if $s(x) < s(y)$, then $|x| < |y|$ and $x_j \geq y_j$ for all $j = 1, \ldots, s(x)$.*

Proof. Since $s(y^i(\mathcal{Z})) = i$, it is clear that $s(x) \neq s(y)$ if $x \neq y$. Suppose that $s(x) < s(y)$. Since $|x| = h([1, s(x)])$ and $|y| = h([1, s(y)])$, we have that $|x| \leq |y|$. Moreover, if $|x| = |y|$, then $x \in \mathcal{B}(\mathcal{Z}, [1, s(y)])$, and hence $y \preceq x$, a contradiction. Finally, $x_j = y^{s(x)}_j(\mathcal{Z}) \geq y^{s(y)}_j(\mathcal{Z}) = y_j$ for all $j = 1, \ldots, s(x)$. □

As a consequence of Lemma 11, the h-minimal points in a hierarchical matroid port behave as in the hierarchical threshold access structure proposed by Simmons [33] (Example 3). Namely, if A and B are both hierarchically minimal qualified sets, but the least member of B is strictly inferior to the least member of A, then B must be larger than A. The last necessary condition for a hierarchical access structure to be ideal is given in the following lemma, whose proof is also omitted here.

Lemma 12. *Let $x, y \in \mathbf{P}$ be two different h-minimal points of Γ with $s(x) < s(y)$ such that there is not any h-minimal point z with $s(x) < s(z) < s(y)$. If $x_i > y_i$ for some $i \in [1, s(x) - 1]$, then $|P_j| = x_j$ for all $j \in [i + 1, s(x)]$.*

6 A Family of Ideal Hierarchical Access Structures

The results in Section 5 provide necessary conditions for a Π-hierarchical access structure to be a matroid port, and hence to be ideal, in terms of the properties of its h-minimal points. A sufficient condition is given in this section by constructing a new family of hierarchical vector space secret sharing schemes. Specifically, we present a family of linearly representable integer polymatroids and we prove that the multipartite access structures that are obtained from them are actually hierarchical. In addition, they are vector space access structures by Theorem 7.

Consider a finite field $\mathbb{K}$ and a pair of integer vectors $\mathbf{a} = (a_0, \ldots, a_m) \in \mathbb{Z}_+^{m+1}$ and $\mathbf{b} = (b_0, \ldots, b_m) \in \mathbb{Z}_+^{m+1}$ such that $a_0 = a_1 = b_0 = 1$, and $a_i \leq a_{i+1} \leq b_i \leq b_{i+1}$ for every $i = 0, \ldots m-1$. Take $d = b_m$ and consider a basis $\{e^1, \ldots, e^d\}$ of $\mathbb{K}^d$ and, for every $i = 1, \ldots, m$, consider the subspace $V_i = \langle e^{a_i}, \ldots, e^{b_i} \rangle \subseteq \mathbb{K}^d$. Let $\mathcal{Z}' = \mathcal{Z}'(\mathbf{a}, \mathbf{b}) = (J'_m, h)$ be the integer polymatroid that is linearly represented by the subspaces $V_0, V_1, \ldots, V_m$. Observe that the rank function h of $\mathcal{Z}'$ is such that $h(A) = |\cup_{i \in A} [a_i, b_i]|$ for all $A \subseteq J'_m$. In particular, $h([j, i]) = |[a_j, b_i]| = b_i - a_j + 1$ whenever $0 \leq j \leq i \leq m$, and hence $h(\{0\}) = 1$. Therefore, for every set of players P and for every m-partition $\Pi = (P_1, \ldots, P_m)$ of P such that $|P_i| \geq h(\{i\}) = b_i - a_i + 1$, we can consider the Π-partite matroid port $\Gamma = \Gamma_0(\mathcal{Z}')$ that is determined as in Theorem 6. Since $\mathcal{Z}'$ is $\mathbb{K}$-linearly representable for every finite field $\mathbb{K}$, we have from Theorem 7 that Γ is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$.

Consider the integer polymatroid $\mathcal{Z} = \mathcal{Z}(\mathbf{a}, \mathbf{b}) = \mathcal{Z}'(J_m) = (J_m, h)$ and, for $i = 1, \ldots, m$, the points $y^i = y^i(\mathcal{Z}) \in \mathbb{Z}_+^m$. Observe that $y^i_j = h([j, i]) - h([j + 1, i]) = a_{j+1} - a_j$ if $j < i$ while $y^i_i = b_i - a_i + 1$. Therefore, $y^i = (a_2 - a_1, \ldots, a_i - a_{i-1}, b_i - a_i + 1, 0, \ldots, 0)$. A proof for the following lemma, which is the key result in this section, will be given in the full version.

Lemma 13. *The access structure Γ is Π-hierarchical.*

By taking into account Lemma 13 and the fact that the h-minimal points of Γ are of the form $y^i(\mathcal{Z}(\mathbf{a}, \mathbf{b}))$, the next proposition can be proved. It provides a sufficient condition for a hierarchical access structure to be ideal.

Proposition 14. *Let $\Pi = (P_1, \ldots, P_m)$ be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P. Let $x^1, \ldots, x^r \in \mathbb{Z}_+^m$ be the h-minimal points of Γ and consider $s_i = s(x^i) = \max(\mathrm{supp}(x^i))$. Suppose that the following properties are satisfied.*

1. *If $i < j$, then $s_i < s_j$ and $x^i_k = x^j_k$ for all $k = 1, \ldots, s_i - 1$.*
2. *If $s_{j-1} < i \leq s_j$, then $|P_i| \geq \sum_{\ell=i}^{s_j} x^j_\ell$.*

Then Γ is ideal and, moreover, it admits a $\mathbb{K}$-vector space secret sharing scheme for every finite field $\mathbb{K}$ with $|\mathbb{K}| > \binom{|P|+1}{|x^r|}$.

The bound on the size of the field is a consequence of the results in [10] (full version) about the representability of multipartite matroids. Observe that, in particular, all hierarchical access structures that have only one h-minimal point are vector space access structures. Because of that, it can be proved by using well known basic decomposition techniques (see [34], for instance) that every hierarchical access structure admits a linear secret sharing scheme in which the length of every share is at most m times the length of the secret, being m the number of h-minimal points.

7 A Characterization of Ideal Hierarchical Access Structures

By using the results in Sections 5 and 6, we present here a complete characterization of ideal hierarchical access structures. Moreover, we prove that every ideal hierarchical access structure is a $\mathbb{K}$-vector space access structure for every large enough finite field $\mathbb{K}$. The next result is a consequence of Proposition 14 and the necessary conditions for a hierarchical access structure to be ideal given in Section 5. It provides a characterization of hierarchical access structures in which the number of participants in every hierarchical level is large enough in relation to the h-minimal points. The proof of this result is omitted here.

Theorem 15. *Let $\Pi = (P_1, \ldots, P_m)$ be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P with $\mathrm{hmin}\,\Gamma = \{x^1, \ldots, x^r\}$. For $i = 1, \ldots, r$, consider $s_i = s(x^i) = \max(\mathrm{supp}(x^i))$ and suppose that $|P_{s_i}| > x^i_{s_i}$. Then Γ is ideal if and only if*

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

Moreover, in this situation Γ is a $\mathbb{K}$-vector space access structure for every finite field $\mathbb{K}$ with $|\mathbb{K}| > \binom{|P|+1}{|x^r|}$.

Finally, we present our complete characterization of ideal hierarchical access structures in terms of the properties of the h-minimal points. Actually, we prove

that a hierarchical access structure is ideal if and only if it is a minor of an access structure in the family that is presented in Section 6. Therefore every ideal hierarchical access structure is a $\mathbb{K}$-vector access structure for all large enough finite fields $\mathbb{K}$, and this proves Theorem 1. The proof of this result will be presented in the full version.

Theorem 16. *Let $\Pi = (P_1, \ldots, P_m)$ be an m-partition of a set P and let Γ be a Π-hierarchical access structure on P with $\min_H \Gamma = \{x^1, \ldots, x^r\}$. For $i = 1, \ldots, m$, consider $s_i = s(x^i) = \max(\mathrm{supp}(x^i))$ and suppose that the h-minimal points are ordered in such a way that $s_i \leq s_{i+1}$. Then Γ is ideal if and only if*

1. *$s_i < s_{i+1}$ and $|x^i| < |x^{i+1}|$ for all $i = 1, \ldots, r-1$, and*
2. *$x^i_j \geq x^{i+1}_j$ if $1 \leq i \leq r-1$ and $1 \leq j \leq s_i$, and*
3. *if $x^i_j > x^r_j$ for some $1 \leq i < r$ and $1 \leq j < s_i$, then $|P_k| = x^i_k$ for all $k = j+1, \ldots, s_i$.*

We present in the following a few examples of applications of our characterization of the ideal hierarchical access structures.

Example 17. Consider a set P with a 4-partition $\Pi = (P_1, P_2, P_3, P_4)$ with $|P_i| = 4$ for every $i = 1, \ldots, 4$. Let Γ be the weighted threshold access structure defined as in Example 2 by the weight vector $w = (7, 5, 4, 3)$ and the threshold $T = 13$. The h-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 $|P_3| > x^2_3$, it follows from Theorem 16 that Γ is not ideal.

Example 18. For a 4-partition $\Pi = (P_1, P_2, P_3, P_4)$ of the set P of participants and positive integers $0 < t_1 < t_2 < t_3 < t_4$, consider the Π-hierarchical access structure Γ that is formed by the sets with at least one participant from P_1 that, in addition, have t_1 participants in P_1, or t_2 participants in $P_1 \cup P_2$, or t_3 participants in $P_1 \cup P_2 \cup P_3$, or t_4 participants in total. If the number of participants in each part is large enough, then Γ is ideal by Theorem 16 because its h-minimal points are $(1, 0, 0, t_4)$, $(1, 0, t_3, 0)$, $(1, t_2, 0, 0)$, and $(t_1, 0, 0, 0)$. In any other case, Γ is a minor of a 4-hierarchical access structure having those h-minimal points, and hence it is ideal as well.

Example 19. From the constructions by Brickell [5] and by Tassa [35], we know that the access structures described in Examples 3 and 4 are ideal. Actually, this fact is proved very easily from our results. The h-minimal points of the access structures in Example 3 are $\mathrm{hmin}\,\Gamma = \{t_1\mathbf{e}^1, \ldots, t_m\mathbf{e}^m\}$, which clearly satisfy the conditions in Theorem 16. Since the access structures in Example 4 have only one h-minimal point, they are ideal as well.

Example 20. Tassa [35] proposed an open problem on hierarchical access structures that can be solved by using our results. For a partition $\Pi = (P_1, \ldots, P_m)$ of the set P of participants, a sequence of integers $0 < t_1 < \cdots < t_m$, and an integer $\ell \in J_m$, consider the Π-hierarchical access structure Γ defined as follows: A point $u \in \mathbf{P}$ is in Γ if and only if $|\{i \in J_m : \sum_{j=1}^{i} u_j \geq k_i\}| \geq \ell$. The open

problem proposed by Tassa [35] is to determine what access structures of this form are ideal. Observe that the extreme cases $\ell = 1$ and $\ell = m$ correspond to the ideal hierarchical access structures in Examples 3 and 4, respectively. By using the results in this paper it can be proved that, if Γ is connected, then it is ideal if and only if $\ell = 1$ or $\ell = m$. This is proved by finding, for every connected access structure of this form with $1 < \ell < m$, two different h-minimal points $x, y \in \operatorname{hmin}\Gamma$ with $s(x) = s(y)$.

8 Ideal Weighted Threshold Access Structures

Beimel, Tassa and Weinreb [1] presented a characterization of the ideal weighted threshold access structures. Their proof is long and complicated. By using our characterization of ideal hierarchical access structures, we obtained a simpler proof for the result in [1]. Due to space constraints, we can only present here a sketch of it. The complete proof will be given in the full version of the paper.

As was noticed in [1], an ideal weighted threshold access structure can be the composition smaller such ideal structures Because of that, we focus on the indecomposable structures in this family.

First, we describe several families of ideal weighted threshold access structures such that, as is stated in Theorem 21, they contain all indecomposable ideal weighted threshold access 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 three families of ideal bipartite hierarchical access structures, that is, ideal Π-hierarchical access structures for some partition $\Pi = (P_1, P_2)$ of the set of participants. The family $\mathbf{B}_1$ consists of the access structures with $\operatorname{hmin}\Gamma = \{(x_1, x_2)\}$, where $0 < x_1 < |P_1|$ and $0 < x_2 = |P_2| - 1$. The family $\mathbf{B}_2$ is formed by the access structures with $\operatorname{hmin}(\Gamma) = \{(x_1, 0), (0, x_1 + 1)\}$ for some integer $x_1 > 1$. The family $\mathbf{B}_3$ contains the access structures with $\operatorname{hmin}\Gamma = \{(y_1 + y_2 - 1, 0), (y_1, y_2)\}$, where $y_1 > 0$, $y_2 > 2$, and $|P_2| \leq y_2 \leq |P_2| + 1$. In addition, we consider three families of ideal tripartite hierarchical access structures. The family $\mathbf{T}_1$ consists of the structures with $\operatorname{hmin}\Gamma = \{(x_1, 0, 0), (0, y_2, y_3)\}$, where $0 < y_2 < |P_2|$ and $1 < y_3 = |P_3| - 1$, and $x_1 = y_2 + y_3 - 1$. We consider as well the family $\mathbf{T}_2$ of the structures such that $\operatorname{hmin}\Gamma = \{(x_1, 0, 0), (y_1, y_2, y_3)\}$ with $0 < y_2 = |P_2|$ and $1 < y_3 = |P_3| - 1$, and $x_1 = y_1 + y_2 + y_3 - 1$. Finally, the family $\mathbf{T}_3$ 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 $1 < y_3 = |P_3|$, and $0 < x_2 = y_2 + 1 = |P_2|$, and $x_1 + x_2 = y_1 + y_2 + y_3 - 1$. It can be proved that all the members of these families are weighted threshold access structures. At this point, we can state the characterization of the ideal weighted threshold access structures.

Theorem 21. *A weighted threshold access structure 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* $\mathbf{B}_1$, $\mathbf{B}_2$ *or* $\mathbf{B}_3$, *or*

3. *it is a tripartite access structure in one of the families* $\mathbf{T}_1$, $\mathbf{T}_2$ *or* $\mathbf{T}_3$, *or*
4. *it is a composition of smaller ideal weighted threshold access structures.*

We present next a sketch of our proof for this result. To begin with, several technical results on the properties of h-minimal points in indecomposable hierarchical access structures are needed. Then, several properties that must be satisfied by every ideal indecomposable weighted threshold access structure Γ are proved. First, if Γ is strictly bipartite, then it is in one of the families $\mathbf{B}_1$, $\mathbf{B}_2$ or $\mathbf{B}_3$. Second, if Γ is strictly m-partite with $m \geq 3$, then it has exactly two h-minimal points. Third, if Γ is strictly tripartite, then it is in one of the families $\mathbf{T}_1$, $\mathbf{T}_2$ or $\mathbf{T}_3$. Finally, it is proved that such an access structure cannot be strictly m-partite with $m > 3$.

Acknowledgements

The authors thank Ronald Cramer and Enav Weinreb for useful discussions, comments and suggestions. The authors thank as well the anonymous referees for their careful revision of the paper and their valuable comments that greatly improved the presentation of the paper.

References

1. Beimel, A., Tassa, T., Weinreb, E.: Characterizing Ideal Weighted Threshold Secret Sharing. SIAM J. Discrete Math. 22, 360–397 (2008)
2. Beimel, A., Weinreb, E.: Monotone Circuits for Monotone Weighted Threshold Functions. Information Processing Letters 97, 12–18 (2006)
3. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, Heidelberg (1990)
4. Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS Conference Proceedings, vol. 48, pp. 313–317 (1979)
5. Brickell, E.F.: Some ideal secret sharing schemes. J. Combin. Math. and Combin. Comput. 9, 105–113 (1989)
6. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. Cryptology 4, 123–134 (1991)
7. Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: On the size of shares of secret sharing schemes. J. Cryptology 6, 157–168 (1993)
8. Collins, M.J.: A Note on Ideal Tripartite Access Structures. Cryptology ePrint Archive, Report 2002/193, http://eprint.iacr.org/2002/193
9. Csirmaz, L.: The size of a share must be large. J. Cryptology 10, 223–231 (1997)
10. Farràs, O., Martí-Farré, J., Padró, C.: Ideal Multipartite Secret Sharing Schemes. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 448–465. Springer, Heidelberg (2007), http://eprint.iacr.org/2006/292
11. Herranz, J., Sáez, G.: New Results on Multipartite Access Structures. In: IEE Proceedings of Information Security, vol. 153, pp. 153–162 (2006)
12. Herzog, J., Hibi, T.: Discrete polymatroids. J. Algebraic Combin. 16, 239–268 (2002)

13. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing any access structure. In: Proc. IEEE Globecom 1987, pp. 99–102 (1987)
14. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. IEEE Trans. Inform. Theory 29, 35–41 (1983)
15. Lehman, A.: A solution of the Shannon switching game. J. Soc. Indust. Appl. Math. 12, 687–725 (1964)
16. Martí-Farré, J., Padró, C.: On Secret Sharing Schemes, Matroids and Polymatroids. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 273–290. Springer, Heidelberg (2007), the full version of this paper is available at the Cryptology ePrint Archive, http://eprint.iacr.org/2006/077
17. Martí-Farré, J., Padró, C.: Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. Des. Codes Cryptogr. 52, 1–14 (2009)
18. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, Molle, Sweden, August 1993, pp. 269–279 (1993)
19. Massey, J.L.: Some applications of coding theory in cryptography. In: Codes and Ciphers: Cryptography and Coding IV, pp. 33–47 (1995)
20. Matúš, F.: Matroid representations by partitions. Discrete Math. 203, 169–194 (1999)
21. Matúš, F.: Two Constructions on Limits of Entropy Functions. IEEE Trans. Inform. Theory 53, 320–330 (2007)
22. Morillo, P., Padró, C., Sáez, G., Villar, J.L.: Weighted Threshold Secret Sharing Schemes. Inf. Process. Lett. 70, 211–216 (1999)
23. Murota, K.: Discrete convex analysis. Math. Programming 83, 313–371 (1998)
24. Murota, K.: Discrete convex analysis. SIAM Monographs on Discrete Mathematics and Applications. SIAM, Philadelphia (2003)
25. Ng, S.-L.: A Representation of a Family of Secret Sharing Matroids. Des. Codes Cryptogr. 30, 5–19 (2003)
26. Ng, S.-L.: Ideal secret sharing schemes with multipartite access structures. IEE Proc.-Commun. 153, 165–168 (2006)
27. Ng, S.-L., Walker, M.: On the composition of matroids and ideal secret sharing schemes. Des. Codes Cryptogr. 24, 49–67 (2001)
28. Oxley, J.G.: Matroid theory. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York (1992)
29. Padró, C., Sáez, G.: Secret sharing schemes with bipartite access structure. IEEE Trans. Inform. Theory 46, 2596–2604 (2000)
30. Padró, C., Sáez, G.: Correction to Secret Sharing Schemes With Bipartite Access Structure. IEEE Trans. Inform. Theory 50, 1373–1373 (2004)
31. Seymour, P.D.: A forbidden minor characterization of matroid ports. Quart. J. Math. Oxford Ser. 27, 407–413 (1976)
32. Shamir, A.: How to share a secret. Commun. of the ACM 22, 612–613 (1979)
33. Simmons, G.J.: How to (Really) Share a Secret. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 390–448. Springer, Heidelberg (1990)
34. Stinson, D.R.: An explication of secret sharing schemes. Des. Codes Cryptogr. 2, 357–390 (1992)
35. Tassa, T.: Hierarchical Threshold Secret Sharing. J. Cryptology 20, 237–264 (2007)
36. Tassa, T., Dyn, N.: Multipartite Secret Sharing by Bivariate Interpolation. J. Cryptology 22, 227–258 (2009)
37. Welsh, D.J.A.: Matroid Theory. Academic Press, London (1976)