Research Article

Renata Kawa* and Mieczysław Kula

Access structures determined by uniform polymatroids

https://doi.org/10.1515/jmc-2022-0017
received April 28, 2022; accepted May 08, 2023

Abstract: In this article, all multipartite access structures obtained from uniform integer polymatroids were investigated using the method developed by Farràs, Martí-Farré, and Padró. They are matroid ports, i.e., they satisfy the necessary condition to be ideal. Moreover, each uniform integer polymatroid defines some ideal access structures. Some objects in this family can be useful for the applications of secret sharing. The method presented in this article is universal and can be continued with other classes of polymatroids in further similar studies. Here, we are especially interested in hierarchy of participants determined by the access structure, and we distinguish two main classes: they are compartmented and hierarchical access structures. The main results obtained for access structures determined by uniform integer polymatroids and a monotone increasing family Δ can be summarized as follows. If the increment sequence of the polymatroid is non-constant, then the access structure is connected. If Δ does not contain any singletons or the height of the polymatroid is maximal and its increment sequence is not constant starting from the second element, then the access structure is compartmented. If Δ is generated by a singleton or the increment sequence of the polymatroid is constant starting from the second element, then the obtained access structures are hierarchical. They are proven to be ideal, and their hierarchical orders are completely determined. Moreover, if the increment sequence of the polymatroid is constant and $|\Delta| > 1$, then the hierarchical order is not antisymmetric, i.e., some different blocks are equivalent. The hierarchical order of access structures obtained from uniform integer polymatroids is always flat, that is, every hierarchy chain has at most two elements.

Keywords: secret sharing, multipartite access structure, ideal access structure, partially hierarchical access structure, uniform polymatroid

MSC 2020: 94A62

1 Introduction

A secret sharing scheme is a method of sharing a secret among a finite set of participants in such a way that only certain specified subsets of participants can compute the secret data. Secret sharing was originally introduced by Blakley [1] and Shamir [2] independently in 1979 as a solution for safeguarding cryptographic keys, but nowadays, it is used in many cryptographic protocols. The reader is referred to the studies of Beimel [3] and Padró [4] for a general introduction to secret sharing.

Let P be a finite set of participants, and let $p_0 \notin P$ be a special participant called the *dealer*. Given a secret, the dealer computes the shares and distributes them secretly to the participants, so that each participant receives only his/her share. It is required that only certain *authorized* subsets of P can recover the secret by

*** Corresponding author: Renata Kawa,** Faculty of Science and Technology, Jan Długosz University, Częstochowa, Poland, e-mail: r.kawa@ujd.edu.pl
Mieczysław Kula: Institute of Mathematics, University of Silesia, Katowice, Poland
ORCID: Renata Kawa 0000-0002-3224-7476; Mieczysław Kula 0000-0001-5743-3809

pooling their shares together. It is easily seen that the family Γ of all authorized sets, called an *access structure*, is monotone increasing, which means that any superset of an authorized subset is also authorized. To avoid borderline cases, we assume that $\emptyset \notin \Gamma$ and $P \in \Gamma$. If no unauthorized set has any information about the secret, regardless of the computational power available, then the secret sharing scheme is said to be *perfect*. Such a scheme can be considered as unconditionally secure.

Ito et al. [5] and Benaloh and Leichter [6] independently proved, in a constructive way, that every monotone increasing family of subsets of P admits a perfect secret sharing scheme. Therefore, every monotone increasing family of subsets of P is referred to as an access structure. Obviously, every access structure is uniquely determined by the family of its minimal sets. An access structure is said to be *connected* if every participant in P is a member of a minimal authorized set.

In a perfect secret sharing scheme, the length of every share is at least the length of the secret. The secret sharing schemes such that all shares have the same length as the secret are said to be *ideal*, and their access structures are called *ideal* as well. More formal definitions can be found in the articles of Beimel [3] and Padró [4]. Shamir's threshold schemes [2] are the best known examples of ideal secret sharing schemes. The secret sharing schemes constructed for a given access structure in the articles of Ito et al. [5] and Benaloh and Leichter [6] are very far from being ideal because the length of the shares grows exponentially with the number of participants.

An access structure is said to be *multipartite* if the set of participants is divided into several blocks that are pairwise disjoint and participants in individual blocks are equivalent (precise definition can be found in Section 2.1). The study of multipartite access structures was initiated by Kothari [7], who posed the open problem of constructing ideal hierarchical secret sharing schemes, and by Simmons [8], who introduced the multilevel and compartmented access structures. This approach, developed by many authors, provides a very effective tool for describing structures in a compact way, by using a few conditions that are independent of the total number of participants (cf. [9–13]) and others.

The characterization of ideal access structures is one of the main open problems in the secret sharing theory. This problem seems to be extremely difficult, and only some particular results are known. In many articles, the authors consider some specific classes of access structures with prescribed properties and try to check whether these structures are ideal. Most of the results obtained are based on the connections between ideal secret sharing schemes and matroids discovered by Brickell [14] and Brickell and Davenport [15]. Later, the use of polymatroids proposed by Farràs et al. in [10] provided a new tool for studying ideal multipartite access structures. In particular, they proved that each access structure determined by a polymatroid with a ground set J and a suitable family of subsets of J is a matroid port with a ground set $P \cup \{p_0\}$. A concise review of the results contained in the literature can be found in the articles [10–12].

Since ideal access structures are known to be matroid ports, it seems quite natural to look for ideal access structures among matroid ports. Given a specific class of polymatroids, one can take all multipartite access structures determined by these polymatroids and investigate their properties. The ideality can be established on the base of properties of particular polymatroids. In this article, the study is restricted to uniform integer polymatroids. This choice is motivated by the fact that each such polymatroid defines a family of ideal access structure (cf. Remark 2.5). But the method presented here is universal and can be continued with other classes of polymatroids in further similar studies (cf. [16]).

Here, we deal with multipartite access structures $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ in a set of participants divided into a partition Π determined by uniform integer polymatroids $\mathcal{Z}$ and monotone increasing families Δ. We examine hierarchical order among the participants induced by the obtained access structure. A short introduction to matroids and polymatroids and their relation to access structures are presented in Section 2.2. In particular, we recall the result of Farràs et al. that every polymatroid with the ground set J and a monotone increasing family of subsets of J, which is compatible with the polymatroid, determine a unique access structure, which is a matroid port. The details are described in Definition [10]. In Section 2.3, some relations between uniform integer polymatroids $\mathcal{Z} = (J, h, \boldsymbol{g})$ and monotone increasing families $\Delta \subseteq \mathcal{P}(J)\setminus\{\emptyset\}$ are presented. We prove several technical properties that are useful in the next sections.

Section 3 is devoted to the study of necessary condition for an access structure obtained from a uniform integer polymatroid to be hierarchical. Under some special conditions, it is proved that the existence of

comparable blocks in the access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ implies that the increment sequence of the polymatroid is (almost) constant. Another result of this section (Corollary 3.10) states that if the height of $\mathcal{Z}$ is greater than 1 or $\boldsymbol{g}$ is not constant, then different blocks in Π are not equivalent.

The main results obtained for access structures determined by uniform polymatroids and a monotone increasing family Δ are contained in Sections 4 and 5. If the increment sequence of the polymatroid is non-constant, then the access structure is connected (Theorem 4.1). This theorem combined with Corollary 3.10 shows that in general, the Π-partite access structures determined by uniform integer polymatroids are well constructed, i.e., all participants are important and the basic partition Π cannot be improved. The exceptions are generated by polymatroids with extreme height (1 or m) and constant increment sequence.

Theorems 4.2 and 4.3 show that large majority of access structures determined by uniform integer polymatroids are compartmented.

Exceptions occur for polymatroids with a maximum height. If Δ is generated by a singleton or the increment sequence is constant starting from the second element, then the obtained access structures are hierarchical (Theorems 4.8, 4.9, and 4.11). In these cases, the hierarchical orders are completely determined. Moreover, if the polymatroid height is two, then complete description of hierarchical structures is also given (Theorem 4.6).

Moreover, we prove in Theorem 4.12 that the maximal length of chains in such hierarchical access structures is equal to 1. This fact seems quite surprising, because for other polymatroids, one can construct hierarchical access structures with chains of arbitrary length. For instance, such constructions can be found in [11–13,16] and others.

As was mentioned earlier, every uniform integer polymatroid determines some ideal access structures, but the question is whether all access structures determined by uniform integer polymatroids are ideal. A direction, which is worth considering and may result in obtaining the answer, is using the fact that a sufficient condition (for access structures to be ideal) can be obtained by proving that the one point extension of a given uniform integer polymatroid is representable (cf. [10, Corollary 6.7]). This method has been applied in Section 5 to the proof that all the structures described in Theorems 4.6, 4.8, and 4.11 are ideal. It is worth noting that the class of access structures obtained from uniform integer polymatroids contains some interesting families of objects that can be useful for the applications of secret sharing.

Another interesting example is the family of uniform access structures characterized by Farrás et al. in [12, Section VI] (cf. Remark 4.10). It consists of multipartite access structures that are invariant under any permutation of blocks of participants. In other words, all participants have the same rights, although they are not hierarchically equivalent. A different situation occurs in compartmented access structures, where there is a set of distinguished participants, whose representatives must be present in all authorized sets. Such a case is described in Theorem 5.2.

This article is intended to initiate research on the access structures obtained from uniform integer polymatroids, but it does not exhaust the topic and leaves space for further study. Some remarks on the new research possibilities can be found in Section 6. Appendix contains a classification of all access structures with four parts obtained from uniform integer polymatroids.

2 Preliminaries

The aim of this section is to provide the necessary definitions and results regarding multipartite access structures and polymatroids. In general, we are using the same or similar notations and definitions as in the articles [11] and [12]. The family of all subsets of a set X is denoted by $\mathcal{P}(X)$ (the power set). Similarly, $\mathcal{P}_k(X)$ denotes the collection of all of k-element subsets of X. Let $\mathbb{N}_0$ and $\mathbb{N}$ denote the set of all non-negative integers and positive integers, respectively. Let J be a finite set. For two vectors $\bar{u} = (u_x)_{x\in J}$ and $\bar{v} = (v_x)_{x\in J} \in \mathbb{N}_0^J$, we write $\bar{u} \le \bar{v}$ if $u_x \le v_x$ for all $x \in J$. Moreover, $\bar{u} < \bar{v}$ denotes $\bar{u} \le \bar{v}$ and $\bar{u} \ne \bar{v}$. Given a vector $\bar{v} = (v_x)_{x\in J}$, we

define the support $\operatorname{supp}(\bar{v}) = \{x \in J : v_x \neq 0\}$ and the modulus $|\bar{v}| = \sum_{x\in J} v_x$. Furthermore, we write $\bar{v}_X = (v'_x)_{x\in J}$, where $X \subseteq J$ and

$$v'_x = \begin{cases} v_x & \text{if } x \in X, \\ 0 & \text{if } x \notin X. \end{cases}$$

In particular, $\bar{v}_\emptyset = (0)_{x\in J}$. Let us observe that $|\bar{v}| = |\bar{v}_X|$ is equivalent to $\operatorname{supp}(\bar{v}) \subseteq X$. For every $z \in J$, we define the vector $\bar{e}^{(z)} \in \mathbb{N}_0^J$ such that $\bar{e}^{(z)} = (e_x^{(z)})_{x\in J}$ with $e_z^{(z)} = 1$ and $e_x^{(z)} = 0$ for all $x \neq z$. For undefined notions, see the articles [10] and [17].

2.1 Multipartite access structures

Let Γ be an access structure on a set of participants P. A participant $p \in P$ is said to be *hierarchically superior or equivalent* to a participant $q \in P$ (written $q \preccurlyeq p$), if $A \cup \{p\} \in \Gamma$ for all subsets $A \subseteq P\setminus\{p, q\}$ with $A \cup \{q\} \in \Gamma$. If $p \preccurlyeq q$ and $q \preccurlyeq p$, then the participants p and q are called *hierarchically equivalent*.

By a *partition* (Π-*partition*) of the set of participants P, we mean a family $\Pi = (P_x)_{x\in J}$ of pairwise disjoint and nonempty subsets of P, called blocks, such that $P = \bigcup_{x\in J} P_x$. An access structure Γ is said to be *multipartite* (Π-*partite*) if all participants in every block P_x are pairwise hierarchically equivalent. Thus, we are allowed to define a hierarchy in Π. Namely, P_x is said to be *hierarchically superior or equivalent* to P_y (written $P_y \preccurlyeq P_x$) if there are $p \in P_y$ and $q \in P_x$ such that $p \preccurlyeq q$. In other words, it can be said that P_y is *hierarchically inferior or equivalent to* P_x. By transitivity, we have $p \preccurlyeq q$ for all $p \in P_y$ and $q \in P_x$ whenever $P_y \preccurlyeq P_x$. The relation $\preccurlyeq$ both in P and in Π is reflexive and transitive but not antisymmetric in general, so it is a preorder. If $P_x \preccurlyeq P_y$ and $P_y \preccurlyeq P_x$, then the blocks P_x and P_y are called *hierarchically equivalent*. Moreover, if $P_x \preccurlyeq P_y$ or $P_y \preccurlyeq P_x$, then the blocks P_x and P_y are called *hierarchically comparable*; otherwise, they are called *hierarchically independent*. Finally, if $P_x \preccurlyeq P_y$ and the blocks are not hierarchically equivalent, then we write $P_x \prec P_y$.

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. A participant who does not belong to any minimal authorized set is called *redundant*. It is easy to see that every participant is hierarchically superior or equivalent to any redundant participant. In particular, all redundant participants are hierarchically equivalent. A block of participants that contains a redundant participant will also be called *redundant*.

A Π-partite access structure is said to be *hierarchical* if there are blocks P_x and P_y in Π such that $P_x \prec P_y$. Otherwise, the access structure is referred to as *compartmented*.

A hierarchical access structure such that the relation $\preccurlyeq$ is antisymmetric and every pair of blocks is hierarchically comparable is referred to as *totally hierarchical*. A complete characterization of ideal totally hierarchical access structure was presented by Farràs and Padró [11]. 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.

Given a partition $\Pi = (P_x)_{x\in J}$ of P and a subset $A \subseteq P$, we define the vector $\pi(A) = (v_x)_{x\in J}$, where $v_x = |A \cap P_x|$. If Γ is a Π-partite access structure, then all participants in every subset P_x are pairwise hierarchically equivalent, 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

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

Obviously, if $A \subseteq B \subseteq P$, then $\pi(A) \leq \pi(B)$. Moreover, if $\bar{u} \in \pi(\Gamma)$ and $\bar{u} \leq \bar{v} \leq \pi(P)$, then $\bar{v} \in \pi(\Gamma)$. Indeed, there is $A \in \Gamma$ such that $\bar{u} = \pi(A)$. The set A can be extended to a set $B \subseteq P$ such that $\bar{v} = \pi(B)$. Hence, $B \in \Gamma$ and consequently, $\bar{v} \in \pi(\Gamma)$. This shows that $\pi(\Gamma) \subseteq \mathfrak{P}(\Pi)$ is a set of vectors monotone increasing with respect to $\leq$. On the other hand, every monotone increasing set $\Gamma' \subseteq \mathfrak{P}(\Pi)$ 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 monotone increasing subsets of $\mathfrak{P}(\Pi)$. Therefore, we use the

same notation Γ for both the access structure and its vector representation. With this convention, we define $\mathrm{supp}(\Gamma) = \{\mathrm{supp}(\bar{v}) \in \mathcal{P}(J) : \bar{v} \in \Gamma\}$.

The hierarchy among blocks in Π can be characterized in vector terms as follows: $P_y \preccurlyeq P_x$ if and only if

$$\bar{v} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \Gamma \quad \text{for all } \bar{v} \in \Gamma \text{ with } v_y \geq 1 \quad \text{and} \quad v_x < |P_x|. \tag{1}$$

To show that $P_y \preccurlyeq P_x$, it is enough to check if the aforementioned condition is satisfied for all vectors $v \in \min\Gamma$. A block P_x in Π is redundant if and only if $v_x = 0$ for every $\bar{v} \in \min\Gamma$.

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
- $h(\varnothing) = 0$;
- h is monotone increasing: if $X \subseteq Y \subseteq J$, then $h(X) \leq h(Y)$;
- h is submodular: if $X, Y \subseteq J$, then $h(X \cap Y) + h(X \cup Y) \leq h(X) + h(Y)$.

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 article are assumed to be integer, so we omit the term "integer" when dealing with polymatroid.

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

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 $\mathcal{V} = (V_x)_{x\in J}$ be a family of subspaces of V. One can show that the mapping $h : \mathcal{P}(J) \longrightarrow \mathbb{N}_0$ defined by $h(X) = \dim(\sum_{x\in X} V_x)$ 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 $\dim V_x \leq 1$ for all $x \in J$, then we obtain a matroid, which is called *representable* as well. The family $\mathcal{V}$ is referred to as a *vector space representation* of the polymatroid (matroid).

Let $\mathcal{Z} = (J, h)$ be a polymatroid. For $J' = J \cup \{x_0\}$ with a certain $x_0 \notin J$ and a monotone increasing family $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$, we define the function $h' : \mathcal{P}(J') \longrightarrow \mathbb{N}_0$ by $h'(X) = h(X)$ for all $X \in \mathcal{P}(J)$ and

$$h'(X \cup \{x_0\}) = \begin{cases} h(X) & \text{if } X \in \Delta, \\ h(X) + 1 & \text{if } X \in \mathcal{P}(J)\backslash\Delta. \end{cases}$$

If h' is monotone increasing and submodular, then Δ is said to be *compatible* with $\mathcal{Z}$ and $\mathcal{Z}' = (J', h')$ is a polymatroid, which is called the *one point extension of* $\mathcal{Z}$ *induced by* Δ. It is easy to see that $h'(x_0) = 1$ and Δ is the polymatroid port of $\mathcal{Z}'$ at the point x_0. The next result, which is a consequence of [18, Proposition 2.3] (cf. also [11, Proposition 5.2]), is very useful in the investigation of access structures induced by polymatroids.

Lemma 2.1. ([18] Csirmaz, [10]) *A monotone increasing family* $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$ *is compatible with the integer polymatroid* $\mathcal{Z} = (J, h)$ *if and only if the following conditions are satisfied*:
(1) *If* $Y \subseteq X \subseteq J$ *and* $Y \notin \Delta$ *while* $X \in \Delta$, *then* $h(Y) < h(X)$.
(2) *If* $X, Y \in \Delta$ *and* $X \cap Y \notin \Delta$, *then* $h(X \cap Y) + h(X \cup Y) < h(X) + h(Y)$.

The following notation will be used very often throughout this article. Let $\mathcal{Z} = (J, h)$ be a polymatroid and let $X \subseteq J$. We define the following set:

$$\mathcal{B}(\mathcal{Z}, X) = \{\bar{v} \in \mathbb{N}_0^J : \mathrm{supp}(\bar{v}) \subseteq X, \quad |\bar{v}| = h(X), \quad \forall_{Y\subseteq X} |\bar{v}_Y| \leq h(Y)\}. \tag{2}$$

The notation $\mathcal{B}(\mathcal{Z}, X)$ was introduced in [10]. Here, we will use its simplified form $\mathcal{B}(X)$. It is easy to see that

$$\text{if } Y \subseteq X \subseteq J \quad \text{and} \quad h(Y) = h(X), \quad \text{then } \mathcal{B}(Y) \subseteq \mathcal{B}(X). \tag{3}$$

On the other hand, $\mathcal{B}(Y) \cap \mathcal{B}(X) = \varnothing$ whenever $h(Y) \neq h(X)$.

The connection between matroids and ideal access structures was discovered by Brickell and Davenport [15]. 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.

The converse is not true. For example, the ports of the Vamos matroid are not ideal access structures (cf. [19]). But the linear construction of ideal secret sharing schemes proposed by Brickell [14] shows that every port of a representable matroid is an ideal access structure.

Following [12, Definition 2.3], we define the main notion of this article.

Definition 2.2. Let $\Pi = (P_x)_{x\in J}$ be a partition of a set P of participants. Consider a polymatroid $\mathcal{Z} = (J, h)$ with $h(\{x\}) \leq |P_x|$ for every $x \in J$, and a monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$, which is compatible with $\mathcal{Z}$. We define a Π-partite access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ in the following way: a vector $\bar{u} \in \mathfrak{P}(\Pi)$ is in $\Gamma(\Pi, \mathcal{Z}, \Delta)$ if and only if there exist a subset $X \in \Delta$ and a vector $\bar{v} \in \mathcal{B}(X)$ such that $\bar{v} \leq \bar{u}$. The family $\Gamma(\Pi, \mathcal{Z}, \Delta)$ will be called the Π-*partite access structure determined by the polymatroid* $\mathcal{Z}$ *and the monotone increasing family* Δ.

Let $\Pi = (P_x)_{x\in J}$ be a partition of a set P of participants. Farràs et al. [10, Theorem 5.3] proved that a Π-partite access structure Γ on P is a matroid port if and only if $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ for some polymatroid $\mathcal{Z}$ with ground set J and monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ compatible with $\mathcal{Z}$. Access structures that are matroid ports are called κ-*ideal* in the literature. Moreover, if there is a (linearly) representable one point extension $\mathcal{Z}'$ of $\mathcal{Z}$ and Δ is a polymatroid port of $\mathcal{Z}'$, then Γ is an ideal acces structure.

Example 2.3. Let us consider $J' = \{0, 1, 2, 3\}$ and the function $h' : \mathcal{P}(J') \longrightarrow \mathbb{N}_0$ defined by:

$$h'(X) = \begin{cases} 0 & \text{if } |X| = 0; \\ 1 & \text{if } |X| = 1; \\ 2 & \text{if } |X| \geq 2. \end{cases}$$

It is easy to check that $\mathcal{Z}' = (J', h')$ is a polymatroid and $\Delta = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ is its port at 0. Moreover, $\mathcal{Z}'$ is a one point extension of $\mathcal{Z} = \mathcal{Z}'|J$, where $J = \{1, 2, 3\}$. Thus, Δ is compatible with $\mathcal{Z}$. Hence, we obtain $\mathcal{B}(\{1, 2\}) = \{(1, 1, 0)\}$, $\mathcal{B}(\{1, 3\}) = \{(1, 0, 1)\}$, $\mathcal{B}(\{2, 3\}) = \{(0, 1, 1)\}$ and $\mathcal{B}(\{1, 2, 3\}) = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$. From the aforementioned definition, we have $\bar{u} \in \Gamma(\Pi, \mathcal{Z}, \Delta)$ if and only if $\bar{u} \leq \pi(P) = (|P_1|, |P_2|, |P_3|)$ and $|\mathrm{supp}(\bar{u})| \geq 2$.

2.3 Uniform polymatroids

We begin this subsection with the definition of uniform polymatroids that play a major role in this article. To shorten notation, we set $I_m = \{0, 1, \ldots, m\}$.

Definition 2.4. An integer polymatroid $\mathcal{Z} = (J, h)$ is called *uniform* if

$$|X| = |Y| \Rightarrow h(X) = h(Y) \quad \text{for all } X, Y \subseteq J.$$

Let $m := |J|$. We define $h_i = h(X)$ for every $i \in I_m$ with $X \subseteq J, |X| = i$. It is obvious that the sequence $(h_i)_{i\in I_m}$ determines the rank function of the polymatroid. For this sequence, we define the *increment sequence* $\boldsymbol{g} = (g_i)_{i\in I_m}$ by $g_i = h_{i+1} - h_i$ for $i = 0, \ldots, m-1$, and additionally, $g_m = 0$. It is easy to see that $\boldsymbol{g}$ is nonincreasing sequence of non-negative integers.

On the other hand, every nonincreasing sequence $\boldsymbol{g} = (g_i)_{i\in I_m}$ of non-negative integers with $g_m = 0$, determines h_j by:

$$h_j = \sum_{i=0}^{j-1} g_i \quad \text{for all } j = 1,\dots,m \quad \text{and} \quad h_0 = 0. \tag{4}$$

This sequence $(h_j)_{j\in I_m}$ actually defines an integer polymatroid.

We define the *height of a polymatroid* as the number of nonzero elements in $\boldsymbol{g}$. A polymatroid is said to be of a *maximal height* if $g_{m-1} > 0$. Note that $g_0 = 0 \Leftrightarrow h_1 = \cdots = h_m = 0$ and $g_1 = 0 \Leftrightarrow h_1 = \cdots = h_m = g_0$. Hence, according to the assumption that we consider only polymatroids such that their rank functions do not have all values equal to 0, from now on, we assume that the height of each uniform polymatroid is greater than zero. To avoid repetition in the further part of this article, a uniform polymatroid will be denoted by $\mathcal{Z} = (J, h, \boldsymbol{g})$, where $\boldsymbol{g} = (g_i)_{i\in I_m}$, $g_0 > g_m = 0$ is a nonincreasing sequence of non-negative integers and $h : \mathcal{P}(J) \to \mathbb{N}_0$ is the rank function such that $h(X) = h_k = \sum_{i=0}^{k-1} g_i$ for every $X \in \mathcal{P}(X)$ with $k = |X|$.

Remark 2.5. We shall show that every uniform polymatroid determines at least one ideal access structure. Indeed, uniform polymatroids are known to be representable (cf. [9, Theorem 6]). Let $\mathbb{K}$ be a finite field, and let $(V_x)_{x\in J}$ be a $\mathbb{K}$-vector space representation of a uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$. Then, V_x are the subspaces of the vector space $\mathbb{K}^{h_m}$ and $\dim V_x = h_1 = g_0$ for every $x \in J$. For any $X \subseteq J$, we define $V_X = \sum_{x\in X} V_x$. Given a nonzero vector $\beta \in \mathbb{K}^{h_m}$, the family $\Delta = \{X \subseteq J : \beta \in V_X\} \subseteq \mathcal{P}(J)$ is a monotone increasing family of subsets of J and Δ is compatible with the polymatroid $\mathcal{Z}$. It is easily seen that $(V_x)_{x\in J\cup\{x_0\}}$, where $x_0 \notin J$ and $V_{x_0} = \operatorname{span}(\{\beta\})$ is a vector space representation of the one point extension of $\mathcal{Z}$ induced by Δ. This shows that the access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ is ideal. Varying the representation of $\mathcal{Z}$ and the vector β, we can control to some extent the selection of Δ that allows us to obtain different ideal access structures. This idea will be used in Section 5 in proofs that the structures considered there are linearly representable.

In order to continue our studies, we need some elementary properties of vectors in $\mathcal{B}(X)$ that are proved in several technical lemmas. In the remainder of this subsection, we assume that $\mathcal{Z} = (J, h, \boldsymbol{g})$ is a uniform polymatroid and $X \subseteq J$. Let us recall that $\mathcal{B}(X)$ is defined by equation (2).

Lemma 2.6. *If* $1 \le k = |X|$ *and* $\bar{w} \in \mathcal{B}(X)$, *then*:

(1) *For every* $x \in X$ *we have* $w_x \ge g_{k-1}$.

(2) *If* $w_x = g_{k-1}$ *for some* $x \in X$, *then* $\bar{w} - w_x\bar{e}^{(x)} \in \mathcal{B}(X\setminus\{x\})$.

Proof.

(1) Let us note that $|\bar{w}_X| = h(X) = h_k$ and $|\bar{w}_{X\setminus\{x\}}| \le h(X\setminus\{x\}) = h_{k-1}$; hence,

$$w_x = |\bar{w}_X| - |\bar{w}_{X\setminus\{x\}}| \ge h_k - h_{k-1} = g_{k-1}.$$

(2) If we set $\bar{v} := \bar{w} - w_x\bar{e}^{(x)}$, then we have $\operatorname{supp}(\bar{v}) \subseteq X\setminus\{x\}$ and

$$|\bar{v}| = h_k - g_{k-1} = h_{k-1} = h(X\setminus\{x\}). \qquad \square$$

Lemma 2.7. *Let* $x, y \in X, x \ne y$, *and* $\bar{w} \in \mathcal{B}(X)$ *such that* $w_x = g_0, w_y \ne 0$. *If* $\bar{v} \in \mathcal{B}(\operatorname{supp}(\bar{v}))$ *and* $\bar{v} \le \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$, *then* $y \notin \operatorname{supp}(\bar{v})$.

Proof. Let $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$ and $Y := \operatorname{supp}(\bar{v})$. It is clear that $\bar{v} \in \mathcal{B}(Y)$ implies $v_x \le h_1 = g_0$ and $|\bar{v}| = h(Y)$. Moreover, $Y \subseteq X$ and $|\bar{w}_Y| \le h(Y)$. Suppose that $y \in Y$. If $x \in Y$, then we have

$$h(Y) = |\bar{v}| \le w_x + (w_y - 1) + |\bar{w}'_{Y\setminus\{x,y\}}| = |\bar{w}_Y| - 1 \le h(Y) - 1,$$

which is a contradiction.

Similarly, if $x \notin Y$, then we have

$$h(Y) = |\bar{v}| \le (w_y - 1) + |\bar{w}'_{Y\setminus\{y\}}| = |\bar{w}_Y| - 1 \le h(Y) - 1,$$

which is a contradiction. This completes the proof. □

Lemma 2.8. *Let $y \in X$ and $x \in J\setminus X$ and $\bar{w} \in \mathcal{B}(X)$ such that $w_y = g_0$. If $k := |X|$, $g_k > 0$, and $\bar{v} \in \mathcal{B}(\mathrm{supp}(\bar{v}))$ such that $\bar{v} \le \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$, then $y \notin \mathrm{supp}(\bar{v})$. Moreover, if $g_0 > 1$, then $x, y \notin \mathrm{supp}(\bar{v})$, i.e., $\mathrm{supp}(\bar{v}) \subseteq X\setminus\{y\}$.*

Proof. Let $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$. Clearly, $\mathrm{supp}(\bar{v}) \subseteq \mathrm{supp}(\bar{w}') \subseteq X \cup \{x\}$. Let $Y := X \cap \mathrm{supp}(\bar{v})$, and let $l := |Y|$. Suppose that $y \in \mathrm{supp}(\bar{v})$. If $x \in \mathrm{supp}(\bar{v})$, then $\mathrm{supp}(\bar{v}) = Y \cup \{x\}$, and we have $l \le k$ and

$$h_{l+1} = |\bar{v}| \le |\bar{w}'_{Y\setminus\{y\}}| + 1 + (g_0 - 1) = |\bar{w}_{Y\setminus\{y\}}| + g_0 = |\bar{w}_Y| \le h_l.$$

Hence, $0 < g_k \le g_l = h_{l+1} - h_l \le 0$, which is a contradiction.

If $x \notin \mathrm{supp}(\bar{v})$, then $\mathrm{supp}(\bar{v}) = Y$, and we have

$$h_l = |\bar{v}| \le |\bar{w}'_{Y\setminus\{y\}}| + (g_0 - 1) = |\bar{w}_{Y\setminus\{y\}}| + g_0 - 1 = |\bar{w}_Y| - 1 = h_l - 1,$$

which is a contradiction. Thus, we have proved that $\mathrm{supp}(\bar{v}) \subseteq (Y\setminus\{y\}) \cup \{x\}$.

Now, we assume $g_0 > 1$ and suppose $\mathrm{supp}(\bar{v}) = (Y\setminus\{y\}) \cup \{x\}$.

$$h_l = |\bar{v}| \le |\bar{w}'_{Y\setminus\{y\}}| + 1 = |\bar{w}_{Y\setminus\{y\}}| + 1 = |\bar{w}_{Y\setminus\{y\}}| + g_0 - (g_0 - 1) = |\bar{w}_Y| - (g_0 - 1) < h_l,$$

as $g_0 - 1 > 0$, which is a contradiction. This shows $\mathrm{supp}(\bar{v}) = Y\setminus\{y\} \subseteq X\setminus\{y\}$, which completes the proof. □

Lemma 2.9. *Let $x, y \in X$, $x \ne y$, and $\bar{w} \in \mathcal{B}(X)$. If $w_y > 0$, then either $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \mathcal{B}(X)$, or there exists a set $Y \subseteq X\setminus\{y\}$, $x \in Y$, such that $\bar{v} := \bar{w}_Y \in \mathcal{B}(Y)$. Furthermore, $\bar{v} \le \bar{w}$ and $\bar{v} \le \bar{w}'$.*

Proof. Note that $\mathrm{supp}(\bar{w}') \subseteq X$ and $|\bar{w}'_X| = |\bar{w}_X| = h(X) = h_{|X|}$. Let us consider the case $\bar{w}' \notin \mathcal{B}(X)$, that is, there is a set $Y \subseteq X$ that $|\bar{w}'_Y| \ge h(Y) + 1$. Let us choose a minimum set Y for this property. It is easy to see that $x \in Y$ and $y \notin Y$. Setting the notation $l := |Y|$, we obtain

$$h_l + 1 \le |\bar{w}'_Y| = (w_x + 1) + |\bar{w}_{Y\setminus\{x\}}| = |\bar{w}_Y| + 1 \le h_l + 1,$$

and consequently, $|\bar{w}_Y| = h_l$. Thus, for $\bar{v} := \bar{w}_Y$, we have $\bar{v} \in \mathcal{B}(Y)$. It is clear that $\bar{v} \le \bar{w}$ and $\bar{v} \le \bar{w}'$, which completes the proof. □

Now, we introduce a notion of a vertex vector. Let J be a finite set and $m := |J|$ and let $\boldsymbol{g} = (g_i)_{i\in I_m}$ be the increment sequence of a uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$. Given $X \subseteq J$ and a bijection $\sigma : X \to \{0, 1, \ldots, k-1\}$, where $k = |X|$, we define the vector $\bar{w} = (w_x)_{x\in J}$ by:

$$\bar{w} = \sum_{x\in X} g_{\sigma(x)} \bar{e}^{(x)},$$

which is referred to as a *vertex vector with basic set X*. Note that in general, we have $\mathrm{supp}(\bar{w}) \subseteq X$, but $\mathrm{supp}(\bar{w}) = X$ whenever $g_{k-1} > 0$. Vertex vectors are the vertices of the convex polytope

$$T = \{\bar{w} \in \mathbb{N}_0^J : |\bar{w}_X| \le h(X) \quad \text{for every } X \subseteq J\},$$

determined by the polymatroid (J, h).

Lemma 2.10. *For every vertex vector $\bar{w}$, we have $\bar{w} \in \mathcal{B}(\mathrm{supp}(\bar{w}))$.*

Proof. Let $\bar{w}$ be any vertex vector and $k := |\mathrm{supp}(\bar{w})|$. Let us take a subset $Y \subseteq \mathrm{supp}(\bar{w})$ and set $l := |Y| \le k$. The sequence $\boldsymbol{g}$ being nonincreasing implies

$$|\bar{w}_Y| = \sum_{x\in Y} w_x = \sum_{x\in Y} g_{\sigma(x)} \le \sum_{i=0}^{l-1} g_i = h_l = h(Y).$$

Here, we use the fact that the sum of l arbitrary elements of a nonincreasing sequence does not exceed the sum of the l initial entries of the sequence. In particular, we obtain $|\bar{w}_{\mathrm{supp}(\bar{w})}| = \sum_{i=0}^{k-1} g_i = h_k = h(\mathrm{supp}(\bar{w}))$, which shows that $\bar{w} \in \mathcal{B}(\mathrm{supp}(\bar{w}))$. □

Remark 2.11. Note that if $\mathcal{Z}$ is a uniform polymatroid, then the set $\mathcal{B}(X)$ is always nonempty since it contains vertex vectors with basic set X. In extreme cases when $X = \varnothing$ or the range function of the polymatroid has all values equal to 0, the family $\mathcal{B}(X)$ contains only the zero vector. Moreover, it is easy to check that if $\bar{w} \in \mathcal{B}(X)$ for some $X \subseteq J$, then $\bar{w} \in \mathcal{B}(\mathrm{supp}(\bar{w}))$.

Deciding if a monotone increasing family is compatible with a given polymatroid is not an easy task. The Csirmaz lemma seems to be the most general tool for solving this problem. For example, it is easy to check that if the increment sequence of a polymatroid with ground set J is strictly decreasing, then every proper monotone increasing family of subsets of J is compatible with the polymatroid. At the end of this section, we present several facts related to the compatibility of monotone increasing families and polymatroids, which are used in proofs in subsequent sections.

Lemma 2.12. *Let $\mathcal{Z} = (J, h, \boldsymbol{g})$ be a uniform polymatroid and let a monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ be compatible with $\mathcal{Z}$.*
(1) *If $g_k = 0$ for some $1 \le k \le |J|$, then all subsets of the set J with at least k elements belong to Δ.*
(2) *If Δ contains a minimal set with k elements, then $g_{k-1} > 0$.*

Proof. (1) By assumption, we have $g_i = 0$ for all $i = k, \dots, m$. Let us consider $X \subseteq J$, $l := |X| \ge k$. Then, we have

$$h(J) - h(X) = h_{|J|} - h_{|X|} = \sum_{i=l}^{m-1} g_i = 0.$$

This implies $h(X) = h(J)$, and by the Csirmaz lemma, we obtain $X \in \Delta$.

(2) Assume that $X \subseteq J$ is a minimal set in Δ, $|X| = k$. Then, for every $Y \subseteq X$ with $|Y| = k - 1$, we have $Y \notin \Delta$, so by the Csirmaz lemma $h_{|Y|} < h_{|X|}$. Hence,

$$g_{k-1} = h_k - h_{k-1} = h_{|X|} - h_{|Y|} > 0.$$ □

Lemma 2.13. *If $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ is a monotone increasing family such that $\min\Delta = \{X\}$ for some $\varnothing \ne X \subseteq J$, then Δ is compatible with a uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ if and only if $g_{m-1} > 0$.*

Proof. Assume Δ is compatible with $\mathcal{Z}$. If $x \in X$, then $J\setminus\{x\} \notin \Delta$, so by Csirmaz lemma $h(J\setminus\{x\}) < h(J)$, thus $g_{m-1} = h(J) - h(J\setminus\{x\}) > 0$.

Now, we shall show that the conditions of the Csirmaz lemma are met whenever $g_{m-1} > 0$. Let us note that $h_i - h_{i-1} = g_{i-1} > 0$ for all $i = 1, \dots, m$, so the sequence $h_0, h_1, \dots, h_m$ is strictly increasing. Let us take such sets $Y \subseteq W \subseteq J$, that $Y \notin \Delta$ and $W \in \Delta$. Of course, $|Y| < |W|$, so we have $h(Y) < h(W)$; thus, condition (1) is satisfied.

Now, let us consider $W, Y \in \Delta$. Then, $X \subseteq W$ and $X \subseteq Y$ since $\min\Delta = \{X\}$, so $W \cap Y \in \Delta$. This shows that the second condition of the Csirmaz lemma is also satisfied. □

Let us recall a result of Farràs et al., which can be restated as follows.

Lemma 2.14. ([12], Lemma 6.1) *For a positive integer $k \in I_m$, the monotone increasing family Δ such that $\min\Delta = \mathcal{P}_k(J)$ is compatible with a uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ if and only if $g_{k-1} > g_k$.*

Further results concerned with compatibility can be found in Section 4.

3 Access structures determined by uniform polymatroids

This section is devoted to the study of necessary conditions for an access structure obtained from a uniform polymatroid to be hierarchical. It is proved in Propositions 3.4, 3.5, 3.7, and 3.8, and Corollary 3.9 that under some special conditions, the existence of comparable blocks in the access structure $\Gamma(\Pi, \mathcal{Z}, \Delta)$ implies $g_1 = g_{m-1}$ i.e., the increment sequence of the polymatroid is (almost) constant. Another result of this section (Corollary 3.10) states that if the height of $\mathcal{Z}$ is greater than 1 or $\boldsymbol{g}$ is not constant, then different blocks in Π are not equivalent. This means that the relation $\preccurlyeq$ is antisymmetric in this case.

From now on, we make the assumptions: J is a finite set with $m := |J| \geq 2$, $\boldsymbol{g} = (g_i)_{i\in I_m}$ being the increment sequence of a uniform polymatroid $\mathcal{Z}$ with ground set J and $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$. Moreover, $0 < g_0 < |P_x|$ for all $x \in J$; hence, height of $\mathcal{Z}$ is greater than or equal to 1. We define $\mu(\Delta) = \min\{|X| : X \in \Delta\}$. Note that $\mu(\Delta) \geq 1$, as $\varnothing \notin \Delta$.

Example 3.1. Let us consider a uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ such that the height of $\mathcal{Z}$ equals 1, i.e., $g_0 > g_1 = 0$, and a monotone increasing family Δ of subsets of J is compatible with $\mathcal{Z}$. Applying Lemma 2.12 (1) yields $\Delta = \mathcal{P}(J)\backslash\{\varnothing\}$. According to equation (4), we have $h(X) = g_0$ for all nonempty subsets X of J. Hence, $\mathcal{B}(X) \subseteq \mathcal{B}(J)$ for every $\varnothing \neq X \subseteq J$ (cf. equation (3)), and consequently, $\bigcup_{X\in\Delta}\mathcal{B}(X) = \mathcal{B}(J)$. Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$. This implies that $\bar{w} \in \min\Gamma$ if and only if $|\bar{w}| = g_0$ or equivalently $\bar{w} \in \Gamma$ if and only if $|\bar{w}| \geq g_0$. This shows that the threshold access structure is the only type of access structures determined by uniform polymatroids with height equal to 1. In particular, all blocks (and participants) are hierarchically equivalent.

Let us collect several simple observations, which are very helpful in many proofs.

Lemma 3.2.
(1) $\mathcal{B}(X) \subseteq \Gamma$ *for all* $X \in \Delta$.
(2) $\operatorname{supp}(\Gamma) = \Delta$.
(3) *If* $\bar{w} \in \min\Gamma$, *then* $\bar{w} \in \mathcal{B}(\operatorname{supp}(\bar{w}))$ *and* $\operatorname{supp}(\bar{w}) \in \Delta$.
(4) *If* $\bar{w} \in \Gamma$, *then there exists* $\bar{v} \in \min\Gamma$ *such that* $\bar{v} \preccurlyeq \bar{w}$, $\bar{v} \in \mathcal{B}(\operatorname{supp}(\bar{v}))$ *and* $\operatorname{supp}(\bar{v}) \in \Delta$.
(5) *If* $\bar{w}$ *is a vertex vector and* $\operatorname{supp}(\bar{w}) \in \Delta$, *then* $\bar{w} \in \Gamma$.

Proof.
(1) This follows directly from Definition 2.2. (2) Let us consider $Y \in \operatorname{supp}(\Gamma)$. Then, there exists $\bar{w} \in \Gamma$ such that $\operatorname{supp}(\bar{w}) = Y$. Let us consider two cases:
   (i) $\bar{w} \in \min\Gamma$. Then, there exists $X \in \Delta$ such that $\bar{w} \in \mathcal{B}(X)$, so $Y \subseteq X$. If $Y = X$, then $Y \in \Delta$. If $Y \subsetneq X$, then also $Y \in \Delta$. Indeed, let us note that $|\bar{w}_Y| \leq h(Y)$, $|\bar{w}_X| = h(X)$, and $|\bar{w}_Y| = |\bar{w}_X|$, where the later equality follows from the fact $\operatorname{supp}(\bar{w}) = Y \subseteq X$. Moreover, if $Y \notin \Delta$, then by the Csirmaz lemma, we would obtain
$$h(X) = |\bar{w}_X| = |\bar{w}_Y| \leq h(Y) < h(X),$$
   which is a contradiction.
   (ii) $\bar{w} \in \Gamma$ and $\bar{w} \notin \min\Gamma$. Then, there is $\bar{v} \in \min\Gamma$ such that $\bar{v} \preccurlyeq \bar{w}$. From Case (i), we obtain $\operatorname{supp}(\bar{v}) \in \Delta$. Let us note that $\operatorname{supp}(\bar{v}) \subseteq \operatorname{supp}(\bar{w})$. Moreover, Δ is a monotone increasing family, so $Y = \operatorname{supp}(\bar{w}) \in \Delta$.

Now, we shall show the converse inclusion. Let us take $X \in \Delta$. As we already have observed in Remark 2.11, the family $\mathcal{B}(X)$ cannot be empty, so there is a certain vector $\bar{w} \in \mathcal{B}(X)$. By (1), we obtain $\bar{w} \in \Gamma$, so $\operatorname{supp}(\bar{w}) \in \operatorname{supp}(\Gamma)$. The family $\operatorname{supp}(\Gamma)$ is monotone increasing and $\operatorname{supp}(\bar{w}) \subseteq X$, so $X \in \operatorname{supp}(\Gamma)$.
(3) If $\bar{w} \in \min\Gamma$, then $\bar{w} \in \mathcal{B}(X)$ for some $X \in \Delta$. Remark 2.11 implies $\bar{w} \in \mathcal{B}(\operatorname{supp}(\bar{w}))$. Moreover, $\operatorname{supp}(\bar{w}) \in \operatorname{supp}(\Gamma)$; hence, and by (2), we obtain $\operatorname{supp}(\bar{w}) \in \Delta$.
(4) It follows from (3) immediately.
(5) If $\bar{w}$ is a vertex vector, then we have $\bar{w} \in \mathcal{B}(\operatorname{supp}(\bar{w}))$ by Lemma 2.10. By assumption and part (1) of this lemma, we obtain $\bar{w} \in \Gamma$. □

Lemma 3.3. *If $g_1 = g_{n-1} > 0$ for some $2 \le n \le m$ and if $X, Y \in \min\Delta$ as well as $|X \cup Y| \le n$, then $X = Y$ or both sets are singletons. Moreover, if $g_0 = g_1$, then $X = Y$ even if both X and Y are singletons.*

Proof. For $n = 2$, the claim is obvious. Let us assume $n \ge 3$. It is enough to consider the case $X \ne Y$. Suppose that at least one of these sets, for example X, has at least two elements. Let us fix $x \in X$ and consider the set

$$Y' = \begin{cases} Y & \text{when } X \cap Y \ne \emptyset; \\ Y \cup \{x\} & \text{when } X \cap Y = \emptyset. \end{cases}$$

Note that $|X \cup Y'| = |X \cup Y| \le n$ and $W \coloneqq X \cap Y' \ne \emptyset$. In addition, W is a proper subset of X, which is a minimum set in Δ, so it does not belong to Δ. Hence, according to the Csirmaz lemma, we obtain

$$h(W) + h(X \cup Y') < h(X) + h(Y').$$

On the other hand, the assumption $g_1 = g_{n-1}$ implies $h_l = g_0 + (l-1)g_1$ for every $1 \le l \le n$. From this, we obtain

$$h_{|W|} + h_{(|X|+|Y'|-|W|)} < h_{|X|} + h_{|Y'|},$$

$$g_0 + (|W| - 1)g_1 + g_0 + (|X| + |Y'| - |W| - 1)g_1 < g_0 + (|X| - 1)g_1 + g_0 + (|Y'| - 1)g_1.$$

The aforementioned expression simplifies to $0 < 0$, which is a contradiction. This shows that if X and Y are different, then they cannot have more than one element.

Let us assume $g_0 = g_1$ and $|X| = |Y| = 1$. Let us suppose $X \ne Y$. Then, $X \cap Y = \emptyset$, so by the Csirmaz lemma we have

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

and consequently, $h_2 < 2h_1$ or equivalently $g_0 + g_1 < 2g_0$, which is a contradiction. □

Proposition 3.4. *If $X \in \min\Delta$, then for all $x, y \in X$, $x \ne y$, the blocks P_x and P_y are hierarchically independent in the access structure $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$.*

Proof. Let $X \in \min\Delta$ and let x and y be two different elements in X. Suppose $P_y \preccurlyeq P_x$, and consider a vertex vector $\bar{w}$ with basic set X and $w_x = g_0$. Setting $k \coloneqq |X|$ and applying Lemma 2.12 (2), we have $g_{k-1} > 0$ so $\operatorname{supp}(\bar{w}) = X$, in particular, $w_y > 0$, and by Lemma 3.2 (5), we obtain $\bar{w} \in \Gamma$. Thus, $\bar{w}' = \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \Gamma$. By Lemma 3.2 (4), there is $\bar{v} \in \min\Gamma$ such that $\bar{v} \le \bar{w}'$ and $\bar{v} \in \mathcal{B}(\operatorname{supp}(\bar{v})) \subseteq \Gamma$, so applying Lemma 2.7, we have $y \notin \operatorname{supp}(\bar{v}) \subsetneq X$, which contradicts the fact that $X \in \min\Delta$. □

Proposition 3.5. *If $X \in \min\Delta$, $1 \le k \coloneqq |X| \le m - 1$ and $g_k > 0$, then for every $y \in X$, the block P_y is not hierarchically inferior or equivalent to any block $P_x \ne P_y$ in the access structure $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$.*

Proof. Let $y \in X$ and let us suppose that $P_y \preccurlyeq P_x$ for some $x \in J$. By Proposition 3.4, we have $x \in J \setminus X$. Let us consider a vertex vector $\bar{w}$ with basic set X and $w_y = g_0$. Obviously, $\bar{w} \in \Gamma$ by Lemma 3.2 (5). Then, the vector $\bar{w}' \coloneqq \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$ also belongs to Γ.

By Lemma 3.2 (4), there exists a minimal authorized vector $\bar{v}$ such that $\bar{v} \le \bar{w}'$, $\bar{v} \in \mathcal{B}(\operatorname{supp}(\bar{v}))$ and $\operatorname{supp}(\bar{v}) \in \Delta$. If $g_0 > 1$, then Lemma 2.8 implies $\operatorname{supp}(\bar{v}) \subseteq X \setminus \{y\}$, but this contradicts the assumption $X \in \min\Delta$.

If $g_0 = 1$, then $g_0 = g_1 = g_k$, and by Lemma 2.8, we have $\operatorname{supp}(\bar{v}) \subseteq (X \setminus \{y\}) \cup \{x\}$. For $Y \in \min\Delta$ such that $Y \subseteq \operatorname{supp}(\bar{v})$, we have $X \cup Y \subseteq X \cup \{x\}$, so $|X \cup Y| \le k + 1$. Applying Lemma 3.3 yields $X = Y$ but $y \in X$ and $y \notin Y$, which is a contradiction. □

Lemma 3.6. *Let us assume that $X \in \min\Delta$ with $k \coloneqq |X|$, and there are $x, y \in J$, $x \ne y$ such that $|X \cup \{x, y\}| \ge 3$ and the blocks P_y and P_x are hierarchically comparable in the access structure Γ. Furthermore, we assume that $g_1 = g_k$ and $g_l > 0$ for certain $1 \le l < m$. If $X \cap \{x, y\} \ne \emptyset$ or $g_0 = g_1$, then $g_1 = g_l$.*

Proof. If $g_1 = 1$, then the claim is obvious.

Assume that $g_1 > 1$ and assume that this is not the case. Let l be the least positive integer that does not satisfy the claim. That means, $g_1 = g_{l-1} > g_l > 0$. Obviously, $k + 1 \leq l \leq m - 1$. This implies $k \leq m - 2$. Without loss of generality, we can assume that $P_y \preccurlyeq P_x$. By Proposition 3.5, we have $y \notin X$. Let now $Y \subseteq J$ be a set with $l + 1$ elements that contains $X \cup \{x, y\}$. Moreover, let us take an element $z \in X \setminus \{x, y\}$.

Let us consider a vertex vector $\bar{w}$ with basic set Y and $w_x = g_0$ and $w_z = g_l$. Obviously, $\mathrm{supp}(\bar{w}) = Y$, as $g_l > 0$. Under the aforementioned assumptions, $w_t = g_1$ for all $t \in Y \setminus \{x, z\}$; in particular, we have $w_y = g_1$. For every $0 < j \leq l$, we have

$$h_j = \sum_{i=0}^{j-1} g_i = g_0 + (j-1)g_1. \tag{5}$$

Let us note that $Y \in \Delta$ as $X \subseteq Y$. Hence, $\bar{w} \in \Gamma$ by Lemma 3.2 (5). Moreover, $h_{l+1} = |\bar{w}| = g_0 + (l-1)g_1 + g_l$. Since $P_y \preccurlyeq P_x$, we have $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \Gamma$. Let us note $\mathrm{supp}(\bar{w}') = Y$. Now by Lemma 3.2 (4), there exists a minimal authorized vector $\bar{v}$ such that $\bar{v} \leq \bar{w}'$, $\bar{v} \in \mathcal{B}(\mathrm{supp}(\bar{v}))$ and $W := \mathrm{supp}(\bar{v}) \in \Delta$. Lemma 2.7 implies $y \notin W$, i.e., $W \subseteq Y \setminus \{y\}$, so $|W| \leq l$. Let $Z \in \min\Delta$ such that $Z \subseteq W$.

Thus, $X \cup Z \subseteq X \cup W \subseteq Y \setminus \{y\}$, so $|X \cup Z| \leq l$ and applying Lemma 3.3 yields $X = Z$ or both X and W are singletons. If $X \cap \{x, y\} \neq \emptyset$, then $x, z \in X$, so X is not a singleton; thus, $X = Z$. If $g_0 = g_1$, then $X = Z$. Thus, in both cases, we have $z \in X = Z \subseteq W$, so applying Lemma 2.6 (1), we obtain $g_{|W|-1} \leq v_z$. Note also that $v_z \leq w'_z = w_z = g_l < g_{l-1} \leq g_{|W|-1}$, a contradiction that proves that $g_1 = g_l$. □

Proposition 3.7. *Let us assume that the height of $\mathcal{Z}$ equals $n \geq 3$. If there are $X \in \min\Delta$ such that $1 \leq |X| \leq n - 2$ and $x, y \in J \setminus X$ such that the blocks P_x and P_y are hierarchically comparable in the access structure Γ, then $g_0 = g_1 = \cdots = g_{n-1} > g_n = 0$.*

Proof. If $g_0 = 1$, then let us observe that

$$1 = h_1 = g_0 \geq g_1 \geq \cdots \geq g_{n-1} \geq 1.$$

Hence, $g_0 = g_1 = \cdots = g_{n-1} > g_n = 0$.

Thus, we assume $g_0 \geq 2$. If the blocks P_x and P_y are hierarchically comparable, then one can assume without loss of generality that $P_y \preccurlyeq P_x$. Let us consider a vertex vector $\bar{w}$ with basic set $X \cup \{y\}$ such that $w_y = g_0$. Obviously, by Lemma 3.2 (5), we have $\bar{w} \in \Gamma$. Then, the vector $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$ belongs to Γ. By Lemma 3.2 (4), there exists a minimal authorized vector $\bar{v}$ such that $\bar{v} \leq \bar{w}'$, $\bar{v} \in \mathcal{B}(\mathrm{supp}(\bar{v}))$ and $\mathrm{supp}(\bar{v}) \in \Delta$. By Lemma 2.8, we have $\mathrm{supp}(\bar{v}) \subseteq X$, but X is minimal in Δ, so $\mathrm{supp}(\bar{v}) = X$. Thus, we have

$$h_k = |\bar{v}| \leq |\bar{w}'_X| = |\bar{w}_X| = \sum_{i=1}^{k} g_i = h_{k+1} - g_0,$$

so $g_0 \leq h_{k+1} - h_k = g_k$. The sequence $\boldsymbol{g}$ is nonincreasing, so $g_0 = g_1 = \cdots = g_k$. Thus, we have shown that $g_1 = \ldots = g_k$. To complete the proof, it is enough to apply Lemma 3.6, assuming $l = n - 1$. □

Proposition 3.8. *Let us assume that the height of $\mathcal{Z}$ equals $n \geq 3$. If there are $X \in \min\Delta$ with $2 \leq |X| \leq n - 1$ and $x \in X$ and $y \in J \setminus X$ such that the blocks P_x and P_y are hierarchically comparable in the access structure Γ, then $g_1 = \cdots = g_{n-1} > g_n = 0$.*

Proof. If the blocks P_x and P_y are hierarchically comparable, then it follows from Proposition 3.5 that $P_y \preccurlyeq P_x$. Let us consider a vertex vector $\bar{w}$ with basic set $X \cup \{y\}$ such that $w_x = g_0$ and $w_y = g_1$. Obviously, $\bar{w} \in \Gamma$ by Lemma 3.2 (5). Then, also the vector $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$ belongs to Γ and $\mathrm{supp}(\bar{w}') \subseteq X \cup \{y\}$. Hence, by Lemma 3.2 (4), there is a minimal authorized vector $\bar{v}$, such that $\bar{v} \leq \bar{w}'$, $\bar{v} \in \mathcal{B}(\mathrm{supp}(\bar{v}))$, and $Y := \mathrm{supp}(\bar{v}) \in \Delta$. Let us observe $Y \subseteq \mathrm{supp}(\bar{w}') \subseteq X \cup \{y\}$.

By Lemma 2.7, we have $y \notin Y$ that shows $Y \subseteq X$, but X is minimal in Δ, so $Y = X$. Thus, we have

$$h_k = |\bar{v}| \le g_0 + \sum_{i=2}^{k} g_i = h_{k+1} - g_1,$$

where $k \coloneqq |X|$. Hence, $g_1 \le h_{k+1} - h_k = g_k$ and $g_1 = g_k$ as the sequence $\boldsymbol{g}$ is nonincreasing. To complete the proof, it is enough to apply Lemma 3.6, assuming $l = n - 1$. □

Corollary 3.9. *Let n be the height of $\mathcal{Z}$. If there are $x, y \in J$ such that P_x and P_y are hierarchically comparable and $3 \le |X \cup \{x, y\}| \le n$ for a certain $X \in \min\Delta$, then $g_1 = g_{m-1}$. Moreover, if $X \cap \{x, y\} = \emptyset$, then $g_0 = g_1 = g_{m-1}$.*

Proof. Assuming with no loss of generality that $P_y \preccurlyeq P_x$, we obtain that $\{x, y\}$ is not contained in X, by Proposition 3.4, so $|X| \le n - 1$. Applying Proposition 3.5 yields $y \notin X$. If $x \in X$, then $2 \le |X| \le n - 1$, and applying Proposition 3.8 yields $g_1 = g_{n-1} > g_n = 0$. If $x \notin X$, in particular $|X| = 1$, then applying Proposition 3.7 yields $g_0 = g_1 = g_{n-1} > g_n = 0$.

Suppose, contrary to our claim, that $n < m$. Then, there is a subset $Z \subseteq J$ such that $|Z| = n + 1$ and $X \cup \{x, y\} \subseteq Z$. Let us choose $z \in X \setminus \{x, y\}$ and denote $Z' = Z \setminus \{z\}$. Lemma 2.12 (1) implies that the set Z' belongs to Δ but it is not minimal as $x, y \in Z'$. So there is $Y \in \min\Delta$ such that $Y \subsetneq Z'$. Applying again Proposition 3.5, we obtain $y \notin Y$, so $X \cup Y \subseteq Z \setminus \{y\}$; thus, $|X \cup Y| \le n$. If $|X| > 2$, then we can apply Lemma 3.3 to obtain $X = Y \subseteq Z'$, which is a contradiction as $z \in X$ but $z \notin Z'$. If $|X| = 1$, then $X \cap \{x, y\} = \emptyset$, and by Proposition 3.7, we have $g_0 = g_1$, and applying again Lemma 3.3 yields $X = Y \subseteq Z'$, a contradiction as mentioned earlier. This completes the proof. □

Corollary 3.10. *Any multipartite access structure determined by uniform polymatroid $\mathcal{Z}$ does not admit hierarchically equivalent blocks unless the height of $\mathcal{Z}$ is 1 or $g_0 = \cdots = g_{m-1}$.*

Proof. It is shown in Example 3.1 that all blocks are hierarchically equivalent in any access structure determined by a uniform polymatroid with height 1. Let $n \ge 2$ be the height of $\mathcal{Z}$ and suppose that there are $x, y \in J$ such that P_x and P_y are hierarchically equivalent. Let us consider a subset $X \subseteq J$ such that $x, y \in X$ and $|X| = n$. Lemma 2.12 (1) and Proposition 3.4 imply that $X \in \Delta$ but X is not minimal, so there is $Y \in \min\Delta$ such that $Y \subsetneq X$. By Proposition 3.5 $x, y \notin Y$. If $n = 2$, then $Y = \emptyset$, which is a contradiction. Hence, we obtain $n \ge 3$ and $3 \le |Y \cup \{x, y\}| \le n$, and applying Corollary 3.9 yields $g_0 = g_{m-1}$. □

4 Hierarchical preorder determined by access structure

In this section, we present some properties of the access structure $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ depending on conditions imposed on $\mathcal{Z}$ and Δ. Theorem 4.1 states that Γ is connected if the increment sequence of $\mathcal{Z}$ is not constant. Assuming that $g_1 > g_{m-1}$, we prove in the next two theorems that the structures are compartmented provided that the height of the polymatroid is maximal or the family Δ does not contain any singleton (Theorems 4.2 and 4.3). Theorems 4.6, 4.8, 4.9, and 4.11 contain complete descriptions of $\Gamma(\Pi, \mathcal{Z}, \Delta)$ in the following cases: the height of the polymatroid is equal to 2, $g_1 = g_{m-1} > 0$ and Δ is generated by a singleton. The section ends with Theorem 4.12 stating that each $<$-preorder chain in the access structures defined by a uniform polymatroid has at most two elements.

Theorem 4.1. *Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ and let $\boldsymbol{g} = (g_i)_{i \in I_m}$ be the increment sequence of a uniform polymatroid $\mathcal{Z}$. If $g_0 > g_{m-1}$, then the access structure $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ is connected.*

Proof. Given $x \in J$, we want to show that there is $\bar{w} \in \min\Gamma$ such that $w_x \ne 0$. If there is $X \in \min\Delta$, $x \in X$, and $i \coloneqq |X|$, then $g_{i-1} > 0$ by Lemma 2.12 (2). It is easy to see that any vertex vector $\bar{w}$ with basic set X belongs to $\min\Gamma$ and $w_x \ne 0$. Now, we assume that $x \notin X$ for all $X \in \min\Delta$. Let us denote $l \coloneqq \min\{i \in I_m : g_0 > g_i\}$. By

assumption, $l \le m-1$. Let us take $X \in \min\Delta$ such that $k := |X| = \mu(\Delta)$ and consider $Y \subseteq J$ such that $|Y| = \max\{k, l\} + 1$ and $\{x\} \cup X \subseteq Y$. Let $\bar{w}$ be a vertex vector with basic set Y such that $w_x = g_0$ and $w_y = g_l$ for a certain $y \in X$. Lemma 3.2 (5) implies that $\bar{w} \in \Gamma$ as $Y \in \Delta$. Thus, there is $\bar{v} \in \min\Gamma$ such that $\bar{v} \le \bar{w}$. Since $\mathrm{supp}(\bar{v}) \in \Delta$, there is $W \in \min\Delta$ such that $W \subseteq \mathrm{supp}(\bar{v})$. By assumption, $x \notin W$, so $W \subseteq Y\setminus\{x\}$.

It turns out that $W = X$. Indeed, if $k \ge l$, then $Y\setminus\{x\} = X$, and by the minimality of X in Δ, we have $W = X$. For the case $k < l$, we have $l \ge 2$, $g_0 = g_1$, and $X \cup W \subseteq Y\setminus\{x\}$; thus, $|X \cup W| \le l$, and consequently, $X = W$ by Lemma 3.3.

If $g_l = 0$, then $v_y \le w_y = g_l = 0$, i.e., $y \notin \mathrm{supp}(\bar{v})$, which contradicts the fact that $y \in X = W \subseteq \mathrm{supp}(\bar{v})$.

If $g_l \ne 0$ and $v_x \ne 0$, then we have the claim. Let us suppose $v_x = 0$, i.e., $x \notin \mathrm{supp}(\bar{v})$. Thus, for $Z = \mathrm{supp}(\bar{v})$, we have

$$h(Z) = |\bar{v}_Z| = \sum_{z\in Z} v_z \le \sum_{z\in Z} w_z = w_y + \sum_{z\in Z\setminus\{y\}} w_z = \sum_{z\in (Z\cup\{x\})\setminus\{y\}} w_z - (w_x - w_y)$$

$$= |\bar{w}_{(Z\cup\{x\})\setminus\{y\}}| - (w_x - w_y) \le h((Z\cup\{x\})\setminus\{y\}) - (g_0 - g_l) < h(Z),$$

which is a contradiction as $|Z| = |(Z \cup \{x\})\setminus\{y\}|$ and $g_0 - g_l > 0$. □

This theorem shows that the access structures determined by uniform polymatroids are connected except for the ones in the column D of Table 1.

Theorem 4.2. *Let $\boldsymbol{g} = (g_i)_{i\in I_m}$ be the increment sequence of a uniform polymatroid $\mathcal{Z}$ and let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$. If $m \ge 3$ and $g_1 > g_{m-1} > 0$ and $\min\Delta \ne \{\{x\}\}$ for any $x \in J$, then the access structure Γ is compartmented.*

Proof. Let us suppose that there are $x, y \in J$ such that the blocks P_x and P_y are hierarchically comparable. According to Proposition 3.4, no minimal set in Δ can contain both x and y, so $|X| \le m-1$ for every $X \in \min\Delta$. By assumption, the height of $\mathcal{Z}$ equals m. If $x, y \notin X$ for a certain $X \in \min\Delta$, then by Proposition 3.7, we obtain $g_0 = g_1 = \ldots = g_{m-1}$, a contradiction.

If does not exist any set X in $\min\Delta$ such that $x, y \notin X$, then without loss of generality, we can assume that $x \in X$ and $y \notin X$ for a certain $X \in \min\Delta$. If $|X| \ge 2$, then by proposition 3.8, we obtain $g_1 = \ldots = g_{m-1}$, which is a contradiction again. If $|X| = 1$, then $\min\Delta = \{\{x\}\}$, as otherwise both x and y would be outside a certain minimal set in Δ, but this is not the case now. □

Let us note that if $g_{m-1} > 0$, then the aforementioned theorem implies that the appearance of non-compartmented access structure can be expected in the first row or in the last column of Table 1. In the next

Table 1: Hierarchical (pre)orders of access structures obtained form uniform polymatroids

		A	B	C	D
	$\boldsymbol{g}$ / Δ	$g_{m-1}=0$		$g_{m-1}>0$	
		$g_1=0$	$g_1>0$	$g_1>g_{m-1}$	$g_1=g_{m-1}$
1	$\mu(\Delta)=1$ $\lvert\min\Delta\rvert=1$	–		H	H
2	$\mu(\Delta)=1$ $\lvert\min\Delta\rvert>1$	T	$C\,\&\,H$	C	H
3	$\mu(\Delta)>1$	–	C	C	$C\,\&\,H$

T: Threshold; C: Compartmented; H: Hierarchical.

theorem, we shall prove that the access structures that appear in the last row of Table 1 are compartmented excluding the cells A3 and D3.

Theorem 4.3. *Let $\boldsymbol{g} = (g_i)_{i\in I_m}$ be the increment sequence of a uniform polymatroid $\mathcal{Z}$ and let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$. If $m \geq 3$ and $g_1 > g_{m-1}$ and $k \coloneqq \mu(\Delta) > 1$, then the access structure Γ is compartmented.*

Proof. Suppose to the contrary that Γ is not compartmented, i.e., there are two blocks that are hierarchically comparable. For simplicity, we assume $P_y \preccurlyeq P_x$ for certain $x, y \in J$ and $x \neq y$. By Proposition 3.4, no set in $\min\Delta$ contains both x and y; in particular, there is a subset of J with k elements that do not belong to $\min\Delta$. This and Lemma 2.12 (1) imply $g_k > 0$. Let n be the height of $\mathcal{Z}$. Obviously, $2 \leq k < n \leq m$ and $g_n = 0$. Proposition 3.5 implies $y \notin X$ for every $X \in \min\Delta$ with $|X| \leq n-1$.

If there exists $X \in \min\Delta$ such that $|X| = k$ and $x \in X$, then $3 \leq |X \cup \{x, y\}| = k+1 \leq n$. Now, we assume that $x \notin X$ for every $X \in \min\Delta$ with $|X| = k$. Suppose $g_{k+1} = 0$. Let us fix $X \in \min\Delta$ with $|X| = k$ and $z \in X$. Let us consider $Z \coloneqq (X\setminus\{z\}) \cup \{x, y\}$. From Lemma 2.12 (1), we have $Z \in \Delta$ as $|Z| = k+1$. By Proposition 3.4, the set Z cannot be minimal as it contains $\{x, y\}$, so there is $Y \in \min\Delta$ such that $Y \subsetneq Z$, and hence, $|Y| = k$. Obviously, $x, y \notin Y$, which implies $Y \subseteq X\setminus\{z\}$, a contradiction. This shows that $g_{k+1} > 0$, so $k+1 < n$. Thus, we have $4 \leq |X \cup \{x, y\}| = k+2 \leq n$ for arbitrary $X \in \min\Delta$ with $|X| = k$.

In both cases, we can apply Corollary 3.9, which implies $g_1 = g_{m-1}$, which is a contradiction. This completes the proof. □

The following table presents a general arrangement of multipartite access structure determined by monotone increasing families contained in $\mathcal{P}(J)\setminus\{\varnothing\}$ and uniform polymatroids. The cells A1, B1, and A3 do not contain any objects since the suitable monotone increasing families and polymatroids are not compatible. A monotone increasing family, which is not compatible with given polymatroid, can occur in every cell of the table. A complete overview of hierarchical orders of all access structure obtained from uniform polymatroids with $m = 4$ can be found in Table A1.

To describe the hierarchical order determined by an access structure Γ in a partition Π of the set of participants P, we introduce the following notations $\mathrm{Ord}(Y, X)$ and $\mathrm{Ord}^*(Y, X)$, which are defined as follows.

Definition 4.4. Let $\Pi = (P_x)_{x\in J}$ be a partition of the set P and let Y and X be two disjoint subsets of J. The hierarchical preorder $\preccurlyeq$ in Π is said to be of type $\mathrm{Ord}(Y, X)$ if

$$P_y \preccurlyeq P_x \Leftrightarrow (x = y \quad \text{or} \quad (y \in Y \quad \text{and} \quad x \in X)).$$

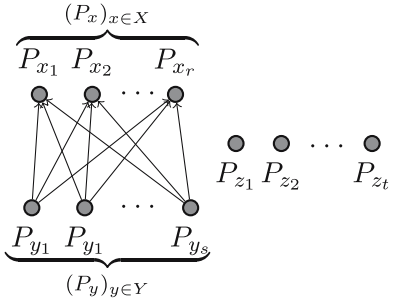
In particular, no different blocks are hierarchically equivalent, i.e., $\preccurlyeq$ is an order. Moreover, if X or Y is empty, then the order $\mathrm{Ord}(Y, X)$ is compartmented.

Definition 4.5. Let $\Pi = (P_x)_{x\in J}$ be a partition of the set P and let X and Y be two disjoint subsets of J. The hierarchical preorder $\preccurlyeq$ in Π is said to be of type $\mathrm{Ord}^*(Y, X)$ if

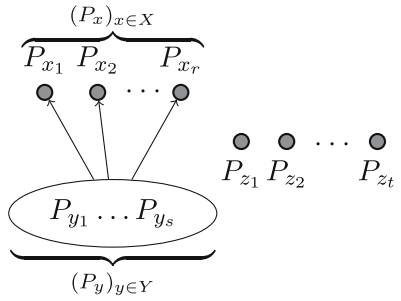
$$P_y \preccurlyeq P_x \Leftrightarrow (x = y \quad \text{or} \quad x, y \in Y \quad \text{or} \quad (y \in Y \quad \text{and} \quad x \in X)).$$

The preorder $\mathrm{Ord}^*(Y, X)$ is not an order (unless $|Y| \leq 1$). In particular, P_x and P_y are hierarchically equivalent whenever $x, y \in Y$, but no different blocks P_x and P_y with $x, y \in J\setminus Y$ are hierarchically equivalent.

One can note that if the set Y is empty, then every two blocks are hierarchically independent in the preorder $\mathrm{Ord}^*(\varnothing, X)$. If the set X is empty, then we obtain $\mathrm{Ord}^*(Y, \varnothing)$, which means each two blocks are hierarchically equivalent (cf. Example 3.1). Noteworthy is also the observation that if $|Y| \leq 1$, then $\mathrm{Ord}(Y, X) = \mathrm{Ord}^*(Y, X)$. The defined preorders can be presented in the form of the following Hasse diagrams.



Order of the type $Ord(Y, X)$.



Preorder of the type $Ord^*(Y, X)$.

Now, we want to describe the hierarchical orders of multipartite access structures determined by some special type of uniform polymatroids. In Example 3.1, we considered the case of polymatroids with height 1. We will now deal with polymatroids $\mathcal{Z} = (J, h, \boldsymbol{g})$ of height equal to 2, i.e., $g_0 \geq g_1 > g_2 = 0$. The result presented in the following refers to some access structures in the column B of Table 1.

Theorem 4.6. *Let $\mathcal{Z} = \mathcal{Z}(\Pi) = (J, h, \boldsymbol{g})$ be a uniform polymatroid with the increment sequence $\boldsymbol{g} = (g_i)_{i\in I_m}$ such that the height of $\mathcal{Z}$ is equal to* 2.

- *If $g_0 > g_1$, then a monotone increasing family $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$ is compatible with the polymatroid $\mathcal{Z}$ if and only if there is a subset $X \subseteq J$ such that* $\min\Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J\backslash X)$.
- *If $g_0 = g_1$, then a monotone increasing family $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$ is compatible with the polymatroid $\mathcal{Z}$ if and only if there is a subset $X \subseteq J$, $|X| \leq 1$ such that* $\min\Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J\backslash X)$.
- *Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ be the access structure determined by the polymatroid $\mathcal{Z}$ and the monotone increasing family $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$ such that* $\min\Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J\backslash X)$ *for some $X \subseteq J$, then the hierarchical order induced by Γ on the set Π is of the type* $\mathrm{Ord}(J\backslash X, X)$.

Proof. (1) and (2). (⇒). If the monotone increasing family Δ is compatible with the polymatroid $\mathcal{Z}$, then Lemma 2.12 (1) and the assumptions $g_2 = 0$ shows that all subsets of J with two elements belong to Δ. Thus, all sets in $\min\Delta$ have one or two elements. Let $X \subseteq J$ denote the collection of those elements that form single-element minimal sets. Hence, the remaining sets in $\min\Delta$ have two elements and do not contain any elements belonging to X. Therefore, $\min\Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J\backslash X)$. If $g_0 = g_1$, then it follows from Lemma 3.3 that $|X| \leq 1$.

(1) and (2). (⇐). To show the reverse implication, consider the monotone increasing family Δ such that $\min\Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J\backslash X)$ for some $X \subseteq J$. Let us recall that every set with two elements belongs to Δ. It is easy to see that $h(Y) = g_0 + g_1$ for all $Y \subseteq J$ with $|Y| \geq 2$. We shall apply the Csirmaz lemma. If $W \subseteq Y \subseteq J$ such that $W \notin \Delta$ and $Y \in \Delta$, then $W = \varnothing$ and $|Y| \geq 1$ or $|W| = 1$ and $|Y| \geq 2$. In the former case, we have $0 = h(W) < g_0 \leq h(Y)$, and in the latter case, $g_0 = h(W) < g_0 + g_1 = h(Y)$. Similarly, if $Y, Z \in \Delta$ and $W = Y \cap Z \notin \Delta$, then $|W| \leq 1$. If $|W| = 1$, then $|Y|, |Z| \geq 2$. Hence,

$$h(W) + h(Y \cup Z) = g_0 + (g_0 + g_1) < (g_0 + g_1) + (g_0 + g_1) = h(Y) + h(Z).$$

Now, we assume $W = \varnothing$, so $|Y \cup Z| \geq 2$ and $|Y|, |Z| \geq 1$. If $g_0 > g_1$, then

$$h(Y \cup Z) = g_0 + g_1 < g_0 + g_0 \leq h(Y) + h(Z).$$

In case $g_0 = g_1$, we assumed that there is at most one singleton in Δ, so $|Y| > 1$ or $|Z| > 1$. Hence,

$$h(Y \cup Z) = g_0 + g_1 < g_0 + g_0 + g_1 \leq h(Y) + h(Z).$$

Thus, both conditions of the Csirmaz lemma are satisfied, which completes the proof of (1) and (2).

(3) If $X = \emptyset$, then $\mu(\Delta) = 2$. For $m = 2$, we have $\Delta = \{J\}$, and by Proposition 3.4, the blocks P_x and P_y are hierarchically independent, so Γ is compartmented. Assuming $m \geq 3$, we can apply Theorem 4.3 and we conclude that the obtained access structure is compartmented, i.e., $\mathrm{Ord}(J, \emptyset)$.

We now turn to the case $X \neq \emptyset$. By assumption $\{x\} \in \min\Delta$ for all $x \in X$, so applying Proposition 3.5, we see that P_x cannot be hierarchically inferior or equivalent to any other P_z. In particular, P_x and P_y are mutually hierarchically independent whenever $x, y \in X$ and $x \neq y$. If $x, y \in J\setminus X$, then $\{x, y\} \in \min\Delta$, so P_x and P_y are hierarchically independent by Proposition 3.4. In particular, if $X = J$, then we obtain the compartmented order $\mathrm{Ord}(\emptyset, J)$.

It remains to show that $P_y \prec P_x$ for $x \in X$ and $y \in J\setminus X$ with $\emptyset \subsetneq X \subsetneq J$. Let $\bar{w}$ be a minimal vector in Γ such that $w_y \neq 0$. If such a vector does not exist, then the block P_y is redundant so $P_y \prec P_x$. Otherwise, applying Lemma 3.2 (3) yields $\bar{w} \in \mathcal{B}(\mathrm{supp}(\bar{w}))$ and $\mathrm{supp}(\bar{w}) \in \Delta$. Note that $\{y\} \notin \min\Delta$, so $|\mathrm{supp}(\bar{w})| \geq 2$. According to equation (3), we obtain $\bar{w} \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(\bar{w})) \subseteq \mathcal{B}(\mathcal{Z}, J)$. Lemma 2.9 shows that $\bar{w}' \coloneqq \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \mathcal{B}(J)$ or there exist a set $Y \subseteq J\setminus\{y\}$, $x \in Y$ and a vector $\bar{v} \in \mathcal{B}(\mathcal{Z}, Y)$, such that $\bar{v} \leq \bar{w}'$. In the first case, we have $\bar{w}' \in \Gamma$ by Lemma 3.2 (1). If the second case occurs, then we note that $\{x\} \subseteq Y \in \Delta$, so from Lemma 3.2 (1), we obtain $\bar{v} \in \Gamma$; hence, $\bar{w}' \in \Gamma$. This proves that $P_y \prec P_x$. In this way, we showed that the order on the set $(\Pi, \preccurlyeq)$ is of the type $\mathrm{Ord}(J\setminus X, X)$. □

Remark 4.7. The aforementioned theorem combined with Example 3.1 is strong enough to classify all bipartite access structure determined by uniform polymatroids with $m = 2$. If the polymatroid height is equal to 1, then we have a threshold access structure (cf. Example 3.1). If the polymatroid height is equal to 2, then we consider three monotone increasing families $\Delta_1 = \{\{x\}, J\}$, $\Delta_2 = \{\{x\}, \{y\}, J\}$, and $\Delta_3 = \{J\}$ of subsets of $J \coloneqq \{x, y\}$. Let us note that $\Delta_1' = \{\{y\}, J\}$ is hierarchically equivalent to Δ_1 as it can be obtained by the permutation of x and y. It is easy to see that Δ_1 is compatible with every polymatroid $(J, h, \boldsymbol{g})$ with $g_1 > 0$ and the resulting access structures induce on $\{P_x, P_y\}$ the order of the type $\mathrm{Ord}(\{y\}, \{x\})$. Moreover, Δ_2 is not compatible with a polymatroid such that $g_0 = g_1$ but in the remaining cases, the resulting access structures are compartmented.

The following theorem describes the hierarchy on the access structures determined by uniform polymatroids with $g_0 = g_1 = \cdots = g_{m-1} > 0$. This result corresponds to the access structures that appear in the column D of Table 1.

Theorem 4.8. *Let $\mathcal{Z} = (J, h, \boldsymbol{g})$ be a uniform polymatroid with $m \coloneqq |J| \geq 3$ and the increment sequence $\boldsymbol{g} = (g_i)_{i \in I_m}$ such that $g_0 = g_{m-1} > 0$.*

(1) *A monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\emptyset\}$ is compatible with the polymatroid $\mathcal{Z}$ if and only if* $\min\Delta = \{X\}$ *for a certain $\emptyset \neq X \subseteq J$.*

(2) *Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ be the access structure determined by the polymatroid $\mathcal{Z}$ and the monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\emptyset\}$ such that* $\min\Delta = \{X\}$ *for a certain $\emptyset \neq X \subseteq J$, then*

(2*a*) *The vector $\sum_{x \in X} g_0 \bar{e}^{(x)}$ is the only minimal authorized vector in the access structure Γ.*

(2*b*) *The hierarchical preorder induced by Γ on the set Π is of the type* $\mathrm{Ord}^*(J\setminus X, X)$.

Proof. (1) Since $g_0 = g_{m-1}$, i.e., the height of $\mathcal{Z}$ is equal to m, we can apply Lemma 3.3, which implies that if Δ is compatible with the polymatroid $\mathcal{Z}$, then $\min\Delta$ contains only one set. To prove the reverse implication, it is enough to apply Lemma 2.13.

(2a) We apply Lemma 2.6 (1) for an arbitrary $Y \in \Delta$ and an arbitrary $\bar{w} \in \mathcal{B}(Y)$. For $l \coloneqq |Y|$, we have $h_1 \geq w_z \geq g_{l-1} = g_0 = h_1$, and consequently, $w_z = h_1 = g_0$ for every $z \in Y$. Since $X \subseteq Y$, so $\bar{w} \geq \sum_{x \in X} g_0 \bar{e}^{(x)}$ for every set $Y \in \Delta$ and for every vector $\bar{w} \in \mathcal{B}(Y)$. This shows that the vector $\sum_{x \in X} g_0 \bar{e}^{(x)}$ is the only minimal authorized vector.

(2b) According to Proposition 3.4, the blocks indexed by the elements in X are hierarchically independent. In particular, if $X = J$, then the hierarchical order on Π induced by Γ is of the type $\mathrm{Ord}^*(\emptyset, J)$.

Now, we assume $|X| < m$. It is shown above that $\sum_{x\in X} g_0 \bar{e}^{(x)}$ is the only minimal authorized vector, so all the blocks P_y with $y \notin X$ are redundant. In particular, they are mutually hierarchically equivalent and every block $P_x, x \in X$ is hierarchically superior but not equivalent to $P_y, y \in J\setminus X$, which follows from Proposition 3.5. Moreover, all blocks in $\{P_x : x \in X\}$ are hierarchically independent by Proposition 3.4. We conclude that the hierarchical order of Π induced by Γ is of the type $\mathrm{Ord}^*(J\setminus X, X)$. □

Now, we shall prove a similar theorem that describes the hierarchical order of access structures determined by uniform polymatroids with $g_0 > g_1 = \cdots = g_{m-1} > 0$ and monotone increasing families compatible with them. This theorem describes access structures located in column D of Table 1.

Theorem 4.9. *Let $\mathcal{Z} = (J, h, \boldsymbol{g})$ be a uniform polymatroid with the increment sequence $\boldsymbol{g} = (g_i)_{i\in I_m}$ such that $m := |J| \geq 3$ and $g_0 > g_1 = g_{m-1} > 0$.*

(1) *A monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ is compatible with $\mathcal{Z}$ if and only if $\min\Delta = \{X\}$ for a certain $X \subseteq J$ or $\min\Delta = \mathcal{P}_1(J)$.*

(2) *Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ be the access structure determined by the polymatroid $\mathcal{Z}$ and the monotone increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$. Then,*

(2a) *If $\min\Delta = \{X\}$ for a certain $\varnothing \neq X \subseteq J$, then the hierarchical order induced by Γ on Π is of the type $\mathrm{Ord}(J\setminus X, X)$.*

(2b) *If $\min\Delta = \mathcal{P}_1(J)$, then the hierarchical order induced by Γ on Π is of the type $\mathrm{Ord}(\varnothing, J)$.*

Proof. (1) Let us assume that Δ is compatible with $\mathcal{Z}$. It is enough to consider the case where Δ has at least two different minimal sets. From the assumption $g_{m-1} > 0$, we have that the height of $\mathcal{Z}$ is equal to m, so applying Lemma 3.3, we conclude that those sets must be singletons. Let $\{x\}, \{y\} \in \min\Delta$ for some $x, y \in J$. Suppose that there is $z \in J$ such that $\{z\} \notin \min\Delta$. Of course, $\{x, z\}, \{y, z\} \in \Delta$, but $\{x, z\} \cap \{y, z\} = \{z\} \notin \Delta$. Using the Csirmaz lemma yields

$$h(\{z\}) + h(\{x, y, z\}) < h(\{x, z\}) + h(\{y, z\}).$$

Hence, we obtain $h_3 - h_2 < h_2 - h_1$, and consequently, $g_2 < g_1$, which is a contradiction, so every singleton belongs to $\min\Delta$. To show the reverse implication, let us consider two cases:

If $\min\Delta = \{X\}$ for some $X \subseteq J$, then we refer to Lemma 2.13.

If $\min\Delta = \mathcal{P}_1(J)$, then the claim it follows from Lemma 2.14.

(2a) Assume $\min\Delta = \{X\}$ for some $\varnothing \neq X \subseteq J$. The fact that P_x and P_y are hierarchically independent for arbitrary $x, y \in X$, $x \neq y$ is obtained directly from Proposition 3.4. In particular, if $X = J$, then the ordered set $(\Pi, \preccurlyeq)$ is of the type $\mathrm{Ord}(\varnothing, J)$.

Now, we assume that $|X| < m$. Consider $x \in X$ and $y \notin X$. According to Proposition 3.5, the blocks P_y and P_x are hierarchically independent or $P_y \prec P_x$. We shall show that $P_y \preccurlyeq P_x$.

Let us assume that $\bar{w}$ is an arbitrary minimal vector in Γ such that $w_y \neq 0$. The existence of such vectors is ensured by Theorem 4.1. Then, from Lemma 3.2 (3), we have $\bar{w} \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(\bar{w}))$ and $\mathrm{supp}(\bar{w}) \in \Delta$, so $X \subseteq \mathrm{supp}(\bar{w})$, in particular, $x \in \mathrm{supp}(\bar{w})$. Note that $k := |\mathrm{supp}(\bar{w})| \geq 2$, because $y, x \in \mathrm{supp}(\bar{w})$. According to Lemma 2.6 (1), we obtain $w_y \geq g_{k-1}$. By assumption, we have $g_{k-1} = g_1$; hence, we can consider two cases:

(i) $w_y = g_1$, so according to Lemma 2.6 (2), we have $\bar{v} := \bar{w} - w_y\bar{e}^{(y)} \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(\bar{w})\setminus\{y\})$, but $X \subseteq \mathrm{supp}(\bar{w})\setminus\{y\}$, so from Lemma 3.2 (1), we obtain $\bar{v} \in \Gamma$. Then, of course, $\bar{v} \leq \bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)}$, so $\bar{w}' \in \Gamma$.

(ii) $w_y > g_1$ and denote $Y := \mathrm{supp}(\bar{w})$. According to Lemma 2.9, we obtain $\bar{w}' := \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \mathcal{B}(\mathcal{Z}, Y)$ or there is a set $Z \subseteq Y\setminus\{y\}$, $x \in Z$ such that $\bar{v} := \bar{w}_Z \in \mathcal{B}(\mathcal{Z}, Z)$. In particular, we have $|\bar{w}_Z| = |\bar{v}| = h_{|Z|}$. Let $Y = Z \cup W \cup \{y\}$ be the union of three disjoint sets, where $W = Y\setminus(Z \cup \{y\})$. Then, using Lemma 2.6 (1) and assumptions, we obtain that each coordinate of the vector $\bar{w}$ is at least g_1; hence,

$$h_{|Y|} = |\bar{w}| = |\bar{w}_Z| + |\bar{w}_W| + w_y > |\bar{v}| + |W|g_1 + g_1 = h_{|Z|} + |W|g_1 + g_1 = h_{|Y|},$$

where the last equality is obtained from equation (4) in the following way:

$$h_{|Y|} - h_{|Z|} = \sum_{i=0}^{|Y|-1} g_i - \sum_{i=0}^{|Z|-1} g_i = \sum_{i=|Z|}^{|Y|-1} g_i = |W|g_1 + g_1.$$

A contradiction we have obtained shows that $\bar{w}' \in \mathcal{B}(Y) \subseteq \Gamma$. In both of the aforementioned cases, we have received that $\bar{w}' \in \Gamma$. Since this holds for all $\bar{w} \in \min\Gamma$ with $w_y > 0$, we conclude $P_y \preccurlyeq P_x$.

It remains to show that P_y and P_x are hierarchically independent when $x, y \notin X$. If it were otherwise, then assuming $n \coloneqq m$ and applying Proposition 3.7, we would obtain $g_0 = g_1$ contrary to the assumption made here. In this way, we showed that the order on Π is of type $\mathrm{Ord}(J\setminus X, X)$.

(2b) Assume $\min\Delta = \mathcal{P}_1(J)$. If $P_y \preccurlyeq P_x$ for some $x, y \in J$, then P_y is hierarchically inferior or equivalent to P_x and $\{x\}, \{y\} \in \min\Delta$, which contradicts Proposition 3.5. In this way, we showed that the order on Π is of type $\mathrm{Ord}(\varnothing, J)$. □

Remark 4.10. The result of (2b) can be generalized to all monotone increasing families Δ with $\min\Delta = \mathcal{P}_k(J)$, where $k = 1, \ldots, m$. According to Lemma 2.14 (cf. [12, Lemma 6.1]) such Δ is compatible with a uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ if and only if $g_{k-1} > g_k$. Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$. If $k = 1$ and $g_1 > 0$, then Γ is compartmented by Proposition 3.5. If $k \geq 2$, then $\mu(\Delta) \geq 2$, so Γ is compartmented, which follows from Theorem 4.3. In both cases, the hierarchical order induced by Γ in Π is of the type $\mathrm{Ord}(\varnothing, J)$. A similar class, called uniform multipartite access structures, was also considered by Farràs et al. [12].

Another theorem describes the hierarchy of blocks in the access structures determined by polymatroids, for which $g_{m-1} > 0$ and monotone increasing families with one minimal set that contains exactly one element. This theorem deals with the existence and hierarchy of access structures placed in the first row of Table 1.

Theorem 4.11. *Let $\mathcal{Z} = (J, h, \boldsymbol{g})$ be a uniform polymatroid with the increment sequence $\boldsymbol{g} = (g_i)_{i \in I_m}$ and let $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ be a monotone increasing family such that* $\min\Delta = \{\{x\}\}$ *for a certain $x \in J$.*

(1) *Then, Δ is compatible with the polymatroid $\mathcal{Z}$ if and only if $g_{m-1} > 0$.*

(2) *Let $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ be the access structure determined by the polymatroid $\mathcal{Z}$ such that $g_{m-1} > 0$ and the monotone increasing family Δ. Then,*

(2a) *If $g_0 = g_{m-1}$, then the hierarchical order induced by Γ on Π is of the type* $\mathrm{Ord}^*(J\setminus\{x\}, \{x\})$.

(2b) *If $g_0 > g_{m-1}$, then the hierarchical order induced by Γ on Π is of the type* $\mathrm{Ord}(J\setminus\{x\}, \{x\})$.

Proof. (1) The fact that Δ is compatible with $\mathcal{Z}$ can be obtained from Lemma 2.13. Conversely, let us suppose that $g_{m-1} = 0$. Then, every subset of J with $m - 1$ elements belongs to Δ by Lemma 2.12 (1). But this contradicts the fact that $J\setminus\{x\} \notin \Delta$. This implies Δ is not compatible with $\mathcal{Z}$ whenever $g_{m-1} = 0$.

(2) We shall show that $P_y \prec P_x$ for every $y \in J\setminus\{x\}$. From Proposition 3.5, it follows that P_x is not hierarchically inferior to any block in Π so P_x is not hierarchically equivalent to any other block. Let us fix $y \in J$ and $y \neq x$. If $w_y = 0$ for every minimal vector $\bar{w} \in \Gamma$, then the block P_y is redundant, so $P_y \preccurlyeq P_x$. Let us assume that $\bar{w}$ is a minimal vector in Γ such that $w_y \neq 0$. Then, from Lemma 3.2 (3), we have $\bar{w} \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(\bar{w}))$ and $\mathrm{supp}(\bar{w}) \in \Delta$, so $x \in \mathrm{supp}(\bar{w})$. From Lemma 2.9, it follows that $\bar{w}' \coloneqq \bar{w} - \bar{e}^{(y)} + \bar{e}^{(x)} \in \mathcal{B}(\mathcal{Z}, \mathrm{supp}(\bar{w}))$ or there is a set $Y \subseteq \mathrm{supp}(\bar{w})\setminus\{y\}$, $x \in Y$ such that $\bar{v} \coloneqq \bar{w}_Y \in \mathcal{B}(\mathcal{Z}, Y)$. In the former case, we obtain $\bar{w}' \in \Gamma$ from Lemma 3.2 (1). If the latter case is fulfilled, then we note that $Y \in \Delta$, so from Lemma 3.2 (1), we obtain $\bar{v} \in \Gamma$ and $\bar{v} \leq \bar{w}'$. This means that in both cases, $\bar{w}' \in \Gamma$. Since this holds for all $\bar{w} \in \min\Gamma$ with $w_y > 0$, we conclude $P_y \preccurlyeq P_x$. This shows that the (pre)order on Π is of the type $\mathrm{Ord}^*(J\setminus\{x\}, \{x\})$ or $\mathrm{Ord}(J\setminus\{x\}, \{x\})$.

(2a) Since $g_0 = g_{m-1}$, applying Theorem 4.8 (2b) yields the claim.

(2b) If the preorder on Π were of the type $\mathrm{Ord}^*(J\setminus\{x\}, \{x\})$, then the blocks P_y and P_z would be hierarchically comparable for some $y, z \in J\setminus\{x\}$. This and Proposition 3.7, for $n = m$, imply $g_0 = g_1 = \cdots = g_{m-1}$. But this is a contradiction to $g_0 > g_{m-1}$, so the order on Π is of type $\mathrm{Ord}(J\setminus\{x\}, \{x\})$. □

The results in this chapter provide information about the hierarchy induced on the set of participants by various access structures contained in Table 1, except the cell B2. That area contains objects obtained from monotone increasing families $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$ with $\mu(\Delta) = 1$ and compatible polymatroids $\mathcal{Z} = (J, h, \boldsymbol{g})$ with the polymatroid height n such that $3 \le n \le m - 1$. Computer calculations show that this area contains both compartmented and hierarchical access structures, and some of them are different of those considered in the aforementioned theorems. Some examples can be seen in Table A1.

Every linearly ordered subset of a partially (pre)ordered set is called a *chain*. A chain that contains only one element is referred to as *trivial*. We assume that a chain in a partition of participants does not contain hierarchically equivalent blocks. Let us observe that every non-trivial chain of blocks in the access structures investigated earlier contains two blocks. The next theorem shows that all hierarchical access structures obtained from uniform polymatroids have this property.

Theorem 4.12. *Every chain in the hierarchical access structure determined by arbitrary uniform polymatroid contains one or two blocks.*

Proof. Let n denote the polymatroid height. For $n = 1$, i.e., $g_0 > g_1 = 0$, it follows from Example 3.1 that $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ is a threshold access structure, so all blocks of participants are mutually hierarchically equivalent; thus, every chain is trivial.

Suppose that $n \ge 2$ and Π contains a chain of blocks composed of three hierarchically non-equivalent blocks, i.e., $P_z < P_y < P_x$ for some $x, y, z \in J$. Let $X \subseteq J$ such that $|X| = n$ and $y, z \in X$. By Lemma 2.12 (1), we have $X \in \Delta$, but Proposition 3.4 implies that $X \notin \min\Delta$. Thus, there is $Y \subsetneq X$ such that $Y \in \min\Delta$, in particular, $|Y| < n$. If $n = 2$, then $|Y| = 1$, but neither $\{y\}$ nor $\{z\}$ is minimal in Δ, which follows from Proposition 3.5, a contradiction. If $n \ge 3$, then by Proposition 3.5, we know that $y, z \notin Y$. Thus, $|Y| \le n - 2$. Using Proposition 3.7, we obtain $g_0 = g_{n-1}$, and this combined with Corollary 3.9 shows that $g_0 = g_{m-1}$. Now from Theorem 4.8, we conclude that every chain in Π contains at most two blocks, which contradicts our assumption. □

The aforementioned theorem seems quite surprising, because for other polymatroids, one can construct hierarchical access structures with chains of arbitrary length. For instance, such objects can be found in [11–13,16] and others.

5 Ideal access structures obtained from uniform polymatroids

In this section, we shall prove that the access structures studied in Theorems 4.6, 4.8, 4.9, and 4.11 are not only κ-ideal, but actually ideal. To do this, we apply the method outlined in Remark 2.5 to show that all one point extensions of suitable uniform polymatroids are representable over sufficiently large finite fields. Then, it suffices to apply [10, Theorem 2.1, and Theorem 6.1]. In Theorems 5.1, 5.2, and 5.4, we prove, respectively, that if the height of polymatroid equals 2 or Δ is generated by a single element or $g_1 = \ldots = g_{m-1} > 0$, then the resulting access structures are ideal.

We begin by recalling Example 3.1 where we noted that every uniform polymatroid with height 1 determines a threshold access structure, which is known to be ideal as it is realized by the Shamir threshold secret sharing scheme. Now, we shall consider the case of polymatroids with height equals 2.

Theorem 5.1. *All access structures determined by any uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ with height equals 2 are ideal.*

Proof. The assumption implies $g_0 \ge g_1 > g_2 = 0$. Let $\Delta \subseteq \mathcal{P}(J)\backslash\{\varnothing\}$ be a monotone increasing family compatible with $\mathcal{Z}$. It is enough to show that the one point extension $\mathcal{Z}'$ of $\mathcal{Z}$ induced by Δ is a representable polymatroid. Let $\mathbb{K}$ be a finite field with $q := |\mathbb{K}| > m$. By an abuse of notation, we will use θ to denote the zero vector in any vector space $\mathbb{K}^n$. Let us consider a collection $(a_x)_{x\in J}$ of pairwise different non-zero elements of $\mathbb{K}$. For every

$x \in J$, we define $V_x \coloneqq \{(a, a_x a) : a \in \mathbb{K}^{g_1}\}$. It easy to check that V_x is a vector subspace of $\mathbb{K}^{g_1} \times \mathbb{K}^{g_1}$ and $\dim V_x = g_1$. Assume $x \neq y$ and $(a_1, a_2) \in V_x \cap V_y$. Hence, $a_2 = a_x a_1$ and $a_2 = a_y a_1$, so $\theta = a_x a_1 - a_y a_1 = (a_x - a_y)a_1$. Since $a_x - a_y \neq 0$, so $a_1 = \theta$. This shows $V_x \cap V_y = \{\theta\}$. Hence, $\dim(V_x + V_y) = \dim V_x + \dim V_y - \dim(V_x \cap V_y) = \dim V_x + \dim V_y = 2g_1$. In particular, $V_x + V_y = \mathbb{K}^{g_1} \times \mathbb{K}^{g_1}$ for all $x, y \in J, \quad x \neq y$. Thus, $(V_x)_{x \in J}$ is a vector space representation of the polymatroid $\mathcal{Z}$ provided $g_0 = g_1$. According to Theorem 4.6 (2), we have two cases. If $\min\Delta = \{\{x\}\} \cup \mathcal{P}_2(J \setminus \{x\})$, then we take $\theta \neq \beta \in V_x$. For a certain $x_0 \notin J$, we define $V_{x_0} \coloneqq \operatorname{span}(\beta)$. It is easily seen that $(V_x)_{x \in J \cup \{x_0\}}$ is a vector space representation of $\mathcal{Z}'$ induced by Δ.

If $\min\Delta = \mathcal{P}_2(J)$, then we take $\beta \in \mathbb{K}^{g_1} \times \mathbb{K}^{g_1} \setminus \bigcup_{x \in J} V_x$. It is possible as $|\bigcup_{x \in J} V_x| \leq mq^{g_1} < q^{g_1+1} \leq q^{2g_1} = |\mathbb{K}^{g_1} \times \mathbb{K}^{g_1}|$. Now, we define $V_{x_0} \coloneqq \operatorname{span}(\beta)$. It is easily seen that $(V_x)_{x \in J \cup \{x_0\}}$ is a vector space representation of $\mathcal{Z}'$ induced by Δ.

Now, we assume $g_0 > g_1$ and define $U_x \coloneqq \mathbb{K}^{g_0 - g_1} \times V_x \subseteq \mathbb{K}^{g_0 - g_1} \times \mathbb{K}^{g_1} \times \mathbb{K}^{g_1}$ for every $x \in J$. For simplicity of notation, the vector space $\mathbb{K}^{g_0 - g_1} \times \mathbb{K}^{g_1} \times \mathbb{K}^{g_1}$ will be identified with $\mathbb{K}^{g_0 + g_1}$. It is clear that $\dim U_x = g_0$. Moreover, $U_x + U_y = (\mathbb{K}^{g_0 - g_1} \times V_x) + (\mathbb{K}^{g_0 - g_1} \times V_y) = \mathbb{K}^{g_0 + g_1}$ and $U_x \cap U_y = \mathbb{K}^{g_0 - g_1} \times \{\theta\} \times \{\theta\}$. In particular, $\varepsilon \coloneqq (1, 0, \ldots, 0) \in U_x$ for all $x \in J$.

If Δ is compatible with $\mathcal{Z}$, then by Theorem 4.6.1, there is $X \subseteq J$ such that $\min\Delta = \mathcal{P}_1(X) \cup \mathcal{P}_2(J \setminus X)$.

To explain the general idea of the next step of the proof, we use projective geometry. Every subspace U_x can be considered as $(g_0 - 1)$-dimensional subspace of the projective space of dimension $g_0 + g_1 - 1$. The projective point $E \coloneqq \operatorname{span}(\varepsilon)$ belongs to the intersection of all subspaces U_x (Figure 1). Now, we take a projective point $B \coloneqq \operatorname{span}(\beta^*)$ that does not belong to any subspace U_x and the translation φ of the whole space sending E to B. Then, the family of $(\varphi(U_x))_{x \in X}$ together with the family $(U_x)_{x \in J \setminus X}$ form another vector space representation of $\mathcal{Z}$ (Figure 2). Now, we only need to add $U_{x_0} \coloneqq \operatorname{span}(\beta^*)$ to those families to obtain a representation of $\mathcal{Z}'$.

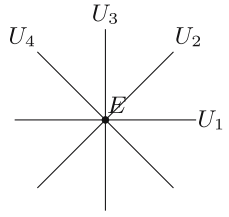


Figure 1: Basic representation of $\mathcal{Z}$

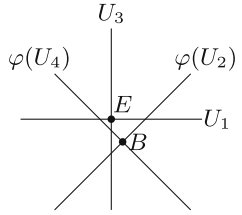


Figure 2: Modified representation of $\mathcal{Z}$

Now, we can do the formal calculations. Let $\nu : \mathbb{K}^{g_0 + g_1} \longrightarrow \mathbb{K}$ be defined by $\nu(a) = \nu(a_1, \ldots, a_{g_0 + g_1}) = a_1$ for every $a = (a_1, \ldots, a_{g_0 + g_1}) \in \mathbb{K}^{g_0 + g_1}$. Let $\beta_1 \in \mathbb{K}^{g_1} \times \mathbb{K}^{g_1} \setminus \bigcup_{x \in J} V_x$ and $\beta \coloneqq (\theta, \beta_1) \in \mathbb{K}^{g_0 + g_1}$. Obviously, $\beta \notin U_x$ for every $x \in J$.

Now, we define $\varphi : \mathbb{K}^{g_0 + g_1} \longrightarrow \mathbb{K}^{g_0 + g_1}$ by setting $\varphi(a) = a + \nu(a)\beta$ for all $a \in \mathbb{K}^{g_0 + g_1}$. Let us note that φ is an isomorphisms of vector spaces, so $\dim \varphi(U_x) = \dim U_x = g_0$. Moreover, $\varphi(a) = a$ for all $a \in \{\theta\} \times \mathbb{K}^{g_1} \times \mathbb{K}^{g_1}$ and $\beta^* \coloneqq \varphi(\varepsilon) = \varepsilon + \beta \notin U_x$ for all $x \in J$.

Let x_0 be any element not in J and let $U_{x_0} \coloneqq \operatorname{span}(\beta^*)$. Then, the family $(\varphi(U_x))_{x\in X} \cup (U_x)_{x\in J\setminus X} \cup \{U_{x_0}\}$ is a vector space representation of the one point extension of $\mathcal{Z}$ induced by Δ. Indeed, if $x \notin X$, then $h(\{x, x_0\}) = \dim(U_x + U_{x_0}) > \dim U_x = h(\{x\}) = g_0$ as $\beta^* \notin U_x$. Thus, $\{x\} \notin \min\Delta$. For $x \in X$ we have $h(\{x, x_0\}) = \dim(\varphi(U_x) + U_{x_0}) = \dim U_x = h(\{x\}) = g_0$, so $\{x\} \in \min\Delta$.

From the fact that φ is a vector space isomorphism, it follows $\varphi(U_x) + \varphi(U_y) = \varphi(U_x + U_y) = \mathbb{K}^{g_0+g_1}$ for all $x, y \in X$. For $x \in X$ and $y \in J\setminus X$, we have $\varphi(U_x) + U_y \supseteq \varphi(\{\theta\} \times V_x) + U_y = (\{\theta\} \times V_x) + U_y = \mathbb{K}^{g_0-g_1} \times (V_x + V_y) = \mathbb{K}^{g_0+g_1}$. In every case $h(\{x, y, x_0\}) = \dim(\mathbb{K}^{g_0+g_1} + U_{x_0}) = g_0 + g_1$, i.e., $\{x, y\} \in \Delta$. If $x, y \notin X$, then $\{x, y\} \in \min\Delta$. □

In the next proof, we will need the following well-known property of vector spaces over finite fields. Let $V_1, \ldots, V_n$ be the proper subspaces of a vector space V over a finite field $\mathbb{K}$. If $|\mathbb{K}| > n$, then $V_1 \cup \ldots \cup V_n \neq V$. Let us recall that every uniform polymatroid is representable.

Theorem 5.2. *All access structures determined by any uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ with height m and monotone increasing family $\Delta \subsetneq \mathcal{P}(J)$ such that $|\min\Delta| = 1$ are ideal.*

Proof. Let $\min\Delta = \{X\}$ for a suitable $\emptyset \neq X \subseteq J$ and let $k \coloneqq |X|$. The assumption that the height of $\mathcal{Z}$ equals m is equivalent to $g_{m-1} > 0$, and this implies $h(Y) < h(Z)$ for all $Y \subsetneq Z \subseteq J$. It follows from Lemma 2.13 that Δ is compatible with $\mathcal{Z}$.

Let $\mathbb{K}$ be a finite field and let $(V_x)_{x\in J}$ be a $\mathbb{K}$-vector space representation of $\mathcal{Z} = (J, h, \boldsymbol{g})$. Then, V_x are the subspaces of the vector space $\mathbb{K}^{h_m}$ and $\dim V_x = h_1 = g_0$ for every $x \in J$. Given any $Y \subseteq J$, we define $V_Y \coloneqq \sum_{y\in Y} V_y$. If $Y \in \Delta$, then $X \subseteq Y$ and $V_X \subseteq V_Y$. If $Y \notin \Delta$, then $X \not\subset Y$ and so $|X \cup Y| > |Y|$. Hence, $\dim(V_X + V_Y) = \dim V_{X\cup Y} = h(X \cup Y) > h(Y) = \dim V_Y$. This shows that $V_X \not\subset V_Y$. Thus, $Y \in \Delta$ if and only if $V_X \subseteq V_Y$. Since $V_Y \cap V_X$ is a proper subspace of V_X whenever $Y \notin \Delta$ and, so assuming $|\mathbb{K}| > 2^m - 2^{m-k}$, we have $V_X \cap \bigcup_{Y\in\mathcal{P}(J)\setminus\Delta} V_Y = \bigcup_{Y\in\mathcal{P}(J)\setminus\Delta}(V_X \cap V_Y)$ is a proper subset of V_X. This shows that there is $\beta \in V_X$ such that $\beta \notin V_Y$ for all $Y \notin \Delta$. Setting $V_{x_0} \coloneqq \operatorname{span}(\beta)$, we obtain $(V_x)_{x\in J\cup\{x_0\}}$, which is a vector space representation of the one point extension of $\mathcal{Z}$ induced by Δ. □

The aforementioned proof is not constructive. Using the fact that every uniform polymatroid is a sum of uniform matroids, one can efficiently build a vector space representation of $\mathcal{Z}$ and then determine a vector β that spans the space V_{x_0} but the calculations are more complicated. A general outline of this procedure is sketched out in [12, sections III and VI].

Let us note that if $\{X\} = \min\Delta$, then X determines a set of distinguished blocks, whose representatives must be present in all authorized sets. Indeed, if $\bar{v} \in \Gamma$ is an authorized vector, then $\operatorname{supp}(\bar{v}) \in \Delta$, so $X \subseteq \operatorname{supp}(\bar{v})$; thus, $v_x \neq 0$ for all $x \in X$. If $|X| \geq 2$, then the access structures Γ is compartmented by Theorem 4.3, so all blocks are mutually hierarchically independent.

For the sake of completeness, we recall the following result obtained by Farràs et al. in [12] who characterized the uniform multipartite access structures mentioned in Remark 4.10 and proved that they are ideal. Contrary to the aforementioned case, all participants in any uniform access structure have the same rights but different blocks are hierarchically independent. Here, we reformulate that result as follows.

Theorem 5.3. [12, Lemma 6.2] *If the monotony increasing family $\Delta \subseteq \mathcal{P}(J)$ such that $\min\Delta = \mathcal{P}_k(J), 1 \leq k \leq m$ is compatible with a uniform polymatroid $\mathcal{Z}$, then the access structure determined by Δ and $\mathcal{Z}$ is ideal.*

Let us note that Theorem 5.2 shows that the access structures presented in Theorem 4.11 are ideal. Now, we turn to the objects considered in Theorems 4.8 and 4.9.

Theorem 5.4. *All access structures determined by any uniform polymatroid $\mathcal{Z} = (J, h, \boldsymbol{g})$ with the increment sequence $\boldsymbol{g} = (g_i)_{i\in I_m}$ such that $|J| \geq 3$ and $g_0 \geq g_1 = g_{m-1} > 0$ are ideal.*

Proof. We want to prove that for every increasing family $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ that is compatible with $\mathcal{Z}$, the access structure determined by $\mathcal{Z}$ and Γ is ideal. The assumption $g_0 \geq g_1 = g_{m-1} > 0$ combined with Theorems 4.8 and 4.9 implies that $\min\Delta = \mathcal{P}_1(J)$ or $|\min\Delta| = 1$. In the former case, the claim follows from Theorem 5.3. In the latter case, applying Theorem 5.2 completes the proof. □

6 Conclusion

This article contains selected results from the first author's PhD thesis [20]. It is intended to initiate research on the access structures obtained from polymatroids. This choice is motivated by the fact that access structures determined by polymatroids are matroid ports, i.e., they satisfy a necessary condition to be ideal. In this article our investigation is limited to uniform polymatroids. We are particularly interested in the hierarchical order on the set of participants determined by the access structures considered here. Most of the results in the literature that is devoted to discussing this subject consider access structures that are compartmented or totally hierarchical. We showed that all non-compartmented access structure with at least three parties considered in this work are partially hierarchical. It is worth pointing out that some examples of partially hierarchical access structures are presented by Farràs et al. [12], but they are not determined by uniform polymatroids. There is good reason to deal with uniform polymatroids. In contrast to general polymatroids, every uniform polymatroid determines ideal access structures. It follows from the fact that every uniform polymatroid is representable. This allows building one point extensions of such polymatroids, which are also representable. Then, according to [10, Theorem 2.1, and Theorem 6.1], the suitable access structures obtained from those polymatroids are ideal.

The conditions presented in Section 3 are used to prove Theorems 4.2 and 4.3, which show that most of the access structures obtained from uniform polymatroids are compartmented (they are placed in the cells C2 and B3–C3 of Table 1). The exact hierarchy in access structures in the cells A2, B2, C1-D1, and D2-3 is described in Theorems 4.6–4.11.

The most diverse collection of objects contains the cell B2 where both compartmented and hierarchical access structures can be found but further precise investigation of that area is necessary. In general, the results presented here do not exhaust the topic and leaves space for further research.

Conjecture 6.1. Let $\Pi = (P_x)_{x\in J}$ be a partition of a set of participants P and let $\mathcal{Z} = (J, h, \boldsymbol{g})$ be a uniform polymatroid of height n such that $2 \leq n < m$. Additionally, let $\Delta \subseteq \mathcal{P}(J)\setminus\{\varnothing\}$ be a monotone increasing family with $\mu(\Delta) = 1$ that is compatible with $\mathcal{Z}$. The hierarchical order in Π induced by $\Gamma = \Gamma(\Pi, \mathcal{Z}, \Delta)$ is of the type $\mathrm{Ord}(Y, X)$ for a certain disjoint subsets X and Y of J.

This conjecture is partially confirmed by Theorem 4.12 that states that every chain in hierarchical access structure contains one or two elements. This fact applies only to access structures induced by uniform polymatroids. For other polymatroids, one can construct hierarchical access structures with chains of arbitrary length.

Some multipartite access structures determined by uniform polymatroids contain redundant blocks or different blocks that are equivalent. We treat such objects as improperly constructed. Fortunately, they appear only as extreme cases (cf. Corollary 3.10 and Theorem 4.1).

The results presented in Section 4 do not depend on the particular values of the rank function of $\mathcal{Z}$ (or equivalently the values of $\boldsymbol{g}$). The only impact on the hierarchy of the described structures has the sequence of signatures of differences of consecutive entries of $\boldsymbol{g}$. This observation is additionally confirmed by computer calculations that suggest the following unproved conjecture.

Conjecture 6.2. Let $\boldsymbol{g} = (g_i)_{i\in I_m}$ and $\boldsymbol{g}' = (g_i')_{i\in I_m}$ be the increment sequences of uniform polymatroids $\mathcal{Z}$ and $\mathcal{Z}'$ with the ground set J, respectively, such that $\mathrm{sgn}(g_{i-1} - g_i) = \mathrm{sgn}(g'_{i-1} - g'_i)$ for all $i = 1, \ldots, m$. If a monotone increasing family Δ is compatible with $\mathcal{Z}$ and $\mathcal{Z}'$, then the hierarchical preorders on Π determined by $\Gamma(\Pi, \mathcal{Z}, \Delta)$ and $\Gamma(\Pi, \mathcal{Z}', \Delta)$ are equal.

Investigating which of the structures considered in this article are ideal is another open issue. A sufficient condition can be obtained by proving that the one point extension of a given uniform polymatroid is representable (cf. [10, Corollary 6.7]). This idea has been used to show that the access structures discussed in Theorems 4.6 and 4.8–4.11 are ideal. By analyzing the structure of the vector space representation of the polymatroid, one can also prove the ideality of many other access structures. However, we cannot rule out the existence of non-ideal access structures derived from uniform polymatroids. In this case, we have the following question. Is it true that upper bound for the information ratio of access structures obtained from uniform polymatroids can be significantly less than the upper bound for the information ratio of arbitrary matroid ports? Let us recall that the information ratio of a secret sharing scheme is the ratio between the maximum length of the shares and the length of the secret with a finite domain of shares. The *information ratio of an access structure* Γ is the infimum of all information ratios taken over all secret sharing schemes with the access structure Γ.

Acknowledgement: The authors would like to thank the anonymous reviewers for many helpful comments.

Funding information: The authors state no funding involved.

Author contributions: Both authors have accepted responsibility for the entire content of this manuscript and approved its submission.

Conflict of interest: The authors state no conflict of interest.

References

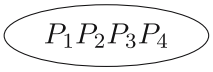
[1] Blakley GR. Safeguarding cryptographic keys. The National Computer Conference 1979. AFIPS. Vol. 48; 1979. p. 313–7.
[2] Shamir A. How to share a secret. Commun. ACM. 1979;22:612–3.
[3] Beimel A. Secret-sharing schemes: a survey. In: Third International Workshop. IWCC 2011. Lecture Notes in Computer Science. vol. 6639; 2011. p. 11–46.
[4] Padró C. Lecture notes in secret sharing. IACR Cryptol. ePrint Arch. 2012;2012:674.
[5] Ito M, Saito A, Nishizeki T. Secret sharing schemes realizing general access structure. In: Proceedings on the IEEE GLOBECOM'87. 1987. p. 99–102.
[6] Benaloh J, Leichter J. Generalized secret sharing and monotone functions. In: Advances in Cryptology. CRYPTO'88. Lecture Notes in Computer Science. vol. 403; 1990. p. 27–35.
[7] Kothari S.C. Generalized linear threshold scheme. Advances in Cryptology - CRYPTOa84. Lecture Notes in Computer Science. Vol. 196; 1985. p. 231–41.
[8] Simmons GJ. How to (really) share a secret. Advances in Cryptology - CRYPTO88. Lecture Notes in Computer Science. Vol. 403; 1990. p. 390–448.
[9] Farràs O, Metcalf-Burton JR, Padró C, Vázquez L. On the optimization of bipartite secret sharing schemes. Des. Codes Cryptogr. 2012;63:255–71.
[10] Farràs O, Martí-Farré J, Padró C. Ideal multipartite secret sharing schemes. J Cryptol. 2012;25:434–63.
[11] Farràs O, Padró C. Ideal hierarchical secret sharing schemes. IEEE Trans Inform Theory. 2012;58:3273–86.
[12] Farràs O, Padró C, Xing C, Yang A. Natural generalizations of threshold secret sharing. IEEE Trans Inform Theory 2014;60:1652–64.
[13] Tassa T. Hierarchical threshold secret sharing. J Cryptol. 2007;20:237–64.
[14] Brickell EF. Some ideal secret sharing schemes. J Combin Math Combin Comput. 1989;6:105–13.
[15] Brickell EF, Davenport DM. On the classification of ideal secret sharing schemes. J Cryptol. 1991;4:123–34.
[16] Kula M. Access structures induced by polymatroids with extreme rank function. Cryptology ePrint Archive, Paper 2023/962 (https://eprint.iacr.org/2023/962).
[17] Csirmaz L., Matús F, Padró Bipartite secret sharing and staircases. 2021. ArXiv/2103.04904.
[18] Csirmaz L. The size of a share must be large. J Cryptol. 1997;10:223–31.
[19] Seymour P.D. On secret-sharing matroids. J Combin Theory Ser B. 1992;56:69–73.
[20] Kawa R. Hierarchity of multipartite access structures. PhD Thesis. 2015. Katowice: University of Silesia; (Polish).

Appendix

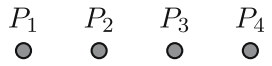
Table A1 presents hierarchical (pre)orders of access structures determined by uniform polymatroids $\mathcal{Z} = (J, h, \boldsymbol{g})$, where $J = \{1, 2, 3, 4\}$. It is worth pointing out that types of orders are invariant with respect to permutations of elements of J, so monotony increasing families appearing in the table are the representatives of invariant classes of the permutation group S_4 acting on J. For example, the monotone increasing families Δ_1 and Δ_2 such that $\min\Delta_1 = \{\{1\}, \{2, 3\}\}$ and $\min\Delta_2 = \{\{2\}, \{3, 4\}\}$ represent the same invariant class. Assuming that Conjecture 6.2 is true, the table presents a complete overview of hierarchical orders of all access structures obtained from uniform polymatroids $(J, h, \boldsymbol{g})$ with $|J| = 4$. If the monotonic family appearing in the first column is not compatible with the polymatroid represented by the values of $\boldsymbol{g}$ in the top rows, then the suitable cell of the table contains $^-$. Otherwise, the types of (pre)orders are denoted according to the following key. It is worth pointing out that according to Remark 2.5, every column of the table contains at least one ideal access structure. More ideal access structures can be obtained form theorems of Section 5.

Table A1: Access structures in the case $m = 4$

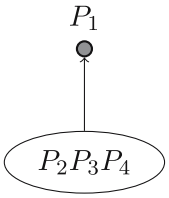
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	g_0	1	2	1	3	2	2	1	3	2	4	3	3	2	2	1
	g_1	0	1	1	2	2	1	1	2	2	3	3	2	2	1	1
	g_2	0	0	0	1	1	1	1	1	1	2	2	2	2	1	1
$\min\Delta$	g_3	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	$\{\{1\}\}$	–	–	–	–	–	–	–	M	M	M	M	M	M	M	I
2	$\{\{1\},\{2\}\}$	–	–	–	C	–	–	–	–	–	C	–	–	–	–	–
3	$\{\{1\},\{2\},\{3\}\}$	–	W	–	C	–	–	–	C	–	C	–	–	–	–	–
4	$\{\{1\},\{2\},\{3\},\{4\}\}$	T	C	–	C	–	C	–	C	–	C	–	C	–	C	–
5	$\{\{1\},\{2\},\{3,4\}\}$	–	K	–	C	–	–	–	C	–	C	–	–	–	–	–
6	$\{\{1\},\{2,3\}\}$	–	–	–	E	E	–	–	–	–	C	C	–	–	–	–
7	$\{\{1\},\{2,3\},\{2,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
8	$\{\{1\},\{2,3\},\{2,4\},\{3,4\}\}$	–	M	M	C	C	–	–	C	C	C	C	–	–	–	–
9	$\{\{1\},\{2,3,4\}\}$	–	–	–	M	M	M	M	–	–	C	C	C	C	–	–
10	$\{\{1,2\}\}$	–	–	–	–	–	–	–	C	C	C	C	C	C	K	V
11	$\{\{1,2\},\{1,3\}\}$	–	–	–	–	–	–	–	–	–	C	C	–	–	–	–
12	$\{\{1,2\},\{3,4\}\}$	–	–	–	C	C	C	C	–	–	C	C	C	C	–	–
13	$\{\{1,2\},\{1,3\},\{1,4\}\}$	–	–	–	–	–	–	–	C	C	C	C	–	–	–	–
14	$\{\{1,2\},\{1,3\},\{2,3\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
15	$\{\{1,2\},\{2,3\},\{1,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
16	$\{\{1,3\},\{2,3\},\{1,4\},\{2,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
17	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
18	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
19	$\{\{1,2\},\{1,3\},\{2,3\},\{1,4\},\{2,4\},\{3,4\}\}$	–	C	C	C	C	–	–	C	C	C	C	–	–	–	–
20	$\{\{1,2\},\{1,3,4\}\}$	–	–	–	–	–	–	–	–	–	C	C	C	C	–	–
21	$\{\{1,2\},\{1,3\},\{2,3,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
22	$\{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$	–	–	–	C	C	–	–	–	–	C	C	–	–	–	–
23	$\{\{1,2\},\{1,3,4\},\{2,3,4\}\}$	–	–	–	C	C	C	C	–	–	C	C	C	C	–	–
24	$\{\{1,2,3\}\}$	–	–	–	–	–	–	–	C	C	C	C	C	C	W	W
25	$\{\{1,2,3\},\{1,2,4\}\}$	–	–	–	–	–	–	–	–	–	C	C	C	C	–	–
26	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\}\}$	–	–	–	–	–	–	–	–	–	C	C	C	C	–	–
27	$\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$	–	–	–	C	C	C	C	–	–	C	C	C	C	–	–
28	$\{\{1,2,3,4\}\}$	–	–	–	–	–	–	–	C	C	C	C	C	C	C	C



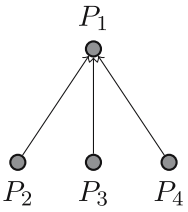
$T := Ord^*(J_4, \emptyset)$



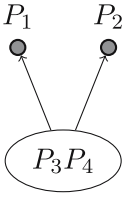
$C := Ord^*(\emptyset, J_4) = Ord(\emptyset, J_4)$



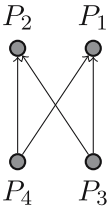
$I := Ord^*(\{2,3,4\}, \{1\})$



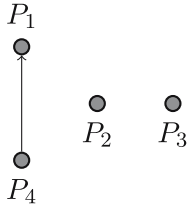
$M := Ord(\{2,3,4\}, \{1\})$



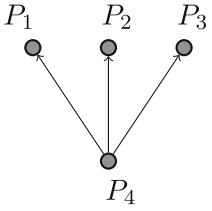
$V := Ord^*(\{3,4\}, \{1,2\})$



$K := Ord(\{3,4\}, \{1,2\})$



$E := Ord(\{4\}, \{1\})$



$W := Ord^*(\{4\}, \{1,2,3\}) = Ord(\{4\}, \{1,2,3\})$