Designs, Codes and Cryptography (2023) 91:1335–1349
https://doi.org/10.1007/s10623-022-01154-9

# Ideal hierarchical secret sharing and lattice path matroids

Songbao Mo[1]

Received: 9 September 2021 / Revised: 16 September 2022 / Accepted: 6 November 2022 /
Published online: 20 November 2022

**Abstract**
By a fundamental result by Brickell and Davenport (J Cryptol 4:123–134, 1991), the access structures of ideal secret sharing schemes are matroid ports. Farràs and Padró (IEEE Trans Inf Theory 58(5):3273–3286, 2012) presented a characterization of ideal hierarchical access structures. In this paper, we provide a different characterization. Specifically, we show that an access structure is ideal and hierarchical if and only if it is a port of a lattice path matroid at some specific points.

**Keywords** Ideal secret sharing · Hierarchical access structures · Lattice path matroids · Nested matroids

**Mathematics Subject Classification** Primary 94A62 · Secondary 05B35

## 1 Introduction

Secret sharing schemes were introduced independently by Shamir [26] and Blakley [3] in 1979.

Initially designed for storing securely highly sensitive data such as numbered bank accounts, missile launch codes etc., secret sharing has now become an integral part of many cryptographic protocols, e.g., general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer (see a survey [2] for more details).

A *secret sharing scheme* is a method to distribute a *secret* among a group of users by giving each user a piece of information called *share*, such that only authorized coalitions of users can recover the secret from their shares. The set of authorized coalitions is called an *access structure*. A scheme is *perfect* if an unauthorized coalition can learn no information about the secret whatsoever. It has been shown that every access structure admits a perfect secret sharing scheme [14] and that for the scheme to be perfect the domain of shares of the

Communicated by C. Padro.

✉ Songbao Mo
smo633@aucklanduni.ac.nz

[1] Department of Mathematics, The University of Auckland, Auckland, New Zealand

users must be at least as large as the domain of the secrets [15]. In the optimal case, when for a perfect scheme the sizes of domains of the shares coincide with the size of the domain of the secrets, the scheme is called *ideal*.

It is one of the most important and long-standing open problems in secret sharing to characterise the class of *ideal access structures*, that is the ones that admit an ideal secret sharing scheme [2]. A milestone paper by Brickell and Davenport [8] revealed an important connection between secret sharing schemes and matroids. A consequence of the result by Brickell and Davenport is that either all ports of a matroid are ideal or none of them is. The matroid whose ports are ideal is called a *secret sharing matroid* [19, 25]. Brickell and Davenport [8] showed that every ideal access structure is a port of a secret sharing matroid. However, not every matroid is a secret sharing matroid, for example, Seymour [25] showed that the Vamos matroid is not a secret sharing matroid. A sufficient condition was given by Brickell and Davenport [8]. They proved every representable matroid is a secret sharing matroid. This sufficient condition is, however, not necessary. For example, the non-Pappus matroid is not representable over any field, but it is a secret sharing matroid [27]. Hence, the problem of characterising ideal access structures is reduced to the problem of classifying secret sharing matroids. This problem has not yet been solved but some partial progress has been made. A number of authors attempted to classify all ideal access structures in subclasses of secret sharing schemes. These include access structures defined by graphs [8], weighted threshold access structures [2, 10, 13], hierarchical access structures [10], bipartite [22, 23] and tripartite access structures [11].

In a *threshold access structure* with $n$ participants, the authorized subsets are those with at least $k$ participants for some $k$. They are also called $k$-out-of-$n$ structures. Shamir [26] and Blakley [3] presented two different methods to construct secret sharing schemes for threshold access structures and these schemes are ideal. In a threshold access structure all participants are equally important. However, in a real organization the powers of members of those organizations are often unequal. As Tassa [29] puts it “it is natural to expect that the participants are not equal in their privileges or authorities.” As an example he suggests a bank scenario, when the shares of the vault key may be distributed among bank employees, and the bank policy could require the presence of, say, three employees in opening the vault, and at least one of them must be a department manager.

Following [10] we call the access structure *hierarchical* if all its participants can be compared and ordered (in a non-strict linear order sense) with respect to their importance.[1]

Simmons [27] proposed two families of access structures, the *multilevel* and *compartmented* ones. These access structures were proved by Brickell [7] to be ideal. The multilevel access structures defined by Simmons are hierarchical and now known as *disjunctive hierarchical access structures*. Tassa [29] studied another class of hierarchical access structures called *conjunctive hierarchical access structure* and showed that they are also ideal. Gvozdeva, Hameed and Slinko [12] studied these two types of access structures in the context of simple game theory.

In [10], Farràs and Padró have given a characterization of ideal hierarchical access structures. Due to the importance of this class, alternative characterizations are desirable. One possible way to do this is to characterise the matroids that correspond to these structures. In this paper, we provide such a characterization. We show that an access structure is ideal and hierarchical if and only if it is a port of a lattice path matroid at some specific points. The proof is based on the characterization of ideal hierarchical access structures by Farràs and Padró [10] and the properties of lattice path matroids by Bonin and de Mier [4]. We first show

[1] Taking a cue from the concept of Isbel’s desirability relation [30] in game theory.

that there is a “one-to-one" correspondence between lattice path matroids and hierarchical access structures, and then prove that the hierarchical access structure coincides with the port of the corresponding lattice path matroid at a specific point. Disjunctive hierarchical access structures and conjunctive hierarchical access structures are two important subclasses of ideal hierarchical access structures. We show that they are ports of nested matroids, which are a subclass of lattice path matroids, at some specific points. These results once again highlight the usefulness of the strong connection between secret sharing schemes and matroids.

The paper is organized as follows. In Sect. 2, we give some basic definitions of background materials: in Sect. 2.1 we define hierarchical access structures. In Sect. 2.2, the basic definitions in matroid theory are given. In Sect. 2.3, we define matroid ports. We define lattice path matroids in Sect. 3, and recall some results regarding lattice path matroids. We will used some of these results to prove our main result. In Sect. 4, we prove our main result Theorem 16. In Sect. 5, we provide characterizations of two subclasses of ideal hierarchical access structures: disjunctive hierarchical access structures and conjunctive hierarchical access structures.

## 2 Preliminaries

### 2.1 Hierarchical access structures

**Definition 1** Let $P$ be a finite set. An *access structure* $\Gamma$ on $P$ is a collection of subsets of $P$ such that the following are satisfied:

**(A1)** $\Gamma \neq \emptyset$,
**(A2)** $\Gamma$ is monotone, that is, if $X \subseteq Y$ and $X \in \Gamma$, then $Y \in \Gamma$.

A subset $X \subseteq P$ is *authorized* if $X \in \Gamma$, otherwise it is *unauthorized*. Due to the monotone property, an access structure is determined by the set of *minimal authorized coalitions*, denoted by $\min \Gamma$. An access structure is *connected* if every participant $x \in P$ is contained in at least one minimal authorized coalition. The *dual* of $\Gamma$, denoted as $\Gamma^*$, is an access structure defined as

$$\Gamma^* = \{X \in P \mid E - X \notin \Gamma\}.$$

**Definition 2** Let $\Gamma$ be an access structure on $P$ and let $p, q \in P$. We say $p$ is *at least as powerful as* $q$, denoted by $q \preceq_\Gamma p$ (the subindex $\Gamma$ is often omitted if the access structure is clear from the context), if $A \cup \{p\} \in \Gamma$ whenever $A \cup \{q\} \in \Gamma$, where $A$ is an arbitrary subset of $P - \{p, q\}$. Two participants $p, q$ are *equivalent*, denoted by $p \sim_\Gamma q$, if $p \preceq q$ and $q \preceq p$. And $p$ is *more powerful* than $q$, denoted as $q \prec p$, if $q \preceq p$ but $p \npreceq q$.

**Definition 3** The access structure $\Gamma$ on $P$ is *m-partite* if $P$ can be partitioned into *m parts* such that elements in the same part are equivalent. It is *strictly m-partite* if elements in different parts are not equivalent.

**Definition 4** A binary relation $\leq$ is a *total preorder* on a set $P$ if it satisfies:

- Reflexivity: $a \leq a$ for all $a \in P$, and
- Transitivity: if $a \leq b$ and $b \leq c$ then $a \leq c$ for all $a, b, c \in P$, and
- Totality: $a \leq b$ or $b \leq a$ for all $a, b \in P$.

**Definition 5** An access structure $\Gamma$ on $P$ is *hierarchical* if and only if $\preceq_\Gamma$ is a total preorder.

In any hierarchical access structure $\Gamma$ on $P$, as $\sim_\Gamma$ is an equivalence relation, the set of participants $P$ can be partitioned into $m$ distinct equivalence classes $P_1, \ldots, P_m$, for some $m \in \mathbb{Z}^+$, so that $\Gamma$ is a strictly $m$-partite access structure and

$$P = \bigcup_{i=1}^{m} P_i,$$

where $p \succ_\Gamma q$ for any $p \in P_i$ and $q \in P_j$ with $i < j$. That is, participants in the first level are strictly superior to those in the second level, the participants in the second level are strictly superior to those in the third level and so on.

**Definition 6** Suppose that $P$ is the set of participants with partition $(P_1, \ldots, P_m)$ and let $k_1 < k_2 < \ldots < k_m$ be a sequence of positive integers. Let $\mathbf{k} = (k_1, k_2, \ldots, k_m)$. Then we define a *disjunctive hierarchical access structure* $\Gamma_\exists(P, \mathbf{k})$ by setting the set of authorized coalitions to be

$$\Gamma_\exists(P, \mathbf{k}) = \left\{ X \in 2^P \middle| \exists i \left( \left| X \cap \left( \bigcup_{j=1}^{i} P_j \right) \right| \geq k_i \right) \right\},$$

and *conjunctive hierarchical access structure* $\Gamma_\forall(P, \mathbf{k})$ by setting the set of authorized coalitions to be

$$\Gamma_\forall(P, \mathbf{k}) = \left\{ X \in 2^P \middle| \forall i \left( \left| X \cap \left( \bigcup_{j=1}^{i} P_j \right) \right| \geq k_i \right) \right\}.$$

For the disjunctive access structure defined in Definition 6, we assume $\sum_{j=1}^{i} |P_j| \geq k_i$ for all $i \in [m]$, otherwise the access structure can be empty or the threshold in level $i$ cannot be exceeded and the existence of $k_i$ is unnecessary. For the conjunctive access structure defined in Definition 6, $|P| \geq k_m$, otherwise the access structure is empty.

It is well-known that both disjunctive and conjunctive hierarchical access structures are ideal [7, 29]. For the formal definitions of perfect and ideal secret sharing schemes, the reader is referred to [2, 28].

In [10], Farràs and Padró introduced the following class of hierarchical access structures which generalizes the class of conjunctive and disjunctive access structures.

**Definition 7** Suppose that $P$ is the set of participants with partition $(P_1, \ldots, P_m)$. Consider two integer vectors $\mathbf{a} = (a_1, \ldots, a_m)$ and $\mathbf{b} = (b_1, \ldots, b_m)$ with $a_1 = 0$ and $a_i \leq a_{i+1} \leq b_i \leq b_{i+1}$ for every $i \in [1, m-1]$. Then an *FP access structure* $\Gamma(P, \mathbf{a}, \mathbf{b})$ is an access structure defined as

$$\left\{ X \in 2^P \middle| \exists_{i \in [m]} \left( \left| X \cap \bigcup_{k=1}^{i} P_k \right| \geq b_i \text{ and } \forall_{j \in [1, i-1]} \left( \left| X \cap \bigcup_{k=1}^{j} P_k \right| \geq a_{j+1} \right) \right) \right\}.$$

For the definition above, we assume $\sum_{j=1}^{i} |P_i| \geq b_i$ for all $i \in [m]$ otherwise the access structure is empty or the threshold of certain level cannot be exceeded. The definition we are giving here is different from the one by Farràs and Padró [10], however they are equivalent. For the definition in [10], vectors $\mathbf{a}$ and $\mathbf{b}$ start from $a_0 = 1$ and $b_0 = 1$, respectively. We remove $a_0$ and $b_0$ here. Also in their definition, $a_1 = 1$ and we set it to be 0, as a consequence, all the entries of vectors $\mathbf{a}$ and $\mathbf{b}$ have been scaled down by 1. They show that the class of FP access structures is precisely the class of ideal hierarchical access structures.

**Theorem 1** [10] *A hierarchical access structure is ideal if and only if it is an FP access structure.*

## 2.2 Matroids

For general references on matroid theory the reader is referred to [20]. For convenience of the reader, here we introduce some basic concepts related to matroids.

**Definition 8** A matroid $M$ is an ordered pair $(E, \mathcal{I})$ consisting of a finite set $E$, known as the *ground set*, and a collection $\mathcal{I}$ of subsets of $E$, known as the set of *independent sets* of $M$, satisfying the following three conditions:

**(I1)** $\emptyset \in \mathcal{I}$.
**(I2)** If $X \in \mathcal{I}$ and $Y \subseteq X$, then $Y \in \mathcal{I}$.
**(I3)** If $X, Y \in \mathcal{I}$ and $|X| < |Y|$, then there is an element $e \in Y - X$ such that $X \cup e \in \mathcal{I}$.

A set is *dependent* if it is not in $\mathcal{I}$. A minimal dependent set is called a *circuit*, that is, $X$ is a circuit if $X$ is dependent and any proper subset of $X$ is independent. A circuit with cardinality one is a *loop*. A maximal independent set is called a *basis*, that is, if $X$ is independent then any proper superset of $X$ is dependent. A *spanning circuit* is a circuit that contains a basis. The set of bases of matroid $M$ is denoted by $\mathcal{B}(M)$.

Let $M$ be a matroid on $E$. The *rank function* of $M$ is a function $r : 2^E \to \mathbb{Z}$ defined by

$$r(X) = \max\{|A| \mid A \subseteq X,\ A \in \mathcal{I}\},$$

for all $X \subseteq E$. The *rank of the matroid* $M$, denoted by $r(M)$, is the rank of the ground set $E$. The difference $|X| - r(X)$ is called the *nullity* of the subset $X$, denoted by $\eta(X)$. The nullity of $E$ in $M$ is called the *nullity* of $M$. The *restriction* of $M$ to $X$, written $M|X$, is the matroid on the set $X$ whose independent sets are the independent sets of $M$ that are contained in $X$. The *contraction* of $M$ by $Y \subseteq E$, written $M/Y$, is the matroid on the underlying set $E - Y$ with rank function defined as $r'(A) = r(A \cup Y) - r(Y)$. The matroid obtained from $M$ by a sequence of restriction and contraction operations is called a *minor* of $M$. Given a matroid $M$, its *dual* matroid $M^*$ is the matroid with ground set $E$ and the set of bases given by

$$\mathcal{B}(M^*) = \{E - B \mid B \in \mathcal{B}(M)\}.$$

A matroid is *connected* if for any $x, y \in E$, there exists a circuit that contains both $x$ and $y$. The *closure* $\mathrm{cl}(X)$ of a subset $X$ of $E$ is the set

$$\mathrm{cl}(X) = \{x \in E \mid r(X \cup x) = r(X)\}.$$

A subset $X \subseteq E$ is a *flat* if $\mathrm{cl}(X) = X$. The flat $X$ of a matroid $M$ is *connected* if the restriction $M|X$ is connected. A flat is *trivial* if it is independent; otherwise it is *nontrivial*. A flat $X$ is said to be a *hyperplane* if $r(X) = r(M) - 1$. A matroid $M = (E, \mathcal{I})$ is say to be *linearly-representable* over a field $\mathbb{F}$, if there exists a vector space $V$ over $\mathbb{F}$ and a mapping $\phi : E \to V$ such that $X$ is independent in $M$ if and only if $\phi(X)$ is linearly independent in $V$, for all $X \subseteq E$. A matroid is *representable* if it is linearly-representable over some field.

Let $E$ be a finite set and $\mathcal{A} = \{A_j \subseteq E \mid j \in [m]\}$ be a set system of $E$. A *transversal* of $\mathcal{A}$ is a subset $\{e_1, e_2, \ldots, e_m\}$ of $E$ such that $e_j \in A_j$ for all $j \in [m]$ and all elements of this subset are distinct. We say $X \subseteq E$ is a *partial transversal* of $\mathcal{A}$ if for some subset $K$ of $[m]$, $X$ is a transversal of $\{A_j \mid j \in K\}$. It is well known that the collection of partial transversals forms a collection of independent sets of a matroid $M$(see for example [20]). The matroid

$M$ is called a *transversal matroid* and $\mathcal{A}$ a *presentation* of $M$. The *incidence function* of $\mathcal{A}$ is given by $n(X) = \{i \mid X \cap A_i \neq \emptyset\}$ for subsets $X \subseteq E$.

**Theorem 2** [24] *A transversal matroid is representable over all sufficiently large fields; in particular, it is representable over all infinite fields.*

### 2.3 Matroid ports

**Definition 9** Let $M$ be a matroid with ground set $E$ and let $p \in E$. The set

$$\Gamma_p(M) = \{A \subseteq E - \{p\} \mid r(A \cup \{p\}) = r(A)\}$$

is the *port of matroid $M$ at point $p$.*

Equivalently, $\Gamma_p(M) = \{A \subseteq E - \{p\} \mid p \in \mathrm{cl}(A)\}$.

Duality in matroids and in access structures nicely relate to each other [18]. More specifically, $\Gamma_p^*(M) = \Gamma_p(M^*)$.

With a slightly different definition of matroid port, Lehman showed in [17] that a matroid port of a connected matroid determines this matroid uniquely.

**Theorem 3** (Lehman, [17]) *Let $M$ be a connected matroid with ground set $E$ and $e \in E$. Let $\mathcal{C}_e$ be the collection of circuits of $M$ which contain $e$. Then $M$ is uniquely determined by $\mathcal{C}_e$.*

**Theorem 4** (Brickell and Davenport, [8]) *Let $\Gamma$ be a connected ideal access structure on $P$. Then there exists a connected matroid $M$ on $P \cup \{p\}$ such that $\Gamma_p(M) = \Gamma$, where $p \notin P$.*

The two theorems above together imply that a connected ideal access structure $\Gamma$ determines a connected matroid $M$ uniquely.

Previously, we defined what it means for two participants of an access structure to be equivalent. Now we define an equivalence relation for elements of a matroid.

**Definition 10** Let $M$ be a matroid on $E$ and $x, y \in E$. The elements $x$ and $y$ are *equivalent* if for any $X \subseteq E - \{x, y\}$, the set $X \cup x$ is a circuit if and only if $X \cup y$ is a circuit. The matroid $M$ is *$m$-partite* if $E$ can be partitioned into $m$ disjoint parts such that elements in the same part are equivalent. It is *strictly $m$-partite* if elements in different parts are not equivalent.

The two notions of equivalence are connected by the following result.

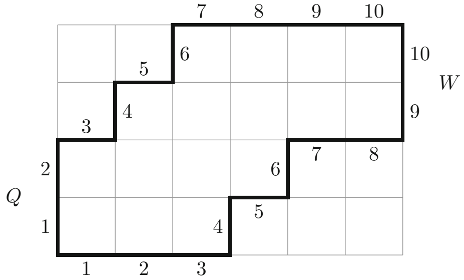
**Theorem 5** (Farràs, Martí-Farré and Padró, [11]) *Let $M$ be a connected matroid with ground set $E$ and let $p \in E$. Then $\Gamma_p(M)$ is $m$-partite with partition $(P_1, \ldots, P_m)$ if and only if $M$ is $(m+1)$-partite with partition $(\{p\}, P_1, \ldots P_m)$.*

## 3 Lattice path matroids

Lattice path matroids were introduced by Bonin, de Mier and Noy [6]. In this section, we briefly recap some of the results about lattice path matroids from Bonin and de Mier [4]; we will use these results in Sect. 4 to prove our main result which is Theorem 16.

A *North-East lattice path* of length $n$ is a sequence of points $v_0, v_1, \ldots, v_n \in \mathbb{Z}^2$ such that each consecutive difference $v_i - v_{i-1}$ lies in $S = \{(0, 1), (1, 0)\}$. The $(0, 1)$ steps are called *North* steps and denoted by $N$'s; the $(1, 0)$ steps are called *East* steps and denoted by $E$'s.

**Fig. 1** A lattice path presentation of a rank-4 lattice path matroid



Paths usually are represented as words in the alphabet $\{E, N\}$. All lattice paths we mention in this paper are North-East lattice paths starting at the point (0, 0) unless otherwise stated. A lattice path $Q$ has a *NE corner at h* if step $h$ of $Q$ is North and step $h + 1$ is East. An *EN corner at h* is defined similarly. A corner can also be specified by the coordinates of the point where the North and East steps meet.

Let $m, r$ be two non-negative integers and let $W$ and $Q$ be two lattice paths from (0, 0) to $(m, r)$ with $W$ never going above $Q$. Let $\mathcal{P}(W, Q)$ be the set of all lattice paths from (0, 0) to $(m, r)$ that go neither above $Q$ nor below $W$. For any $i$ with $1 \leq i \leq r$, let $N_i$ be the set

$$N_i := \{j \mid \text{ step } j \text{ is the } i\text{-th North step of a path in } \mathcal{P}(W, Q)\}.$$

It is easy to see that, $N_1, N_2, \ldots, N_r$ is a sequence of intervals in $[m + r]$, and both the left endpoints and the right endpoints form strictly increasing sequences; moreover, the left and right endpoints of $N_i$ correspond to the positions of the $i$-th North steps in $Q$ and $W$, respectively. The matroid $M[W, Q]$ is the transversal matroid on the ground set $[m + r]$ that has $(N_1, N_2, \ldots, N_r)$ as its presentation. We call $(N_1, N_2, \ldots, N_r)$ the *standard presentation* of $M[W, Q]$.

Let $N_i = [t_i, s_i]$ for $i \in [r]$. Since $W$ and $Q$ determine the matroid $M[W, Q]$, we call $(W, Q)$ the *lattice path presentation* of $M[W, Q]$. Note that $M[W, Q]$ has rank $r$ and nullity $m$. A *lattice path matroid* is any matroid isomorphic to $M[W, Q]$. If we fix one of the path by setting $W = E^m N^r$, then the lattice path matroid is called a *nested matroid*.

***Example 1*** Figure 1 depicts the lattice path presentation of the lattice path matroid $M[W, Q]$, with $W = E^3NENE^2N^2$ and $Q = N^2ENENE^4$, whose standard presentation is ([1, 4], [2, 6], [4, 9], [6, 10]).

A lattice path matroid $M[W, Q]$ of rank $r$ and nullity $m$ is connected if and only if $W$ and $Q$ intersect only at (0, 0) and $(m, r)$. We refer reader to [4] for more detail. Throughout this paper, we only consider connected lattice path matroids and connected access structures.

**Definition 11** Let $X$ be a connected flat of a connected lattice path matroid $M$ for which $|X| > 1$ and $r(X) < r(M)$. We say that $X$ is a *fundamental flat* of $M$ if for some spanning circuit $C$ of $M$ the intersection $X \cap C$ is a basis of $M|X$.

Fundamental flats were introduced in [4] to study lattice path matroids. Observe that the set of NE corners of $Q$ determines the path $Q$ and the set of EN corners of $W$ determines the path $W$. It turns out that the corners of the lattice paths $W$ and $Q$ nicely correspond to the fundamental flats.

**Theorem 6** [4] *A connected lattice path matroid is determined by the fundamental flats and their ranks.*

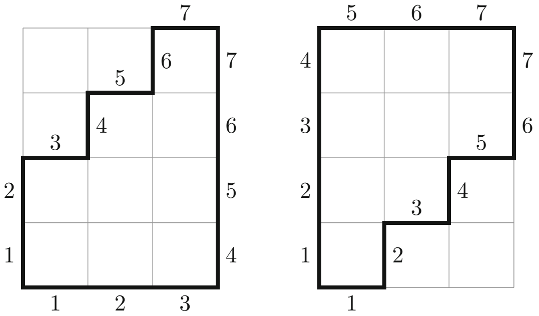


**Fig. 2** A 180° rotation of a nested matroid

**Theorem 7** [4, Theorem 5.3] *Let $M[W, Q]$ on $[n]$ be connected and has rank $r$. Let the $EN$ corners of $Q$ be at $i_1, i_2, \ldots, i_h$, with $i_1 < i_2 < \ldots < i_h$, and the $NE$ corners of $W$ be at $j_1 - 1, j_2 - 1, \ldots, j_k - 1$, with $j_1 < j_2 < \cdots < j_k$. The fundamental flats of $M[W, Q]$ are $[i_1] \subset [i_2] \subset \ldots \subset [i_h]$ and $[j_k, m + r] \subset \cdots \subset [j_2, m + r] \subset [j_1, m + r]$.*

These two theorems imply that a lattice path matroid can have at most two chains of fundamental flats under inclusion, and the lattice path matroid is determined by these two chains of fundamental flats. It is obvious that when a lattice path matroid has only one chain of fundamental flats, it is a nested matroid.

***Example 2*** Consider the lattice path matroid given in Fig. 1. The sets $\{1, 2, 3\}$, $\{4, 5\}$, $[1, 10]$ are all flats. The set $\{1, 2, 3\}$ is a fundamental flat because the circuit $C = \{1, 2, 4, 6, 7\}$ is a spanning circuit of $M$ and $\{1, 2, 3\} \cap C = \{1, 2\}$ is a basis of $M|\{1, 2, 3\}$. The set $\{4, 5\}$ is flat, and it is trivial since it is independent. The set $[1, 10]$ is not a fundamental flat since its intersection with any spanning circuit $C$ would be $C$ itself, and thus not a basis of $M|[1, 10]$.

The bounding paths $W$ and $Q$ of a connected lattice path matroid $M[W, Q]$ are determined by the matroid structure [4], up to a 180° rotation.

***Example 3*** The lattice path matroid $M$ presented in Fig. 2 on the left is a nested matroid. The matroid on the right is obtained by rotating the lattice path presentation of $M$ through 180° which is isomorphic to $M$.

**Theorem 8** [4, Theorem 3.1] *The class of lattice path matroids is closed under matroid duality.*

The following theorem will be used to prove Lemma 14 in Section 4.

**Theorem 9** *([4], Theorem 3.9) Let $C = \{c_0, c_1, \ldots, c_k\} \subseteq [m+r]$ be a set in the lattice path matroid $M[W, Q]$ with the standard representation $(N_1, \ldots, N_r)$; assume $c_0 < c_1 < \cdots < c_k$. Let $n(C)$ be $\{i_1, i_2, \ldots, i_s\}$, where $i_1 < i_2 < \cdots < i_s$. Then $C$ is a circuit of $M[W, Q]$ if and only if*

(1) $s = k$,
(2) $c_0 \in N_{i_1}$,
(3) $c_k \in N_{i_k}$, *and*
(4) $c_j \in N_{i_j} \cap N_{i_{j+1}}$ *for all $j$ with $0 < j < k$.*

*Furthermore, if $C$ is a circuit, then $i_{h+1} = i_h + 1$ for $1 \leq h < k$.*

***Example 4*** In Fig. 1, $C = \{1, 2, 4, 5\}$ is a circuit, because $n(C) = \{1, 2, 3\}$; $s = 3 = k$; $c_0 = 1 \in N_1 = [1, 4]$; $2 \in N_2, 4 \in N_3$; and $c_1 = 2 \in N_1 \cap N_2, c_2 = 4 \in N_2 \cap N_3$. However $D = \{1, 2, 4, 6\}$ is not a circuit, because $n(D) = \{1, 2, 3, 4\}$, $s = 4 \neq 3 = k$.

Let $\pi_1$ and $\pi_2$ be two partitions of a set $P$. We say that $\pi_1$ is *finer* than $\pi_2$ (and $\pi_2$ is *coarser* than $\pi_1$) if $\pi_1$ can be obtained from $\pi_2$ by splitting some of its parts into smaller pieces. The *meet* of two partitions, denoted by $\pi_1 \wedge \pi_2$, is the coarsest partition which is finer than both of them.

Consider the notation in Theorem 7, the set of $EN$ corners of $Q$ partitions $[n]$ into $h + 1$ parts, $[1, i_1], [i_1 + 1, i_2], \ldots, [i_h + 1, n]$, call this partition $\pi_1$. The set of $NE$ corners of $W$ partition $[n]$ into $k + 1$ parts, $[1, j_1 - 1], [j_1, j_2 - 1], \ldots, [j_k, n]$, call this partition $\pi_2$. We call $\pi_1 \wedge \pi_2$ the *natural ordered partition* of $[n]$ in $M$. The part that contains 1 and the part that contains $n$ are called the *head* and the *tail* of the partition, respectively.

The following corollary follows directly from Theorem 9.

**Corollary 10** [4, Corollary 3.13] *Let $C = \{c_0, c_1, \ldots, c_k\}$ be the circuit of $M[W, Q]$ with $c_0 < c_1 < \cdots < c_k$. If $x$ is not in $C$ and $Z \cup \{x\}$ is a circuit of $M[W, Q]$ for some subset $Z$ of $C$, then $Z$ is either $\{c_0, c_1, \ldots, c_i\}$ or $\{c_j, c_{j+1}, \ldots, c_k\}$.*

**Lemma 11** *Let $M[W, Q]$ be a connected lattice path matroid on $n$ elements. Then $x$ and $y$ are equivalent if and only if they are in the same set of fundamental flats.*

***Proof*** Suppose $x$ and $y$ are not in the same set of fundamental flats. Without lose of generality, there is a fundamental flat $F$ such that $x \in F$ and $y \notin F$. A fundamental flat is a connected flat, so there is a subset $A \subset F - \{x\}$ such that $A \cup \{x\}$ is a circuit. However $y \notin F$, so $A \cup \{y\}$ is independent. Therefore $x$ and $y$ are not equivalent.

Suppose $x$ and $y$ are in the same set of fundamental flats. Assume $x$ and $y$ are not equivalent. There is a subset $A \subseteq E - \{x, y\}$ such that $A \cup \{x\} = \{c_0, c_1, \ldots, c_k\}$ is a circuit but $A \cup \{y\}$ is not a circuit. By Theorem 9, $n(A \cup \{x\}) = \{h + 1, \ldots, h + k\}$ for some $h$. We have two cases to consider. Either there is a proper subset $A'$ of $A$ such that $A' \cup \{y\}$ is a circuit or $A \cup \{y\}$ is independent. For the former case, by Corollary 10, either $A'$ is $\{c_0, c_1, \ldots, c_i\}$ with $i < k$ or $\{c_j, c_{j+1}, \ldots, c_k\}$ with $j > 1$. If $A' = \{c_0, c_1, \ldots, c_i\}$, then by Theorem 9, $A' \cup \{y\}$ is a circuit implies $y \in N_{h+i}$, $y \notin N_{h+i+1}$ and $x > y$. Let $F_1$ be the smallest fundamental flat that contains $A' \cup \{y\}$ and the element 1. The containment relation is proper otherwise we have a contradiction immediately. We can find a circuit $C = B \cup A' \cup \{y\} - \{c_0\}$ with $n(C) = \{1, \ldots, h, h + 1, \ldots, h + k\}$ by carefully choosing the elements from $F_1$ so that $C$ satisfies the properties in Theorem 9. It is easy to see that $x \notin N_i$ for all $i \in [h]$, and any circuit $C'$ that contains both $x$ and 1 must have $n(C') \supset n(C)$. Therefore $x \notin F_1$. This contradicts the fact that $x$ and $y$ are in the same set of fundamental flats. If $A' = \{c_j, c_{j+1}, \ldots, c_k\}$, then the argument is similar, except we have $x < y$ and we find the smallest fundamental flats that contains $A' \cup \{y\}$ and the element $n$.

For the case $A \cup \{y\}$ is independent, there is a set $B \supset A$ such that $B \cup \{y\}$ is a circuit but $B \cup \{x\}$ is not a circuit and there is a proper subset $A$ of $B$ such that $A \cup \{x\}$ is a circuit. This is essentially the same case as before except the exchange of $x$ and $y$. □

**Lemma 12** *Let $M[W, Q]$ be a connected lattice path matroid on $[n]$ with elements go in the natural order. Then $M$ is multipartite with distinct equivalence classes which are the same as that of the natural ordered partition of $[n]$ in $M$.*

***Proof*** Let $\pi_1 \wedge \pi_2$ be the natural ordered partition of $[n]$ in $M$. By Lemma 11, $x$ and $y$ are equivalent if and only if they are in the same set of fundamental flats. By Theorem 7, $x$ and $y$ are in the same set of fundamental flats if and only if they are in the same part of $\pi_1 \wedge \pi_2$. □

By Theorem 5 and Lemma 12, the following lemma is straightforward.

**Lemma 13** *Let $M[W, Q]$ be a connected $m$-partite lattice matroid $M$ on $n$ elements. Let $(P_1, P_2, \dots, P_m)$ be the natural ordered partition of $[n]$, where $1 \in P_1$. Then $\Gamma_1(M)$ is $m$-partite with distinct equivalence classes $(P_1\backslash\{1\}, P_2, \dots, P_m)$.*

## 4 Ideal hierarchical access structures

In this section, we prove our main theorem. We first prove the following lemma.

**Lemma 14** *Let $M[W, Q]$ be a rank-$r$ lattice path matroid on $m + r$ elements. Let $X \subseteq E$ such that $1 \in \text{cl}(X)$. If $y \in E - X$ and $x \in X$ such that $y < x$, then $1 \in \text{cl}(X \cup y - x)$.*

***Proof*** Let $c_0 = 1$. Since $1 \in \text{cl}(X)$, there exists $A = \{c_1, \dots, c_k\} \subseteq X$ such that $C = A \cup \{1\}$ is a circuit. If $x \notin A$, then it is trivial that $1 \in \text{cl}(X \cup y - x)$. We only need to consider the case that $x \in A$. Let $c_{t-1} < y < c_t$ for some $t \in [k]$. Since $C$ is a circuit, by Theorem 9, $n(C) = [k]$, and

(i) $|C| = |n(C)| + 1$,
(ii) $1 \in N_1$,
(iii) $c_k \in N_k$,
(iv) $c_j \in N_j \cap N_{j+1}$ for all $j$ with $0 < j < k$.

In particular, $c_{t-1} \in N_{t-1} \cap N_t$, and $c_t \in N_t$. Hence $y \in N_t$. There are two cases to consider.

- Suppose $y \notin N_{t+1}$. It is easy to see $x > y$ implies $x \in \{c_t, c_{t+1}, \dots, c_k\}$. We show $C' = \{1, c_1, \dots, c_{t-1}, y\}$ is a circuit by showing it satisfies the four properties in Theorem 9. From the above results, it is easy to see $n(C') = \{1, 2, \dots, t-1\}$. So $|C'| = |n(C')|+1$, hence Property (1) holds. By $(ii)$, $1 \in N_1$, hence Property (2) holds. We already know that $y \in N_t$, that is Property (3) holds. By $(iv)$, $c_j \in N_j \cap N_{j+1}$ for all $j$ with $0 < j < t$, that is Property (4) holds.
- Suppose $y \in N_{t+1}$. We know that $x \in \{c_t, c_{t-1}, \dots, c_k\}$. If $x = c_t$, we will show $C' = \{1, c_1, c_2, \dots, c_{t-1}, y, c_{t+1}, \dots, c_k\}$ is a circuit. By (i)–(iii), Property (1)-(3) holds. By $(v)$, Property (4) almost holds except we need to show $y \in N_t \cap N_{t+1}$, however we know $y \in N_t$ and by assumption $y \in N_{t+1}$. So Property (4) holds. Now assume $x \neq c_t$, then $x = c_s$ for some $s \in [t + 1, k]$. If $c_j \in N_{j+2}$ for all $j \in [t, s - 1]$, we show that $A' = \{1, y\} \cup A - \{x\} = \{1, c_1, \dots, c_{t-1}, y, c_t, c_{t+1}, \dots, c_{s-1}, c_{s+1}, \dots, c_k\}$ is a circuit by checking $A'$ satisfies the properties in Theorem 9. It is obvious that Property (1) holds, as $|A'| = |n(A')| + 1 = k + 1$. By $(ii)$ and $(iii)$, Property (2) and (3) hold. By $(iv)$, we know $c_i \in N_j \cap N_{j+1}$ for all $j$ with $0 < j < k$. In particular, $c_j \in N_j \cap N_{j+1}$ for all $j$ with $0 < j < t$ or $s < j < k$. We also have $c_j \in N_{j+1}$ for all $j$ with $t \leq j < s$. Together with the assumption that $c_j \in N_{j+2}$ for all $j \in [t, s-1]$, obtain $c_j \in N_{j+1} \cap N_{j+2}$ for all $j$ with $t < j < s$. Furthermore, we know $y \in N_t \cap N_{t+1}$. Therefore Property (4) holds. So $A'$ is a circuit If $c_j \notin N_{j+2}$ for some $j \in [t, s-1]$, then we let $g$ be the smallest number in $[t, s - 1]$ such that $c_g \notin N_{g+2}$. We show that $A' = \{1, c_1, \dots, c_{t-1}, y, c_t, \dots, c_{g-1}, c_g\}$ is a circuit. Property (1) holds, as $|A'| = g+1 = n(A')+1$. Property (2) holds, as $1 \in N_1$ by $(ii)$. Property (3) holds, as $c_g \in N_{g+1}$ by $(iv)$. By $(iv)$, we have $c_j \in N_j \cap N_{j+1}$ for all $j$ with $0 < j < t$. By assumption, we have $y \in N_t \cap N_{t+1}$ and $c_j \in N_{j+1} \cap N_{j+2}$ for all $j$ with $t < j < g$. Therefore Property (4) holds. So $A'$ is a circuit.

So $1 \in \text{cl}(X \cup y - x)$ as required. □

**Proposition 15** *Let $M[W, Q]$ be a lattice path matroid on $[n]$ with elements go in the natural order. Then $\Gamma_1(M)$ is ideal and hierarchical with $2 \succeq 3 \succeq \cdots \succeq n$.*

***Proof*** Since a lattice path matroid is transversal, by Theorem 2, it is representable. Therefore $\Gamma_1(M)$ is ideal. We know that $X$ is authorized if and only if $1 \in \mathrm{cl}(X)$. Hence it follows directly from Lemma 14 that $x \succeq y$ if $x < y$. □

**Theorem 16** *An access structure $\Gamma$ is an ideal hierarchical access structure if and only if $\Gamma = \Gamma_p(M)$ for some lattice path matroid $M$ where $p$ is in the head (or the tail) of the natural ordered partition of $M$.*

***Proof*** By Theorem 1, an access structure is ideal and hierarchical if and only if it is isomorphic to an FP access structure $\Gamma([2, n], \mathbf{a}, \mathbf{b})$, where $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_m)$ such that $a_i \le a_{i+1} \le b_i \le b_{i+1}$ for all $i \in [m-1]$. Let $(P_1, \ldots, P_m)$ be the partition of $[2, n]$ in $\Gamma$ such that $P_1 = [2, n_1+1]$, $P_2 = [n_1+2, n_1+n_2+1], \ldots, P_m = [2 + \sum_{i=1}^{m-1} n_i, 1 + \sum_{i=1}^{m} n_i]$. That is $|P_i| = n_i$ for all $i \in [m]$. To complete the proof, we prove the following two claims. □

**Claim 1** *Up to isomorphism, there is a one-to-one correspondence between ideal hierarchical access structures and lattice path matroids.*

By definition of $\Gamma$, $a_k \le a_{k+1} \le b_k \le b_{k+1}$ for all $k \in [m-1]$. The entries of $\mathbf{a}$ can be partition into $c$ parts such that the entries are the same in the same part and different in different parts. That is, there exist $j_1, j_2, \ldots, j_{c-1} \in [m-1]$ such that

$$a_j = \begin{cases} s_1 & \text{if } j \in [1, j_1] \\ s_2 & \text{if } j \in [j_1+1, j_2] \\ \vdots & \\ s_c & \text{if } j \in [j_{c-1}+1, m] \end{cases}$$

and $s_1 < s_2 < \cdots < s_c$. Similarly there exist $i_1, \ldots, i_{d-1} \in [m-1]$ such that

$$b_i = \begin{cases} r_1 & \text{if } i \in [1, i_1] \\ r_2 & \text{if } i \in [i_1+1, i_2] \\ \vdots & \\ r_d & \text{if } i \in [i_{d-1}+1, m] \end{cases}$$

and $r_1 < r_2 < \cdots < r_d$.

Construct a lattice path $Q$ with $d-1$ $EN$ corners such that the $k$-th $EN$ corner is at $1 + \sum_{l=1}^{i_k} n_l$ with height $r_k$ for all $k \in [d-1]$. Construct a lattice path $W$ with $c-1$ $NE$ corners such that the $k$-th $NE$ corner is at $1 + \sum_{l=1}^{j_k} n_l$ with height $s_{k+1}$ for all $k \in [c-1]$. Let $M$ be the matroid with lattice path presentation $(W, Q)$. Then by Theorem 7, $[n_{i_1}+1] \subset [n_{i_1} + n_{i_2} + 1] \subset \cdots \subset [n_{i_1} + \cdots + n_{i_{c-1}} + 1]$ is a chain of fundamental flats with ranks $r_1 < r_2 < \cdots < r_{d-1}$, and $[n_{j_1} + 2, n] \supset [n_{j_2} + 2, n] \supset \cdots \supset [n_{j_c-1} + 2, n]$ is the other chain of fundamental flats with nullities $s_2 < s_3 < \cdots < s_c$.

As discussed in Sect. 2.1, $b_k < 1 + \sum_{j=1}^{k} n_j$ for all $k \in [m]$. Since $a_{k+1} \le b_k < 1 + \sum_{j=1}^{k} n_j$, for all $k \in [m-1]$, the path $W$ never goes above $Q$. The connected lattice path matroid $M[W, Q]$ is well-defined (as illustrated in Fig. 3).

Now suppose $M[W, Q]$ is a connected lattice path matroid that has rank $r$ and nullity $m$. By Theorem 7, $M[W, Q]$ has two chains of fundamental flats: $[i_1] \subset [i_2] \subset \ldots \subset [i_{d-1}]$

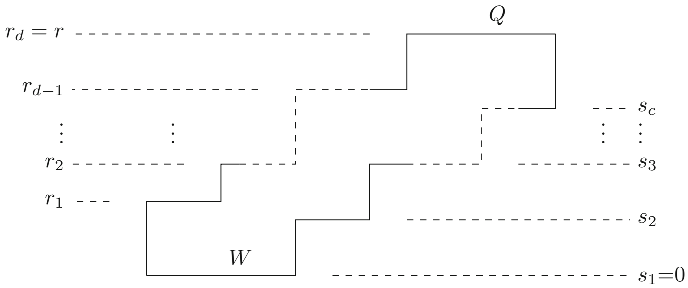


**Fig. 3** Constructing lattice path matroid $M[W, Q]$ from $\Gamma([2, n], \mathbf{a}, \mathbf{b})$

with ranks $r_1 < r_2 < \cdots < r_{d-1}$ and $[j_{c-1}, m + r] \subset \ldots \subset [j_2, m + r] \subset [j_1, m + r]$ with nullities $s_c > s_{c-1} > \cdots > s_2$. Recall that the two chains of fundamental flats give us two different partitions of $[m + r]$: $\pi_1 = \{[i_1], [i_1 + 1, i_2], \ldots, [i_{d-1} + 1, m + r]\}$, and $\pi_2 = \{[j_1 - 1], [j_1, j_2 - 1], \ldots, [j_{c-1}, m + r]\}$. The meet $\pi_1 \wedge \pi_2 = \{[n_1 + 1], [n_1 + 2, n_1 + n_2], \cdots, [n_1 + \cdots + n_{m-1} + 2, m + r]\}$. By Lemma 13, $\{[2, n_1 + 1], [n_1 + 2, n_1 + n_2], \cdots, [n_1 + \cdots + n_{m-1} + 2, m + r]\}$ is the partition of $[2, n]$ with cardinalities $n_1, n_2, \ldots, n_m$ respectively. One reverses the construction given in the first part of the proof, obtain an FP access structure $\Gamma([2, n], \mathbf{a}, \mathbf{b})$. Notice that the path $W$ never goes above $Q$, so $a_{k+1} \le b_k$ for all $k \in [m - 1]$.

**Claim 2** *Let $M[W, Q]$ be the lattice path matroid defined as in the proof of Claim 1 and let $\Gamma_1(M)$ be the port of $M[W, Q]$ at 1. Then $\Gamma_1(M) \cong \Gamma([2, n], \mathbf{a}, \mathbf{b})$.*

Consider the chain of fundamental flats $[n_{i_1} + 1] \subset [n_{i_1} + n_{i_2} + 1] \subset \cdots \subset [n_{i_1} + \cdots + n_{i_{c-1}} + 1]$. For any set $X \subseteq [2, n]$, if $1 \in \text{cl}(X)$, then $\text{cl}(X)$ must be either one of the fundamental flats or the ground set $[n]$. Consider the other chain of fundamental flats $[n_{j_1} + 2, n] \supset [n_{j_2} + 2, n] \supset \cdots \supset [n_{j_c - 1} + 2, n]$. Element 1 is not in any of these flats. So if $X \cap [n_{j_1} + 2, n] \neq \emptyset$, then $|X \cap [n_{j_1} + 1]| \geq s_2$ as required. Similarly, for each $x \in [c - 1]$, if $X \cap [n_{j_x} + 2, n] \neq \emptyset$, then $|X \cap [n_{j_x} + 2]| \geq s_{x+1}$ as required. When these necessary conditions apply to the refinement of the partition of $[2, n]$ obtained from Lemma 13, we have the following statement: if $1 \in \text{cl}(X)$, then

$$\exists_{i \in [m]} \left( |X \cap [2, n_i + 1]| \geq b_i \text{ and } \forall_{j \in [1, i-1]} \left( |X \cap [2, n_j + 1]| \geq a_{j+1} \right) \right). \tag{1}$$

Conversely, suppose $X$ satisfies the condition in (1), we show $1 \in \text{cl}(X)$. Let $i$ be the smallest element in $[m]$ such that $X$ satisfies the condition. That is,

$$|X \cap [2, n_i + 1]| \geq b_i \text{ and } \forall_{j \in [1, i-1]} \left( |X \cap [2, n_j + 1]| \geq a_{j+1} \right). \tag{2}$$

Since $b_i \in \{r_1, \ldots, r_d\}$ is the rank of a fundamental flat that contains 1, if $X$ is independent then $X$ spans the fundamental flat, hence $1 \in \text{cl}(X)$.

Let $l_1, \ldots, l_{s_2}$ be the North steps of $W$ up to the first $NE$ corner. Similarly, let $l_{s_{g-1}+1}, \ldots, l_{s_g}$ be the North steps of $W$ between the $(g - 2)$-th NE-corner (exclusive) and the $(g - 1)$-th NE-corner (inclusive), for all $g \in [2, i]$. Let $l_{s_i+1}, \ldots, l_{b_i}$ be the North steps of $W$ with the smallest labels after the $(i - 1)$-th NE corner and up to the $i$-th NE corner. Then $A = \{l_1, \ldots, l_{s_i}, l_{s_i+1}, \ldots, l_{b_i}\}$ is independent and satisfies condition (1). So $1 \in \text{cl}(A)$. Since $X$ satisfies condition (1), there are at least $s_2$ elements of $X$, say $x_1 < \cdots < x_{s_2}$, are in $[2, 1 + n_1 + \cdots + n_{j_2}]$, that is $x_1, \ldots, x_{s_2}$ are between 2 and the first corner. Since $l_1, \cdots, l_{s_2}$ are the North steps of $W$, it is obvious that $x_1 \leq l_1, x_2 \leq l_2, \ldots, x_{s_2} \leq l_{s_2}$. Use the same argument we can see that there are $b_i$ elements of $X$, say $x_1 < \cdots < x_{b_i}$, such that $x_1 \leq l_1, \ldots, x_{b_i} \leq l_{b_i}$. Applying Lemma 14 repeatedly, obtain $1 \in \mathrm{cl}(\{x_1, \ldots, x_{b_i}\})$, hence $1 \in \mathrm{cl}(X)$. □

## 5 Conjunctive and disjunctive access structures

### 5.1 Nested matroids

Nested matroids, also known as shifted matroids or generalized Catalan matroids, were first introduced by Crapo [9] to show that there are at least $\binom{n}{r}$ nonisomorphic matroids of rank $r$ on $n$ elements. They were later investigated in [21] as a particular kind of transversal matroids, and appeared again in [4] and [6] as a kind of lattice path matroids. They were rediscovered and related to shifted complexes by Ardila [1] and Klivans [16]. For a more detailed history of these matroids, we refer the reader to [4].

In this section, we show that a hierarchical access structure is disjunctive (conjunctive resp.) if and only if it is a matroid port of a nested matroid $M$ at point $p$, where $p$ is in the head (tail resp.) of the natural ordered partition of $M$. The proofs are basically the same as the one for Theorem 16.

The following two propositions were observed by Farràs and Padró in [10].

**Proposition 17** *Suppose that the set of participants $P$ is partitioned into $m$ disjoint subsets $P = \bigcup_{i=1}^{m} P_i$ and let $k_1 < k_2 < \ldots < k_m$ be a sequence of positive integers. Let $\mathbf{k} = (k_1, k_2, \ldots, k_m)$. Then $\Gamma_{\exists}(P, \mathbf{k}) = \Gamma(P, \mathbf{a}, \mathbf{k})$, where $\mathbf{a} = (0, 0, \ldots, 0)$.*

**Proposition 18** *Suppose that the set of participants $P$ is partitioned into $m$ disjoint subsets $P = \bigcup_{i=1}^{m} P_i$ and let $k_1 < k_2 < \ldots < k_m$ be a sequence of positive integers. Let $\mathbf{k} = (k_1, k_2, \ldots, k_m)$. Then $\Gamma_{\forall}(P, \mathbf{k}) = \Gamma(P, \mathbf{a}, \mathbf{b})$, where $\mathbf{a} = (0, k_1, \ldots, k_{m-1})$ and $\mathbf{b} = (k_m, k_m, \ldots, k_m)$.*

**Corollary 19** *An access structure $\Gamma$ is disjunctive hierarchical if and only if there is a nested matroid $M$ on $n$ elements such that $\Gamma = \Gamma_p(M)$ and $p$ is in the head of the partition.*

***Proof*** Let $\Gamma_{\exists}(P, \mathbf{k})$ be a disjunctive hierarchical access structure. By Proposition 17, $\Gamma_{\exists}(P, \mathbf{k}) = \Gamma(P, \mathbf{a}, \mathbf{k})$, where $\mathbf{a} = (0, 0, \ldots, 0)$. Using the same proof in Theorem 16, we can construct lattice paths $W$ and $Q$ to obtain a lattice path presentation $(W, Q)$ for a lattice path matroid $M$. Since $\mathbf{a} = (0, 0, \ldots, 0)$, obtain $W = E^{n-r}N^r$. Since $\mathbf{k} = (k_1, \ldots, k_m)$, for each $i \in [m-1]$, the $i$-th EN corner of $Q$ is at height $k_i$, that is with $k_i$ North steps. The matroid we constructed is a nested matroid $M(E^m N^r, Q)$. Claim 1 shows that there is a one-to-one correspondence between $\Gamma(P, \mathbf{a}, \mathbf{k})$ and nested matroids. Claim 2 shows that $\Gamma(P, \mathbf{a}, \mathbf{k}) = \Gamma_1(M)$. □

**Corollary 20** *An access structure $\Gamma$ is conjunctive hierarchical if and only if there is a nested matroid $M$ on $n$ elements such that $\Gamma = \Gamma_p(M)$ and $p$ is in the tail of the partition.*

***Proof*** Let $\Gamma_{\forall}(P, \mathbf{k})$ be a conjunctive hierarchical access structure. By Proposition 18, $\Gamma_{\forall}(P, \mathbf{k}) = \Gamma(P, \mathbf{a}, \mathbf{b})$, where $\mathbf{a} = (0, k_1, \ldots, k_{m-1})$ and $\mathbf{b} = (k_m, k_m, \ldots, k_m)$. Using the same proof in Theorem 16, we can construct lattice paths $W$ and $Q$ to obtain a lattice path presentation $(W, Q)$ for a lattice path matroid $M$. Since $\mathbf{b} = (k_m, k_m, \ldots, k_m)$, obtain $Q = N^r E^{n-r}$, where $r = k_m$. Since $\mathbf{a} = (0, a_2, \ldots, a_m)$, for each $i \in [m-1]$, the $i$-th EN corner of $W$ is at height $a_i + 1$. By Claim 1, there is a one-to-one correspondence between $\Gamma(P, \mathbf{a}, \mathbf{b})$ and matroid $M$. By Claim 2, we have $\Gamma(P, \mathbf{a}, \mathbf{b}) = \Gamma_1(M)$. Note that rotating the lattice path presentation $(W, Q)$ 180° is a lattice path presentation of a nested matroid, say $N$. We also know that $M$ and $N$ are isomorphic with the labels reversed. Therefore $\Gamma(P, \mathbf{a}, \mathbf{b}) = \Gamma_n(N)$. □

## 6 Conclusion

Farràs and Padró [10] gave a structural characterization of the class of ideal hierarchical access structures. We give a different characterization of this class in terms of matroid ports. An interesting feature of our characterization of ideal hierarchical access structures as ports of lattice path matroids is that these structures only come from the matroid ports at points that belong to one of the ends (head or tail) of the naturally ordered partition of a lattice path matroid. The matroid ports at points not belonging to the ends of the partition are not hierarchical, however, this class of matroid ports corresponds to a more general class of access structures, which might be worth studying. Another class of access structures which might be worth studying is the matroid ports that come from multi-path matroids [5], which are a subclass of transversal matroids that is both minor-closed and duality-closed. This class of matroids properly contains the class of lattice path matroids.

**Acknowledgements** This research is supported by a PhD scholarship from The University of Auckland. The author thanks Prof Arkadii Slinko for his advice and the reviewers for their useful suggestions.

## References

1. Ardila F.: The catalan matroid. J. Comb. Theory Ser. A **104**(1), 49–62 (2003).
2. Beimel A.: Secret-sharing schemes: a survey. In: Chee Y.M., Guo Z., Ling S., Shao F., Tang Y., Wang H., Xing C. (eds.) Coding and Cryptology, vol. 6639, pp. 11–46. Lecture Notes in Computer Science. Springer, Berlin (2011).
3. Blakley G.R.: Safeguarding cryptographic keys. AFIPS Conf. Proc. **48**, 313–317 (1979).
4. Bonin J., de Mier A.: Lattice path matroids: structural properties. Eur. J. Comb. **27**(5), 701–738 (2006).
5. Bonin J., Giménez O.: Multi-path matroids. Comb. Probab. Comput. **16**(2), 193–217 (2007).
6. Bonin J., de Mier A., Noy M.: Lattice path matroids: enumerative aspects and Tutte polynomials. J. Comb. Theory Ser. A **104**(1), 63–94 (2003).
7. Brickell E.: Some ideal secret sharing schemes. J. Comb. Math. Comb. Comput. **9**, 105–113 (1989).
8. Brickell E., Davenport D.: On the classification of ideal secret sharing schemes. J. Cryptol. **4**, 123–134 (1991).
9. Crapo H.: Single-element extensions of matroids. J. Res. Natl. Bureau Stand. B **69B**, 55–65 (1965).
10. Farràs O., Padró C.: Ideal hierarchical secret sharing schemes. IEEE Trans. Inf. Theory **58**(5), 3273–3286 (2012).
11. Farràs O., Martí-Farré J., Padró C.: Ideal multipartite secret sharing schemes. J. Cryptol. **25**, 434–463 (2012).
12. Gvozdeva T., Hameed A., Slinko A.: Weightedness and structural characterization of hierarchical simple games. Math. Soc. Sci. **65**(3), 181–189 (2013).
13. Hameed A., Slinko A.: A characterisation of ideal weighted secret sharing schemes. J. Math. Cryptol. **9**(4), 227–244 (2015).
14. Ito M., Saito A., Nishizeki T.: Secret sharing scheme realizing any access structure. Proc. IEEE Glob. **87**, 99–102 (1987).
15. Karnin E.D., Greene J.W., Hellman M.E.: On secret sharing systems. IEEE Trans. Inf. Theory **29**, 35–41 (1983).
16. Klivans C.: Combinatorial properties of shifted complexes. Doctoral dissertation, Massachusetts Institute of Technology (2003).

17. Lehman A.: A solution of the Shannon switching game. J. Soc. Ind. Appl. Math. **12**, 687–725 (1964).
18. Martí-Farré J., Padró C.: On secret sharing schemes, matroids and polymatroids. J. Math. Cryptol. **4**, 95–120 (2010).
19. Matúš F.: Matroid representations by partitions. Discret. Math. **203**(1–3), 169–194 (1999).
20. Oxley J.: Matroid Theory, 2. Oxford University Press, New York (2011).
21. Oxley J., Prendergast K., Row D.: Matroids whose ground sets are domains of functions. J. Austral. Math. Soc. Ser. A **32**, 380–387 (1982).
22. Padró C., Sáez G.: Secret sharing schemes with bipartite access structure. IEEE Trans. Inf. Theory **46**(7), 2596–2604 (2000).
23. Padró C., Sáez G.: Correction to "Secret sharing schemes with bipartite access structure". IEEE Trans. Inf. Theory **50**(6), 1373 (2004).
24. Piff M.J., Welsh D.J.A.: On the vector representation of matroids. J. Lond. Math. Soc. **2**, 284–288 (1970).
25. Seymour P.D.: On secret-sharing matroids. J. Comb. Theory Ser. B **56**(1), 69–73 (1992).
26. Shamir A.: How to share a secret. Commun. ACM **22**, 612–613 (1979).
27. Simonis J., Ashikhmin A.: Almost affine codes. Des. Codes Cryptogr. **14**, 179–197 (1998).
28. Stinson D.R.: An explication of secret sharing schemes. Des. Codes Cryptogr. **2**(4), 357–390 (1992).
29. Tassa T.: Hierarchical threshold secret sharing. J. Cryptol. **20**, 237–264 (2007).
30. Taylor A.D., Zwicker W.S.: Simple Games: Desirability Relations, Trading, Pseudoweightings. Princeton University Press, Princeton (1999).

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.