ACCESS STRUCTURES INDUCED BY POLYMATROIDS WITH EXTREME RANK FUNCTION

MIECZYSŁAW KULA

Institute of Mathematics,
University of Silesia, Katowice, Poland

Abstract. In this paper we consider multipartite access structures obtained from polymatroids with extreme rank function. They are proved to be ideal and partially hierarchical. It turns out that the family of structures induced by polymatroids with minimal rank function is a natural generalization of the class of disjunctive access structure considered by Simmons [14] and the class of conjunctive access structures introduced by Tassa [15]. The results are based on the connections between multipartite access structures and polymatroids discovered by Farràs, Martí-Farré and Padró [6].

1. Introduction

Secret sharing was originally introduced independently by Blakley [2] and Shamir [13] in 1979 and is used in many cryptographic protocols.

In a secret sharing scheme every participant is given a share, that is partial information about the secret. Only *authorized* sets of participants can recover the secret by pooling their shares together. The family Γ of these subsets of the set of participants P which are able to recover the secret is called the *access structure*. It is easily seen that Γ, is monotone increasing, which means that any superset of an authorized subset is also authorized. To avoid trivial cases, we assume that $\emptyset \notin \Gamma$ and $P \in \Gamma$. If every unauthorized set of participants cannot reveal any information about the secret, then the secret sharing is said to be *perfect*.

Ito, Saito, Nishizeki [9] and Benaloh, Leichter [1] independently proved, that every monotonic family of subsets of P admits a perfect secret sharing scheme, therefore every monotonic family of subsets of participants is called an access structure. An access structure is said to be *connected* if every participant in P is a member of a minimal authorized set that is, each participant is important. If the set of participants of an access structure can be divided into several parts and all participants in the same part play an equivalent role, then the access structures is said to be *multipartite*. The use of this concept allows to describe the structures in a compact way, by using a few conditions that are independent of the total number of participants.

Given a secret sharing scheme, let S_0 be the set of all possible secrets and let S_p be the set of all possible values of shares that can be assigned to the participant p for every $p \in P$. One can show that for every perfect secret sharing scheme with connected access structure the size of S_0 is not greater than the size of S_p for all $p \in P$. A perfect secret sharing scheme is called *ideal* if $|S_0| = |S_p|$ for all $p \in P$. In other words, the length in bits of every share is

E-mail address: mkula@us.edu.pl.

2020 *Mathematics Subject Classification.* 94A62, 94A60.

Key words and phrases. secret sharing, multipartite access structure, ideal access structure, partially hierarchical access structure, integer polymatroids.

the same as the length of the secret. The secret sharing schemes constructed for given access structure in [9] and [1] are very far from being ideal because the length of the shares grows exponentially with the number of participants. An access structures is said to be *ideal*, if it can be realized as the access structure of an ideal secret sharing scheme.

The characterization of ideal access structures is one of the main open problems in the secret sharing theory. The connections between ideal access structure and matroid ports discovered by Brickell and Davenport in papers [3] and [4] was an important step towards solving this problem. Those results were generalized in [6] by using polymatroids to study ideal multipartite access structures. But this problem still seems to be extremely difficult and only some particular results are known. A complete characterization of ideal totally hierarchical access structure has been proved by Farràs and Padró [7]. Several families of ideal access structure are presented in [8]. The use of polymatroids has opened up new possibilities for the construction of new ideal access structures which are partially hierarchical or compartmented. Given a specific class of polymatroids, one can take all access structures induced by the polymatroids and investigate their properties. This approach ensures that the objects under consideration are matroids ports, so they satisfy necessary condition to be ideal proved by Brickell. In some cases, for instance if the used polymatroids are linearly representable, the obtained access structures are indeed ideal. This is the case we deal with in this paper, where we consider access structures determined by polymatroids with extreme rank function. This idea is also used in [10] for investigation access structures obtained from uniform polymatroids. For more background on the access structures and detailed description of the connections of secret sharing with matroid theory, the reader may consult [3, 4, 11]. More information about the known classes of ideal access structures can be found in [6, 7, 8].

Multipartite access structures are defined in Subsection 2.1 A short introduction to matroids and polymatroids and their relation to access structures are presented in Subsection 2.2. The connections between access structures and matroids are recalled here in Theorems 1 and 2. It follows from Theorem 4 (by Farràs, Martí-Farré and Padró [6]) that every polymatroid with the ground set J and a monotonic family of subsets of J which is compatible with the polymatroid induce a unique access structure which is a matroid port. The details are described in Remark 6. In Subsection 2.3 extreme polymatroids and their Boolean representations are introduced.

Access structures induced by polymatroids with maximal rank function are considered in Section 3. It is proved that those access structure are ideal and compartmented i.e., the participants are hierarchically equivalent or independent. They are special cases of access structures with lower bound considered first by Brickell [3].

Section 4 begins with a characterization of monotonic families of subsets of J, which are compatible with a polymatroid with minimal rank function. In Theorem 12 we prove that all access structures induced by the polymatroid are connected and ideal. Moreover, elements of those access structures are characterized by a collection of threshold conditions. Then the hierarchical orders of the obtained access structures are discussed in Theorem 13. Finally, we point out that disjunctive access structure introduced by Simmons [14] and conjunctive access structure studied by Tassa [15] are special cases of the access structures induced by polymatroids with minimal rank function.

2. Preliminaries

We use similar notations and definitions as in [10], but we recall them here to make the article self-contained.

The family of all subsets of a set X is denoted by $\mathcal{P}(X)$ (the power set). Let $\mathbb{N}_0$ denote the set of all non-negative integers. Let J be a finite set. For two vectors $\mathbf{u} = (u_i)_{i\in J}$, $\mathbf{v} = (v_i)_{i\in J} \in \mathbb{N}_0^J$ we write $\mathbf{u} \leq \mathbf{v}$ if $u_i \leq v_i$ for all $i \in J$. Moreover, $\mathbf{u} < \mathbf{v}$ denotes $\mathbf{u} \leq \mathbf{v}$ and $\mathbf{u} \neq \mathbf{v}$. Given a vector $\mathbf{v} = (v_i)_{i\in J}$, we define $\operatorname{supp}(\mathbf{v}) = \{i \in J \ : \ v_i \neq 0\}$ and the modulus $|\mathbf{v}| = \sum_{i\in J} v_i$. Furthermore, we denote $\mathbf{v}_X = (v'_i)_{i\in J}$, where $X \subseteq J$ and

$$v'_i = \begin{cases} v_i & \text{if } i \in X, \\ 0 & \text{if } i \notin X. \end{cases}$$

Let us observe that $|\mathbf{v}| = |\mathbf{v}_X|$ is equivalent to $\operatorname{supp}(\mathbf{v}) \subseteq X$. For every $k \in J$, we define the vector $\mathbf{e}^{(k)} \in \mathbb{N}_0^J$ such that $\mathbf{e}^{(k)} = (e_i^{(k)})_{i\in J}$ with $e_k^{(k)} = 1$ and $e_i^{(k)} = 0$ for all $i \neq k$.

2.1. **Multipartite access structures.** Let Γ be an access structure on a set of participants P. A participant $q \in P$ is said to be *hierarchically superior* to a participant $p \in P$ (written $p \preceq q$), if $A \cup \{q\} \in \Gamma$ for all subsets $A \subseteq P \setminus \{q, p\}$ with $A \cup \{p\} \in \Gamma$. If $q \preceq p$ and $p \preceq q$, then the participants q, p are called *hierarchically equivalent*. The relation $\preceq$ is reflexive and transitive but not antisymmetric in general, so it is a preorder in P. Participants $p, q \in P$ are said to be *hierarchically independent* if q is not hierarchically superior to p nor p is hierarchically superior to q.

By a *partition* (Π-*partition*) of a set of participants P we mean a family $\Pi = (P_i)_{i\in J}$ of disjoint and nonempty subsets (*blocks*) of P such that $P = \bigcup_{i\in J} P_i$. An access structure Γ on P is said to be *multipartite* (Π-*partite*) if all participants in every subset P_i are pairwise hierarchically equivalent. Thus we are allowed to define a hierarchy in Π. Namely, P_j is said to be *hierarchically superior* to P_i (written $P_i \preceq P_j$) if there are $p \in P_i$ and $q \in P_j$ such that $p \preceq q$. By transitivity we have $p \preceq q$ for all $p \in P_i$ and $q \in P_j$ whenever $P_i \preceq P_j$. Similarly, blocks P_i and P_j are said to be *hierarchically independent* if there are $p \in P_i$ and $q \in P_j$ such that p and q are hierarchically independent. Moreover, if $P_i \preceq P_j$ and $P_j \preceq P_i$, then the blocks P_i, P_j are called *hierarchically equivalent*. A Π-partite access structure is said to be *compartmented* if every pair of blocks in Π is either hierarchically equivalent or independent. Otherwise the access structure is referred to as *hierarchical*. If no pair of blocks in Π is hierarchically independent, then the access structure will be called *totally hierarchical*. A complete characterization of ideal totally hierarchical access structure was presented by Farràs and Padró [7]. It is worth pointing out that the phrase 'compartmented access structure' used here is very general and covers several notions with the same name appearing in the literature. Let us recall that an access structure is said to be *connected* if every participant in P is a member of a minimal authorized set. If an access structure is not connected, then every participant which does not belong to any minimal authorized set is called *redundant* because its share is never necessary to recover the secret. Therefore all access structures considered here are assumed to be connected, unless stated otherwise.

Given a partition $\Pi = (P_i)_{i\in J}$ of P and $A \subseteq P$ we define the vector $\pi(A) = (v_i)_{i\in J}$, where $v_i = |A \cap P_i|$. All participants in every subset P_i are hierarchically equivalent to each other, so if $A \in \Gamma$, $B \subseteq P$ and $\pi(A) = \pi(B)$, then $B \in \Gamma$. We put $\pi(\Gamma) = \{\pi(A) \in \mathbb{N}_0^J \ : \ A \in \Gamma\}$ and

$$\Omega(\Pi) = \{\pi(A) \in \mathbb{N}_0^J \ : \ A \subseteq P\} = \{\mathbf{v} \in \mathbb{N}_0^J \ : \ \mathbf{v} \leq \pi(P)\}.$$

Obviously, if $A \subseteq B \subseteq P$, then $\pi(A) \leq \pi(B)$. Moreover, if $\mathbf{u} \in \pi(\Gamma)$ and $\mathbf{u} \leq \mathbf{v} \leq \pi(P)$, then $\mathbf{v} \in \pi(\Gamma)$. Indeed, there is $A \in \Gamma$ such that $\mathbf{u} = \pi(A)$. The set A can be extended to a set $B \subseteq P$ such that $\mathbf{v} = \pi(B)$. Hence $B \in \Gamma$ and consequently $\mathbf{v} \in \pi(\Gamma)$. This shows that $\pi(\Gamma) \subseteq \Omega(\Pi)$ is a set of vectors that is monotonic with respect to $\leq$. On the other hand, every monotonic set $\Gamma' \subseteq \Omega(\Pi)$ determines the Π-partite access structure $\Gamma = \{A \subseteq P \ : \ \pi(A) \in \Gamma'\}$. This shows that there is a one-to-one correspondence between

the family of Π-partite access structures defined on P and the family of monotonic subsets of $\Omega(\Pi)$. Therefore we use the same notation Γ for both the access structure and its vector representation.

The hierarchy among blocks in Π can be characterized in vector terms as follows: $P_i \preceq P_j$ if and only if

$$\mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)} \in \Gamma \text{ for all } \mathbf{v} \in \Gamma \text{ with } v_i \geq 1 \text{ and } v_j < |P_j|. \tag{1}$$

2.2. **Polymatroids and access structures.** Let J be a nonempty finite set and let $\mathcal{P}(J)$ denote the power set of J. *A polymatroid* $\mathcal{Z}$ is a pair (J, h), where h is a mapping $h : \mathcal{P}(J) \longrightarrow \mathbb{R}$ satisfying

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

The mapping h is called *the rank function* of a polymatroid. If all values of the rank function are integer, then the polymatroid is called *integer*. An integer polymatroid (J, h) such that $h(X) \leq |X|$ for all $X \subseteq J$ is called a *matroid*. All polymatroids considered in this paper are assumed to be integer. For simplicity of notation we write $h(i)$ instead of $h(\{i\})$ for $i \in J$.

Let $\mathcal{Z} = (J, h)$ be a polymatroid and let $i \in J$ such that $h(i) = 1$. The set $\{X \in \mathcal{P}(J \setminus \{i\}) \ : \ h(X \cup \{i\}) = h(X)\}$ is called a *polymatroid port* or more precisely, the *port of* $\mathcal{Z}$ *at* i. One can show that every polymatroid port is a monotonic family of subsets of $J \setminus \{i\}$, which does not contain $\emptyset$.

The following examples of polymatroids play a special role in studying ideal access structures. Let V be a vector space of finite dimension and let $\mathfrak{V} = (V_i)_{i \in J}$ be a family of subspaces of V. One can show that the mapping $h : \mathcal{P}(J) \longrightarrow \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ for $X \in \mathcal{P}(J)$ is the rank function of the polymatroid $\mathcal{Z} = (J, h)$. The polymatroids that can be defined in this way are said to be *representable*. If $\dim V_i \leq 1$ for all $i \in J$, then we obtain a matroid which is called *representable* as well. The family $\mathfrak{V}$ is referred to as a *vector space representation* of the polymatroid (matroid).

Let $\mathfrak{B} = (B_i)_{i \in J}$ be a family of finite sets. One can show that the mapping $h : \mathcal{P}(J) \longrightarrow \mathbb{Z}$ defined by $h(X) = |\bigcup_{i \in X} B_i|$ for $X \in \mathcal{P}(J)$ is the rank function of the integer polymatroid $\mathcal{Z} = (J, h)$. Every polymatroid that can be defined in this way is said to be *Boolean* and the family $\mathfrak{B}$ is called a *Boolean representation* of the polymatroid. Let $\mathbb{F}$ be an arbitrary field. Let us consider an $\mathbb{F}$-vector space $V = \mathbb{F}^B$, where $B = \bigcup_{i \in J} B_i$ and the elements of B are identified with the vectors of the canonical basis of V. The collection of subspaces $V_i = \operatorname{span}(B_i) \subseteq V$ is a vector space representation of $\mathcal{Z}$ as we have $h(X) = |\bigcup_{i \in X} B_i| = \dim(\sum_{i \in X} V_i)$. This shows that every Boolean polymatroid is representable.

The connection between matroids and ideal access structures was discovered by Brickell and Davenport [4]. They proved that if $\Gamma \subseteq \mathcal{P}(P)$ is the access structure of an ideal secret sharing scheme on a set of participants P with a dealer $p_0 \notin P$, then there is a matroid $\mathcal{S}$ with the ground set $P \cup \{p_0\}$ such that Γ is the port of $\mathcal{S}$ at the point p_0.This result can be stated as follows.

Theorem 1 (E.F. Brickell, D.M. Davenport [4])**.** *Every ideal access structure is a matroid port.*

The converse is not true. For example, the ports of the Vamos matroid are not ideal access structures (cf. [12]). The following result is obtained as a consequence of the linear construction of ideal secret-sharing schemes due to Brickell [3].

Theorem 2 (E.F. Brickell [3]). *Every port of a representable matroid is an ideal access structure.*

Let $\mathcal{Z} = (J, h)$ be a polymatroid. Let us denote $J' = J \cup \{j_0\}$ with a certain $j_0 \notin J$ and let $\Delta \subseteq \mathcal{P}(J) \setminus \{\emptyset\}$ be a monotonic family of subsets of J. Let us define the function $h' : \mathcal{P}(J') \longrightarrow \mathbb{N}_0$ by $h'(X) = h(X)$ for all $X \in \mathcal{P}(J)$ and

$$h'(X \cup \{j_0\}) = \begin{cases} h(X) & \text{if } X \in \Delta, \\ h(X) + 1 & \text{if } X \in \mathcal{P}(J) \setminus \Delta. \end{cases}$$

If h' is monotonic and submodular, then Δ is said to be *compatible* with $\mathcal{Z}$ and $\mathcal{Z}' = (J', h')$ is a polymatroid which is called the *simple extension of $\mathcal{Z}$ induced by Δ*. It is easy to see that $h'(j_0) = 1$ and Δ is the polymatroid port of $\mathcal{Z}'$ at the point j_0.

The next result, which is a consequence of [5, Proposition 2.3] is very useful in the investigation of access structures induced by polymatroids.

Lemma 3 (L. Csirmaz [5]). *A monotonic family Δ on J with $\emptyset \notin \Delta$ is compatible with an integer polymatroid $\mathcal{Z} = (J, h)$ if and only if the following conditions are satisfied.*

1. *If $X \subseteq Y \subseteq J$ and $X \notin \Delta$ while $Y \in \Delta$, then $h(X) < h(Y)$.*
2. *If $X, Y \in \Delta$ and $X \cap Y \notin \Delta$, then $h(X \cup Y) + h(X \cap Y) < h(X) + h(Y)$.*

Now, we want to recall an important characterization of multipartite access structures which are matroid ports. This result was discovered by Farràs, Martí-Farré and Padró [6].

Let $\mathcal{Z} = (J, h)$ be a polymatroid and let $X \subseteq J$. We define the following set

$$\mathcal{B}(\mathcal{Z}, X) = \{\mathbf{v} \in \mathbb{N}_0^J \ : \ \operatorname{supp}(\mathbf{v}) \subseteq X,\ |\mathbf{v}| = h(X),\ \forall_{Y \subseteq X} |\mathbf{v}_Y| \leq h(Y)\}.$$

For $\Delta \subseteq \mathcal{P}(J)$ we define $\mathcal{B}(\mathcal{Z}, \Delta) = \bigcup_{X \in \Delta} \mathcal{B}(\mathcal{Z}, X)$.

Theorem 4 ([6] Theorem 5.3). *Let $\Pi = (P_i)_{i \in J}$ be a partition of a set P and let Γ be a Π-partite access structure on P. Then Γ is a matroid port if and only if there exists a polymatroid $\mathcal{Z} = (J, h)$ such that $h(i) \leq |P_i|$ for all $i \in J$, $\Delta = \operatorname{supp}(\Gamma)$ is compatible with $\mathcal{Z}$ and $\min \Gamma = \min \mathcal{B}(\mathcal{Z}, \Delta)$.*

The following theorem generalizes the result of Brickell [3].

Theorem 5 ([6] Theorem 6.1). *Let $\Pi = (P_i)_{i \in J}$ be a partition of a set P. Let $\Delta \subseteq \mathcal{P}(J)$ be a monotonic family compatible with a polymatroid $\mathcal{Z} = (J, h)$ such that $h(i) \leq |P_i|$ for all $i \in J$. If the simple extension of $\mathcal{Z}$ determined by Δ is a representable polymatroid, then the multipartite access structure Γ such that $\min \Gamma = \min \mathcal{B}(\mathcal{Z}, \Delta)$ is ideal.*

Remark 6. Theorem 4 can be used as a simple tool for constructing multipartite access structures which are matroids ports. Given a partition $\Pi = (P_i)_{i \in J}$ it is enough to take a polymatroid $\mathcal{Z} = (J, h)$ with $h(i) \leq |P_i|$ for every $i \in J$ and a monotonic family $\Delta \subseteq \mathcal{P}(J)$ which is compatible with $\mathcal{Z}$ and construct the smallest monotonic family $\Gamma \subseteq \Omega(\Pi)$ which contains $\min \mathcal{B}(\mathcal{Z}, \Delta)$. According to Theorem 4 the access structure obtained in this way satisfies necessary condition to be ideal. Such Γ will be denoted by $\Gamma(\Pi, \mathcal{Z}, \Delta)$. Moreover, Theorem 5 provides a sufficient condition for $\Gamma(\Pi, \mathcal{Z}, \Delta)$ to be ideal. If $h(i) = 0$, then all participants in P_i are redundant, so every access structure induced by $\mathcal{Z}$ is not connected. Therefore, from now on we assume that $h(i) > 0$ for all $i \in J$.

2.3. **Extreme polymatroids.** Let (J, h) be a polymatroid. It is easy to see that the rank function satisfies the following condition

$$\max\{h(i) \ : \ i \in X\} \leq h(X) \leq \sum_{i \in X} h(i)$$

for every nonempty subset $X \subseteq J$.

For a given rank function $h : \mathcal{P}(J) \longrightarrow \mathbb{Z}$ one can define two functions $h_*(X) = \max\{h(i) : i \in X\}$ and $h^*(X) = \sum_{i\in X} h(i)$ for every nonempty subset $X \subseteq J$. Moreover, it is assumed $h_*(\emptyset) = h^*(\emptyset) = 0$. It is easy to prove that (J, h_*) and (J, h^*) are integer polymatroids and

$$h_*(X) \leq h(X) \leq h^*(X)$$

for every $X \in \mathcal{P}(J)$. This means that the functions h_*, h^* are minimal and maximal, respectively, among all monotonic and submodular functions defined on $\mathcal{P}(J)$ with given values on singletons.

We say that (J, h) is a *polymatroid with maximal* (respectively *minimal*) *rank function* if $h = h^*$ (respectively $h = h_*$). Such polymatroids are referred to as *extreme*.

Remark 7. 1. Let $\mathcal{Z} = (J, h)$ be a polymatroid with maximal rank function, i.e., $h(X) = \sum_{i\in X} h(i)$ for all $X \in \mathcal{P}(J) \setminus \{\emptyset\}$. Let $(B_i)_{i\in J}$ be a collection of mutually disjoint sets such that $|B_i| = h(i)$ for all $i \in J$. It easy to see that this collection is a Boolean representation of $\mathcal{Z}$.

2. Let $J = \{1, \ldots, m\}$ and let $\mathcal{Z} = (J, h)$ be a polymatroid with minimal rank function, i.e., $h(X) = \max\{h(i) : i \in X\}$ for all $X \in \mathcal{P}(J) \setminus \{\emptyset\}$. Assume $h(1) \leq \ldots \leq h(m)$. It is easy to see that a chain $B_1 \subseteq \ldots \subseteq B_m$ of finite sets such that $|B_i| = h(i)$ for all $i \in J$ is a Boolean representation of $\mathcal{Z}$. This shows that extreme polymatroids are Boolean.

3. Access structures induced by polymatroids with maximal rank function

Throughout this section we assume that (J, h) is a polymatroid with maximal rank function, i.e., $h(X) = \sum_{i\in X} h(i)$ for every non-empty $X \subseteq J$ and $h(i) > 0$ for all $i \in J$. It is easily seen that

$$h(X) < h(Y) \quad \text{for all } X \subsetneq Y \subseteq J, \tag{2}$$

$$h(X \cup Y) + h(X \cap Y) = h(X) + h(Y) \quad \text{for all } X, Y \subseteq J. \tag{3}$$

The following lemma characterizes monotonic families in $\mathcal{P}(J)$ which are compatible with polymatroids with maximal rank functions.

Lemma 8. *A monotonic family $\Delta \subseteq \mathcal{P}(J) \setminus \{\emptyset\}$ is compatible with a polymatroid with maximal rank function if and only if Δ contains exactly one minimal set.*

Proof. Observe that the inequality (2) immediately implies the statement (1) of Csirmaz Lemma. Assume that Δ is compatible with $\mathcal{Z} = (J, h)$ and suppose $X, Y \subseteq J$ are different minimal sets in Δ. Then $X \cap Y \notin \Delta$, so by Csirmaz Lemma 3 we get

$$h(X \cup Y) + h(X \cap Y) < h(X) + h(Y)$$

which contradicts (3).

Conversely, assume that U is the only minimal set in Δ, so $U \subseteq X \cap Y$ for all $X, Y \in \Delta$ thus $X \cap Y \in \Delta$ which implies (2) of Csirmaz Lemma and consequently shows that Δ is compatible with $\mathcal{Z}$. □

The following theorem presents properties of access structures induced by polymatroids with maximal rank function.

Theorem 9. *Let $\Pi = (P_i)_{i\in J}$ be a partition of a set of participants P. Let $\mathcal{Z} = (J, h)$ be a polymatroid with maximal rank function such that $h(i) \leq |P_i|$ for all $i \in J$ and let $\Delta \subseteq \mathcal{P}(J)$ be a monotonic family which is compatible with $\mathcal{Z}$. Then there is a vector $\mathbf{u} \in \mathbb{N}_0^J$ such that $\Gamma(\Pi, \mathcal{Z}, \Delta) = \{\mathbf{v} \in \Omega(\Pi) : \mathbf{v} \geq \mathbf{u}\}$. The access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ is connected if and*

only if $\Delta = \{J\}$. *If* $\Delta = \{J\}$ *and* $h(i) < |P_i|$ *for all* $i \in J$, *then* $\Gamma(\Pi, \mathcal{Z}, \Delta)$ *is an ideal and compartmented access structure.*

Proof. Let us denote $\mathbf{w} = \sum_{i\in J} h(i)\mathbf{e}^{(i)}$. By definition, $\mathbf{v} = (v_i)_{i\in J} \in \mathcal{B}(\mathcal{Z}, X)$, $\emptyset \neq X \subseteq J$ if and only if $\operatorname{supp}(\mathbf{v}) \subseteq X$, $\sum_{i\in X} v_i = |\mathbf{v}| = h(X) = \sum_{i\in X} h(i)$ and $v_i \leq h(i)$. Hence $v_i = h(i)$ for $i \in X$ and $v_i = 0$ for $i \in J \setminus X$, i. e., $\mathbf{v} = \mathbf{w}_X$. This shows that $\mathcal{B}(\mathcal{Z}, X) = \{\mathbf{w}_X\}$ for every $X \in \mathcal{P}(J) \setminus \{\emptyset\}$. If $\mathbf{v} \in \mathcal{B}(\mathcal{Z}, X)$, $\mathbf{u} \in \mathcal{B}(\mathcal{Z}, Y)$ with $X \subseteq Y \subseteq J$, then we have $\mathbf{v} = \mathbf{w}_X \leq \mathbf{w}_Y = \mathbf{u}$. To shorten notation, we write Γ instead of $\Gamma(\Pi, \mathcal{Z}, \Delta)$. According to Remark 6 we have $\min\Gamma = \min\bigcup_{X\in\Delta} \mathcal{B}(\mathcal{Z}, X)$. Let U be the only minimal set in Δ. Thus $\min\Gamma = \min\bigcup_{X\in\Delta} \mathcal{B}(\mathcal{Z}, X) = \min\mathcal{B}(\mathcal{Z}, U) = \{\mathbf{w}_U\}$. This implies that $\mathbf{v} \in \Gamma$ if and only if $\mathbf{v} \geq \mathbf{w}_U$. If $U \neq J$, then the participants in P_i are redundant for every $i \in J \setminus U$, thus the access structure Γ is not connected. Otherwise, i.e., $\Delta = \{J\}$, the access structure Γ is connected, as every component of the minimal authorized vector $\mathbf{w}$ is different from 0.

It is easily seen that $\mathbf{w} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)}, \mathbf{w} - \mathbf{e}^{(j)} + \mathbf{e}^{(i)} \notin \Gamma$, so the blocks P_i and P_j are hierarchically independent. Thus Γ is a compartmented access structure.

Let $(B_i)_{i\in J}$ be a Boolean representation of the polymatroid $\mathcal{Z}$ and let $B = \bigcup_{i\in J} B_i$. Given a finite field $\mathbb{F}$, we consider the vector space $V = \mathbb{F}^B$. Assuming that the canonical basis of V is identified with B we can define the subspace $V_i = \operatorname{span}(B_i)$ for every $i \in J$. Moreover, we define the vector $\alpha = \sum_{\beta\in B} \beta$ and the subspace $V_{j_0} = \operatorname{span}(\{\alpha\}) \subseteq V$ for a certain $j_0 \notin J$. Then the collection $(V_i)_{i\in J}$ together with V_{j_0} form a vector space representation of the simple extension $\mathcal{Z}' = (J', h')$ of $\mathcal{Z}$ with $J' = J \cup \{j_0\}$ induced by $\Delta = \{J\}$. Indeed, it is easily seen that $\alpha \notin \sum_{i\in X} V_i$, so $h'(X \cup \{j_0\}) = h(X) + 1$ for all $X \subsetneq J$ and $h'(J \cup \{j_0\}) = h(J)$. This combined with Theorem 5 proves that Γ is an ideal access structure. □

It turns out that $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ presented above is a special case of a compartmented access structure considered first by Brickell [3] as an access structure with lower bound. Tassa and Dyn [16, Section 3] presented a construction of an ideal secret sharing scheme for that Γ based on bivariate polynomial interpolation.

4. Access structures induced by polymatroids with minimal rank function

The main goal of this section is to describe all access structures induced by polymatroids with minimal rank function and investigate their hierarchical order.

Throughout this section we will use the notation $J_n = \{1, \ldots, n\}$ for every $n \in \mathbb{N}$. From now on, we assume that $J = J_m$ and $\mathcal{Z} = (J_m, h)$ is a polymatroid with minimal rank function. Without loss of generality we may assume that $0 < h(1) \leq h(2) \leq \ldots \leq h(m)$. This assumption implies

$$h(X) = \max\{h(i) \ : \ i \in X\} = h(\max X)$$

for every non-empty subset X of J_m.

We begin with a characterization of monotonic families in $\mathcal{P}(J_m)$ which are compatible with polymatroids with minimal rank function.

Lemma 10. *A monotonic family* $\Delta \subseteq \mathcal{P}(J_m) \setminus \{\emptyset\}$ *is compatible with a polymatroid with minimal rank function if and only if the following conditions are satisfied.*

1. *Every minimal set in* Δ *is a singleton;*
2. *Let* $l = \min\{i \in J_m \ : \ \{i\} \in \Delta\}$. *Then* $\min\Delta = \{\{l\}, \ldots, \{m\}\}$ *and* $h(l-1) < h(l)$ *unless* $l = 1$.

Proof. Let us assume that Δ is compatible with a polymatroid (J_m, h) with minimal rank function.

1. Given $X \in \min \Delta$ and $|X| \geq 2$. Let $i = \max X$. Hence $h(X) = h(i)$ and $\{i\} \notin \Delta$ as X is minimal. By Csirmaz Lemma $h(i) < h(X)$, which is a contradiction.

2. It is enough to prove that $\{i\} \in \Delta$ for every $i > l$. Let us assume $i > l$. Then $X = \{l, i\} \in \Delta$ as $\{l\} \in \Delta$ and Δ is a monotonic family. Moreover, $h(X) = h(i)$. This and Csirmaz Lemma imply $\{i\} \in \Delta$. If $l > 1$, then $X = \{l-1, l\} \in \Delta$, but $\{l-1\} \notin \Delta$. By Csirmaz Lemma we have $h(l-1) < h(X) = h(l)$.

Conversely, we assume (1) and (2). Given $\emptyset \neq X \subseteq Y \subseteq J_m$ such that $X \notin \Delta$ and $Y \in \Delta$. Thus $1 \leq \max X < l \leq \max Y$ hence $h(X) = h(\max X) \leq h(l-1) < h(l) \leq h(\max Y) = h(Y)$. Let $X, Y \in \Delta$ such that $X \cap Y \notin \Delta$. Let $i = \max X$, $j = \max Y$. If $X \cap Y = \emptyset$, then

$$h(X \cup Y) + h(X \cap Y) = h(\max\{i, j\}) < h(i) + h(j) = h(X) + h(Y).$$

Otherwise, $k = \max X \cap Y < l \leq i, j$ and $i \neq j$ since $X \cap Y \notin \Delta$. Without loss of generality we may assume $i > j$. Thus we have

$$h(X \cup Y) + h(X \cap Y) = h(i) + h(k) < h(i) + h(j) = h(X) + h(Y).$$

Applying Csirmaz Lemma yields the claim. □

From now on we assume that $\Pi = \{P_1, \ldots, P_m\}$ is a partition of a set of participants P and $\Delta \subseteq \mathcal{P}(J_m)$ is a monotonic family compatible with a polymatroid $\mathcal{Z} = \{J_m, h\}$. Moreover, we will use the notation $l(\Delta) = \min\{i \in J_m \ : \ \{i\} \in \Delta\}$. The following lemma simplifies the description of the multipartite access structure $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$.

Lemma 11. *If $X \subseteq Y$ and $h(X) = h(Y)$, then $\mathcal{B}(\mathcal{Z}, X) \subseteq \mathcal{B}(\mathcal{Z}, Y)$. Moreover,*

$$\min \Gamma(\Pi, \mathcal{Z}, \Delta) = \min \bigcup_{k=l(\Delta)}^{m} \mathcal{B}(\mathcal{Z}, J_k).$$

Proof. If $\mathbf{w} \in \mathcal{B}(\mathcal{Z}, X)$, then $\operatorname{supp}(\mathbf{w}) \subseteq X \subseteq Y$ and $|\mathbf{w}_Y| = |\mathbf{w}_X| = h(X) = h(Y)$. Moreover, for every $U \subseteq Y$ we have $|\mathbf{w}_U| = |\mathbf{w}_{U \cap X}| \leq h(U \cap X) \leq h(U)$. This shows $\mathbf{w} \in \mathcal{B}(\mathcal{Z}, Y)$.

It is sufficient to prove that

$$\bigcup_{X \in \Delta} \mathcal{B}(\mathcal{Z}, X) = \bigcup_{k=l(\Delta)}^{m} \mathcal{B}(\mathcal{Z}, J_k).$$

Let $\mathbf{w} \in \bigcup_{X \in \Delta} \mathcal{B}(\mathcal{Z}, X)$. Then there is $X \in \Delta$ such that $\mathbf{w} \in \mathcal{B}(\mathcal{Z}, X)$. For $k = \max X$ we have $k \geq l(\Delta)$. Then $X \subseteq J_k$ and $h(X) = h(k) = h(J_k)$, so we have $\mathbf{w} \in \mathcal{B}(\mathcal{Z}, X) \subseteq \mathcal{B}(\mathcal{Z}, J_k)$ which shows $\bigcup_{X \in \Delta} \mathcal{B}(\mathcal{Z}, X) \subseteq \bigcup_{k=l}^{m} \mathcal{B}(\mathcal{Z}, J_k)$.The converse inclusion is obvious. □

Now we are in a position to state the main results concerning the access structures induced by polymatroids with minimal rank function. Let us recall that we have defined $|\mathbf{v}_X| = \sum_{s \in X} v_s$. In particular, $|\mathbf{v}_{[g,k]}| = \sum_{s=g}^{k} v_s$ for the interval $X = [g, k] = [g, g+1, \ldots, k]$. For simplicity of notation we assume $h(0) = 0$, $J_0 = \emptyset$ and $|\mathbf{v}_{J_0}| = 0$ for every $\mathbf{v} \in \mathbb{N}_0^m$.

Theorem 12. *Let $\Pi = (P_i)_{i \in J_m}$ be a partition of P. Let $\mathcal{Z} = (J_m, h)$ be a polymatroid with minimal rank function such that $0 < h(1) \leq \ldots \leq h(m)$ and $h(i) \leq |P_i|$ for $i \in J_m$. If $\Delta \subset \mathcal{P}(J_m) \setminus \{\emptyset\}$ is a monotonic family compatible with $\mathcal{Z}$, then the access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ is connected and ideal. Moreover, $\mathbf{v} = (v_i)_{i \in J} \in \Gamma(\Pi, \mathcal{Z}, \Delta)$ if and only if $\mathbf{v} \in \Omega(\Pi)$ and there is $k \in J_m$, $k \geq l(\Delta)$ such that*

$$|\mathbf{v}_{[g,k]}| \geq h(k) - h(g-1) \text{ for all } 1 \leq g \leq l(\Delta). \tag{4}$$

Proof. At first, we shall prove that $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ is connected. Let $l = l(\Delta)$. If $k \in J_m,\ k \geq l$, then the vector $h(k)\mathbf{e}^{(k)}$ belongs to $\mathcal{B}(\mathcal{Z}, J_k)$ and is minimal in Γ. If $1 \leq k < l$, then $0 < h(k) \leq h(l-1) < h(l)$, so the vector $\mathbf{e}^{(k)} + (h(l)-1)\mathbf{e}^{(l)}$ belongs to $\mathcal{B}(\mathcal{Z}, J_l)$ and is minimal in Γ. This shows that in both cases the participants in P_k are not redundant for every $k \in J_m$.

By assumption, Δ is compatible with $\mathcal{Z}$, so there is a simple extension $\mathcal{Z}' = (J'_m, h')$ of $\mathcal{Z}$ with $J'_m = J_{m+1}$ such that the port of $\mathcal{Z}'$ at $j_0 = m+1$ is equal to Δ.

Let $B_1 \subseteq B_2 \subseteq \ldots \subseteq B_m$ with $|B_k| = h(k)$ for all $k \in J_m$ be a Boolean representation of $\mathcal{Z}$ (cf. Remark 7.2). According to Lemma 10.2 we have $h(l-1) < h(l)$. Thus we can take $b \in B_l \setminus B_{l-1}$ (assuming $B_0 = \emptyset$) and form the set $B_{m+1} = \{b\}$. It is easy to check that the collection $(B_k)_{k \in J_{m+1}}$ is a Boolean representation of $\mathcal{Z}'$. The fact that every Boolean polymatroid is representable combined with Theorem 5 proves that $\Gamma(\Pi, \Delta, \mathcal{Z})$ is ideal.

Let us denote

$$\widehat{\Gamma} = \left\{ \mathbf{v} \in \Omega(\Pi) \ : \ \exists_{k \in J_m \setminus J_{l-1}} \forall_{g \in J_l} \ |\mathbf{v}_{[g,k]}| \geq h(k) - h(g-1) \right\}.$$

We shall show that $\Gamma = \widehat{\Gamma}$. If $\mathbf{v} \in \Gamma$, then there is $\mathbf{w} \in \min \Gamma$ such that $\mathbf{w} \leq \mathbf{v}$. This implies $\mathbf{w} \in \mathcal{B}(\mathcal{Z}, J_k)$ for a suitable $l \leq k \leq m$. By definition, $|\mathbf{w}| = |\mathbf{w}_{J_k}| = h(k)$ and $|\mathbf{w}_{J_{g-1}}| \leq h(g-1)$ for all $1 \leq g \leq k$. Hence

$$|\mathbf{v}_{[g,k]}| = \sum_{s=g}^{k} v_s \geq \sum_{s=g}^{k} w_s = |\mathbf{w}_{J_k}| - |\mathbf{w}_{J_{g-1}}| \geq h(k) - h(g-1)$$

for all $g \in J_l$. This shows that $\mathbf{v} \in \widehat{\Gamma}$.

To prove that $\widehat{\Gamma} \subseteq \Gamma$, let us consider an arbitrary $\mathbf{w} \in \min \widehat{\Gamma}$. Let $k \in J_m$ be the smallest integer such that $k \geq l$ and $|\mathbf{w}_{[g,k]}| \geq h(k) - h(g-1)$ for all $g \in J_l$. We shall show that $\mathbf{w} \in \mathcal{B}(\mathcal{Z}, J_k) \subseteq \Gamma$.

It can be easily seen, that $\mathbf{w}_{J_k} \in \widehat{\Gamma}$ and $\mathbf{w}_{J_k} \leq \mathbf{w}$. Hence we have $\mathbf{w} = \mathbf{w}_{J_k}$ as $\mathbf{w}$ is minimal in $\widehat{\Gamma}$ and in particular $\operatorname{supp}(\mathbf{w}) \subseteq J_k$.

Now, we show that $w_k > 0$. Indeed, if $k = l$, then we have $w_l = |\mathbf{w}_{[l,l]}| \geq h(l) - h(l-1) > 0$ by Lemma 10. Suppose $k > l$ and $w_k = 0$. Thus we have $|\mathbf{w}_{[g,k-1]}| = \sum_{s=g}^{k-1} w_s = \sum_{s=g}^{k} w_s \geq h(k) - h(g-1) \geq h(k-1) - h(g-1)$ for all $g \in J_l$. This implies that $\mathbf{w}$ satisfies (4) with k replaced by $k-1$, contrary to the choice of k.

Let us observe that $|\mathbf{w}| = |\mathbf{w}_{[1,k]}| \geq h(k)$. We claim that $|\mathbf{w}| = h(k)$. On the contrary, suppose that $|\mathbf{w}| > h(k)$. Let $g_0 = \min \operatorname{supp}(\mathbf{w})$ and let $\mathbf{w}' = \mathbf{w} - \mathbf{e}^{(g_0)}$. For $g \leq g_0, l$ we have

$$|\mathbf{w}'_{[g,k]}| = |\mathbf{w}_{[g,k]}| - 1 = |\mathbf{w}_{[1,k]}| - 1 \geq h(k) \geq h(k) - h(g-1).$$

Moreover, $|\mathbf{w}'_{[g,k]}| = |\mathbf{w}_{[g,k]}|$ for $g_0 < g \leq l$. So we get $\mathbf{w}' \in \widehat{\Gamma}$ and $\mathbf{w}' < \mathbf{w}$ which contradicts the minimality of $\mathbf{w}$. This proves that $|\mathbf{w}| = h(k)$.

We proceed to show that $|\mathbf{w}_{J_i}| \leq h(i)$ for all $i < k$. If $i < l$, then we have

$$|\mathbf{w}_{J_i}| = \sum_{s=1}^{i} w_s = |\mathbf{w}| - |\mathbf{w}_{[i+1,k]}| \leq h(k) - (h(k) - h(i)) = h(i).$$

It remains to show the same for $l \leq i \leq k-1$. Let us notice that $\mathbf{w}_{J_i} < \mathbf{w}_{J_k} = \mathbf{w}$ as $w_k > 0$, thus $\mathbf{w}_{J_i} \notin \widehat{\Gamma}$. This implies $|\mathbf{w}_{[g,i]}| < h(i) - h(g-1)$ for a suitable $g \in J_l$. Hence we get

$$|\mathbf{w}_{J_i}| = |\mathbf{w}_{J_{g-1}}| + |\mathbf{w}_{[g,i]}| < h(g-1) + (h(i) - h(g-1)) = h(i).$$

Summarizing, we have proved that $\min\widehat{\Gamma} \subseteq \mathcal{B}(\mathcal{Z},\Delta) \subseteq \Gamma$. To complete the proof it is enough to notice that Γ is a monotonic set, so all supersets of sets in $\min\widehat{\Gamma}$ belong to Γ. $\square$

Now we shall investigate the hierarchical order in Π determined by the access structures $\Gamma(\Pi,\Delta,\mathcal{Z})$. Let us recall that $P_i \preceq P_j$ if and only if

$$\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)} \in \Gamma \text{ for every } \mathbf{v} \in \Gamma \text{ with } v_i > 0, v_j < |P_j|.$$

It is easily seen that

$$|\mathbf{v}'_{[g,k]}| = |\mathbf{v}_{[g,k]}| \text{ for all } g,k \in J_m \text{ with } g \le i,j \le k \text{ or } i,j < g \le k \text{ or } g \le k < i,j. \tag{5}$$

Theorem 13. *Let us assume that $\Pi, \mathcal{Z}, \Delta$ and $l = l(\Delta)$ satisfy the hypotheses of Theorem 12. If $h(i) < |P_i|$ for all $i \in J$, then*

$$P_i \preceq P_j \text{ if and only if } h(i) \le h(j) \le h(l) \text{ or } h(l) \le h(j) \le h(i). \tag{6}$$

for every $i,j \in J_m$. In particular, if h is not a constant function, then the access structure $\Gamma(\Pi,\mathcal{Z},\Delta)$ is hierarchical.

Proof. The proof is divided into several parts. First we shall prove the implication from right to left of the condition (6). It is obvious that the assertion is true for $i = j$, so we assume hereinafter $i \neq j$.

Claim 1. If $\mathbf{v} \in \Gamma$ and k is the maximal integer in J_m such that the condition (4) holds for $\mathbf{v}$, then $h(n) > h(k)$ for all $n \in J_m,\ n > k$. Indeed, if $n > k$, then (4) does not hold for n, i.e., $|\mathbf{v}_{[g,n]}| < h(n) - h(g-1)$ for a certain $g \le l$. Thus we have

$$h(n) - h(g-1) > |\mathbf{v}_{[g,n]}| \ge |\mathbf{v}_{[g,k]}| \ge h(k) - h(g-1),$$

which implies the claim.

Claim 2. If $h(i) \le h(j) \le h(l)$, then $P_i \preceq P_j$. Let us observe that the inequality $h(i) \le h(j)$ is equivalent to $i < j$ or $i \ge j$ with $h(i) = h(j)$. First we assume $i < j$. Given arbitrary vector $\mathbf{v} \in \Gamma$ such that $v_i > 0$ and $v_j < |P_j|$, we have to show that $\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)} \in \Gamma$. Let k be the maximal integer in J_m such that the condition (4) holds for $\mathbf{v}$. By definition $l \le k$. If $j > k$, then by Claim 1 we have $h(k) < h(j) \le h(l) \le h(k)$. This contradiction shows that $j \le k$. Thus for $i < g \le j$ we have $|\mathbf{v}'_{[g,k]}| = |\mathbf{v}_{[g,k]}| + 1 \ge h(k) - h(g-1)$. This combined with condition (5) implies $\mathbf{v}' \in \Gamma$, as required.

Now we need to consider the case $j < i$ and $h(i) = h(j) \le h(l)$. Let us take $\mathbf{v} \in \Gamma$ with $v_i > 0$ and $v_j < |P_j|$ and the maximal $k \in J_m$ such that the condition (4) is satisfied for $\mathbf{v}$. Similarly as above, we have $i \le k$. Let us define $\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)}$. If $j \ge l$, then it suffices to use (5) to obtain $\mathbf{v}' \in \Gamma$. If $j < l$, then it follows from Lemma 10.2 that $h(i) = h(j) < h(l)$, so $i < l$. Let assume $j < g \le i$. Then we have $j \le g-1 < i$ and $h(j) \le h(g-1) \le h(i) = h(j)$, which yields $h(i) = h(g-1)$. Thus we have

$$|\mathbf{v}'_{[g,k]}| = \sum_{s=g}^{i} v'_s + \sum_{s=i+1}^{k} v'_s \ge \sum_{s=i+1}^{k} v_s \ge h(k) - h(i) = h(k) - h(g-1).$$

This and (5) show that $\mathbf{v}' \in \Gamma$, so the claim is proved.

Claim 3. If $h(l) \le h(j) \le h(i)$, then $P_i \preceq P_j$. In this case we have $l \le i,j$ by Lemma 10.2. We first assume $j < i$. Let $\mathbf{v}$ be an arbitrary vector in Γ such that $v_i > 0$ and $v_j < |P_j|$. There is $k \in J_m \setminus J_{l-1}$ such that $|\mathbf{v}_{[g,k]}| \ge h(k) - h(g-1)$ for all $g \in J_l$. For $\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)}$ we have $|\mathbf{v}'_{[g,k]}| = |\mathbf{v}_{[g,k]}| + 1$ if $j \le k < i$. This and condition (5) gives $|\mathbf{v}'_{[g,k]}| \ge |\mathbf{v}_{[g,k]}| \ge h(k) - h(g-1)$ for all $g \in J_l$, which shows that $\mathbf{v}' \in \Gamma$.

Now we consider the case $i < j$ and $h(i) = h(j)$. Let us assume again that $\mathbf{v} \in \Gamma$ and let $k \in J_m \setminus J_{l-1}$ be the maximal integer such that the condition (4) is satisfied for $\mathbf{v}$. If

$k < i$, then applying (5) yields $\mathbf{v}' \in \Gamma$. Assuming $i \leq k < j$ and applying Claim 1 we obtain $h(i) \leq h(k) < h(j) = h(i)$, a contradiction. Thus we have $k \geq j$ and $\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)} \in \Gamma$ by (5), which completes the proof of the claim.

To prove the converse implication of (6) we assume that the right hand side of (6) does not hold. That means that $h(j) < h(i), h(l)$ or $h(i), h(l) < h(j)$.

Claim 4. If $h(j) < h(i), h(l)$, then P_j is not hierarchically superior to P_i. One can notice that the assumption $h(j) < h(i), h(l)$ implies $j < i, l$. Let us consider $\mathbf{v} = h(j)\mathbf{e}^{(j)} + (h(i) - h(j))\mathbf{e}^{(i)} + (h(k_0) - h(i))\mathbf{e}^{(k_0)}$, where $k_0 = \max\{i, l\} \geq l$. It is easy to see, that $\mathbf{v} \in \Gamma$ and $h(i) - h(j) > 0$ and by assumption $h(j) < |P_j|$. We shall show that $\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)} \notin \Gamma$. Indeed, for every $k \in J_m,\ l \leq k < k_0$ we have $\mathbf{v}'_{[j+1,k]} = 0$. Moreover, $\mathbf{v}'_{[j+1,k]} = h(k_0) - h(j) - 1 < h(k) - h(j)$ for all $k \geq k_0$. Thus the condition (4) is not satisfied for all $k \geq l$.

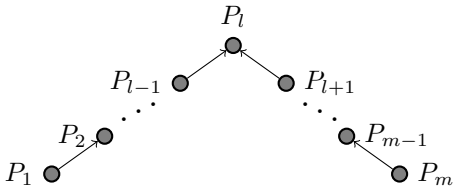
Claim 5. If $h(i), h(l) < h(j)$, then P_j is not hierarchically superior to P_i. One can notice that the assumption $h(i), h(l) < h(j)$ implies $i, l < j$. Let us consider $\mathbf{v} = h(i)\mathbf{e}^{(i)} + (h(k_0) - h(i))\mathbf{e}^{(k_0)}$, where $k_0 = \max\{i, l\}$. It is easy to see that $\mathbf{v} \in \Gamma$. It can be easily checked that for $\mathbf{v}' = \mathbf{v} - \mathbf{e}^{(i)} + \mathbf{e}^{(j)}$ we have

$$\mathbf{v}'_{[1,k]} = \begin{cases} 0 & \text{if } l \leq k < i, \\ h(k_0) - 1 & \text{if } i \leq k < j, . \\ h(k_0) & \text{if } j < k. \end{cases}$$

Thus $|\mathbf{v}'_{[1,k]}| < h(k) - h(0)$ for every $l \leq k \leq m$, so $\mathbf{v}' \notin \Gamma$ by the condition (4).

To show that Γ is hierarchical, it only remains to notice that there is $i \in J_m$ such that $h(i) < h(i+1)$ since the rank function h is not constant. Thus the blocks P_i and P_{i+1} are not hierarchically equivalent nor independent. This completes the proof. □

According to Theorem 13 the blocks $P_1, \ldots, P_l$ form an increasing chain and the blocks $P_l, \ldots, P_m$ form a decreasing chain. The blocks P_i and P_j are hierarchically equivalent if and only if $h(i) = h(j)$. For $h(i) < h(l) < h(j)$ the blocks P_i and P_j are hierarchically independent. If h restricted to J_m is an injective function the Hasse diagram of the hierarchical order determined by the access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ has the following form.



One can observe that the access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ becomes totally hierarchical for $l(\Delta) = 1$ and $l(\Delta) = m$. We shall investigate these two extreme cases in detail. A similar description of these cases can be found in [7, Exercises 4.2 and 4.3].

Remark 14. Let $0 = t_0 < t_1 < \ldots < t_m$ be a sequence of integers such that $t_i < |P_i|$ for $i \in J_m$. The access structure defined by

$$\Gamma_\exists = \{\mathbf{v} \in \pi(P) \ : \ \sum_{i=1}^{k} v_i \geq t_k \text{ for some } k \in J_m\}$$

is called *disjunctive*. This type of access structures was introduced by G. J. Simmons [14]. It turns out that $\Gamma_\exists$ is induced by the polymatroid (J_m, h) with minimal rank function h such that $h(i) = t_i$ and the monotonic family Δ with $l(\Delta) = 1$, i.e, $\Delta = \mathcal{P}(P) \setminus \{\emptyset\}$. Indeed, it is easily seen, that $\mathbf{v} \in \Gamma_\exists$ if and only if $\mathbf{v}$ fulfills the condition (4) with $l(\Delta) = 1$.

Remark 15. T. Tassa [15] introduced another class of hierarchical access structure, which was called *conjunctive*. Let $0 = t_{m+1} < t_m < t_{m-1} < \ldots < t_1$ be a sequence of integers such that $t_i < |P_i|$. The access structure is defined by

$$\Gamma_\forall = \{\mathbf{v} \in \pi(P) \ : \ \sum_{s=g}^{m} v_s \geq t_g \text{ for every } g \in J_m\}.$$

This access structure is determined by the polymatroid (J_m, h) with minimal rank function h such that $h(i) = t_1 - t_{i+1}$ and the monotonic family $\Delta \subseteq \mathcal{P}(J_m)$ with $l(\Delta) = m$. Indeed, it is easily seen, that $\mathbf{v} \in \Gamma$ if and only if $\sum_{s=g}^{m} v_s \geq h(m) - h(g-1) = (t_1 - t_{m+1}) - (t_1 - t_g) = t_g$ for all $g \leq m$ and this is equivalent to $\mathbf{v} \in \Gamma_\forall$. In general settings introduced here the conjunctive access structures have the hierarchical order reversed to that defined in [15].

Two classes of ideal partially hierarchical access structures other than the one described in this chapter are presented in [8]. In the first class, every structure contains one block hierarchically superior to all other blocks, that are mutually independent. The second class consists of compartmented access structures with hierarchical compartments.

References

[1] Benaloh, J.C., Leichter, J.: Generalized secret sharing and monotone functions. Advances in Cryptology - CRYPTO88, 27-36 (1990)

[2] Blakley, G.R.: Safeguarding Cryptographic Keys. The National Computer Conference 1979, AFIPS 48, 313-317 (1979)

[3] Brickell, E. F.: Some ideal secret sharing schemes. J. Combin. Math. Combin. Comput. 6, 105-113 (1989)

[4] Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. Cryptology 4, 123-134 (1991)

[5] Csirmaz, L.: The size of a share must be large. J. Cryptology 10, 223-231 (1997)

[6] Farràs, O., Martí-Farré, J., Padró, C.: Ideal Multipartite Secret Sharing Schemes. J. Cryptology 25, 434-463 (2012)

[7] Farràs, O., Padró, C.: Ideal hierarchical secret sharing schemes. IEEE Trans.Inf. Theory 58, 3273 - 3286 (2012)

[8] Farràs, M., Padró, C., Xing, C., Yang, A.: Natural Generalizations of Threshold Secret Sharing. IEEE Trans. Inform. Theory 60, 1652 - 1664, (2014)

[9] Ito, M., Saito, A., Nishizeki, T.: Secret sharing schemes realizing general access structure. Proc. of the IEEE Global Telecommunication Conf., Globecom 87, 99 - 102 (1987)

[10] Kawa R., Kula M.: Access Structures Determined by Uniform Polymatroids. J. Math. Cryptology, preprint arXiv:2005.04509v2.

[11] Padró C. Lecture Notes in Secret Sharing. *IACR Cryptol. ePrint Arch.* (2012); 2012:674.

[12] Seymour, P.D.: On secret-sharing matroids. J. Combin. Theory Ser. B, 56, 69-73 (1992)

[13] Shamir, A.: How to share a secret. Commun. of the ACM 22, 612 -613 (1979)

[14] Simmons, G.J.: How to (really) share a secret. Advances in Cryptology - CRYPTO 88, Lecture Notes in Comput. Sci. 403, 390-448 (1990)

[15] Tassa, T.: Hierarchical threshold secret sharing. J. Cryptology 20, 237-264 (2007)

[16] Tassa, T., Dyn, N.: Multipartite secret sharing by bivariate interpolation. J. Cryptology 22, 227-258 (2009)