

On Representable Matroids and Ideal Secret Sharing

Chingfang Hsu^{1✉} Qi Cheng²

¹Information Security Lab, College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, China

²Engineering Department, Institute of Wuhan Digital Engineering, Wuhan, China

Abstract

In secret sharing, the exact characterization of ideal access structures is a longstanding open problem. Brickell and Davenport (J. of Cryptology, 1991) proved that ideal access structures are induced by matroids. Subsequently, ideal access structures and access structures induced by matroids have attracted a lot of attention. Due to the difficulty of finding general results, the characterization of ideal access structures has been studied for several particular families of access structures. In all these families, all the matroids that are related to access structures in the family are representable and, then, the matroid-related access structures coincide with the ideal ones.

In this paper, we study the characterization of representable matroids. By using the well known connection between ideal secret sharing and matroids and, in particular, the recent results on ideal multipartite access structures and the connection between multipartite matroids and discrete polymatroids, we obtain a characterization of a family of representable multipartite matroids, which implies a sufficient condition for an access structure to be ideal.

By using this result and further introducing the reduced discrete polymatroids, we provide a complete characterization of quadripartite representable matroids, which was until now an open problem, and hence, all access structures related to quadripartite representable matroids are the ideal ones. By the way, using our results, we give a new and simple proof that all access structures related to unipartite, bipartite and tripartite matroids coincide with the ideal ones.

Keywords: Cryptography, Ideal secret sharing schemes, Ideal access structures, Representable multipartite matroids, Discrete polymatroids.

1 Introduction

Secret-sharing schemes, which were introduced by Shamir [1] and Blakley [2] nearly 30 years ago, are nowadays used in many cryptographic protocols. In these schemes there is a finite set of participants, and a collection Γ of subsets of the participants (called the access structure). A secret-sharing scheme for Γ is a method by which a dealer distributes shares of a secret value to the participants such that (1) any subset in Γ can reconstruct the secret from its shares, and (2) any subset not in Γ cannot reveal any partial information about the secret in the information theoretic sense. Clearly, the access structure Γ must be monotone, that is, all supersets of a set in Γ are also in Γ .

Ito, Saito, and Nishizeki [3] proved that there exists a secret-sharing scheme for every monotone access structure. Their proof is constructive, but the obtained schemes are very inefficient: the ratio between the length in bits of the shares and that of the secret is exponential in the number of parties. Nevertheless, some access structures admit secret-sharing schemes with much shorter shares. A secret-sharing scheme is called ideal if the shares of every participant are taken from the same domain as the secret. As proved in [4], this is the optimal size for the domain of the shares. The access structures which can be realized by ideal secret-sharing schemes are called ideal access structures.

The exact characterization of ideal access structures is a longstanding open problem, which has interesting connections to combinatorics and information theory. The most important result towards giving such characterization is by Brickell and Davenport [5], who proved that every ideal access structure is induced by a matroid (that is, matroid-related), providing a necessary condition for an access structure to be ideal. A sufficient condition is obtained as a consequence of the linear construction of ideal secret-sharing schemes due to Brickell [6]. Namely, an access structure is ideal if it is induced by a matroid that is representable over some finite field. However, there is a gap between the necessary condition and the sufficient condition. Seymour [7] proved that the access structures induced by the Vamos matroid are not ideal. Other examples of non-ideal access structures induced by matroids have been presented by Matus [8]. Hence, the necessary condition above is not sufficient. Moreover, Simonis and Ashikmin [9] constructed ideal secret-sharing schemes for the access structures induced by the non-Pappus matroid, which is not representable over any field. This means that the sufficient condition is not necessary. The results in [5] have been generalized in [10] by proving that, if all shares in a secret sharing scheme are shorter than $3/2$ times the secret value, then its access structure is matroid-related.

Due to the difficulty of finding general results, the characterization of ideal access structures has been studied for several particular families of access structures: the access structures on sets of four [11] and five [12] participants, the access structures defined by graphs [13, 14, 15, 16, 17], the bipartite access structures [18], the access structures with three or four minimal qualified subsets [19], the access structures with intersection number equal to one [20], the access structures with rank three [21, 22], and the weighted threshold access structures [23]. In all these families, all the matroids that are related to access structures in the family are representable and, then, the matroid-related access structures coincide with the ideal ones.

In addition, several authors studied this open problem for multipartite access structures since every access structure can be seen as a multipartite access structure. Multipartite access structure, informally, is that the set of participants can be divided into several parts in such a way that all participants in the same part play an equivalent role in the structure. Since we can always consider as many parts as participants, every access structure is multipartite (in the same way, every matroid is multipartite). More accurately, we can consider in any access structure the partition that is derived from a suitable equivalence relation on the set of participants.

Multipartite access structures were first introduced by Shamir [1] in his seminal work, in which weighted threshold access structures were considered. Beimel, Tassa and Weinreb [23] presented a characterization of the ideal weighted threshold access structures that generalizes the partial results in [24, 18]. Another important result about weighted threshold access structures has been obtained recently by Beimel and Weinreb [25]. They prove that all such access structures admit secret sharing schemes in which the size of the shares is quasi-polynomial in the number of users. A complete characterization of the ideal bipartite access structures was given in [18], and related results were given independently in [26, 27]. Partial results on the characterization of the ideal tripartite access structures appeared in [28, 29], and this question was solved in [30]. Another important result about a complete characterization of the ideal hierarchical access structures has been obtained recently by Farras and Padro [31]. They prove that every ideal hierarchical access structure is induced by a representable matroid. In every one of these families of multipartite access structures, all access structures are related to representable matroids, and hence, they are all ideal access structures.

In this paper we continue the line of research of those previous works by studying the following question: which matroids are representable? Specifically, we are not restricting ourselves to a particular

family of access structures related to representable matroids, but we study the characterization of representable matroids. By using the well known connection between ideal secret sharing and matroids and, in particular, the recent results on ideal multipartite access structures and the connection between multipartite matroids and discrete polymatroids, we obtain a characterization of a family of representable multipartite matroids (since every matroid and every access structure are multipartite, this sufficient condition is a general result), which implies a sufficient condition for an access structure to be ideal. Further, using this result and introducing the reduced discrete polymatroids, we provide a complete characterization of quadripartite representable matroids, which was until now an open problem, and hence, all access structures related to quadripartite representable matroids are the ideal ones. By the way, using our results, we give a new and simple proof that all access structures related to unipartite, bipartite and tripartite matroids coincide with the ideal ones. More specifically, our results are the following:

1. By using a group of inequalities related to the rank functions of the associated discrete polymatroids, a characterization of a family of representable multipartite matroids is present (that is, Theorem 3.2), and hence, all access structures related to this family of representable multipartite matroids are the ideal ones.
2. Using Theorem 3.2, we give a new and simple proof that every unipartite, bipartite and tripartite discrete polymatroid is representable, which implies all access structures related to unipartite, bipartite and tripartite matroids coincide with the ideal ones.
3. By using Theorem 3.2 and introducing the definition of D -reduction, we obtain a complete characterization of quadripartite representable matroids (that is, Theorem 5.3), which was until now an open problem, and hence, all access structures related to quadripartite representable matroids are the ideal ones.

2 Definitions and Preliminaries

In this section we review some basic definitions and notations in [30] that will be used through the paper. The reader is referred to [33] for an introduction to secret sharing and to [34, 35] for general references on Matroid Theory.

A matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is formed by a finite set \mathcal{Q} together with a family $\mathcal{I} \subseteq \mathcal{P}(\mathcal{Q})$ ($\mathcal{P}(\mathcal{Q})$ is the power set of the set \mathcal{Q} .) such that

1. $\emptyset \in \mathcal{I}$, and
2. if $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$, and
3. if $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there exists $x \in I_2 - I_1$ such that $I_1 \cup \{x\} \in \mathcal{I}$.

The set \mathcal{Q} is the ground set of the matroid \mathcal{M} and the elements of \mathcal{I} are called the independent sets of \mathcal{M} . The bases of the matroid are the maximally independent sets. All bases have the same number of elements, which is the rank of \mathcal{M} .

Let \mathbb{K} be a field. A matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is \mathbb{K} -representable (or representable for short) if there exists a matrix M over \mathbb{K} whose columns are indexed by the elements of \mathcal{Q} such that a subset $I = \{i_1, \dots, i_k\} \subseteq \mathcal{Q}$ is independent if and only if the corresponding columns of M are independent. In this situation, we say that the matrix M is a \mathbb{K} -representation of the matroid \mathcal{M} .

Let \mathbb{K} be a finite field and let $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ be a \mathbb{K} -representable matroid. Let $p_0 \in \mathcal{Q}$ be special participant called dealer. and $\mathcal{Q} = P \cup \{p_0\}$. For every $k \times (n+1)$ matrix M representing \mathcal{M} over \mathbb{K} , let E be a vector space of finite dimension $\dim E = k$ over \mathbb{K} . For every $i \in \mathcal{Q}$, we define a surjective linear mapping: $\pi_i : E \rightarrow \mathbb{K}$, and the i -th column of M corresponds to the linear form π_i . In that situation, for every random choice of an element $x \in E$, we can obtain $s_i = \pi_i(x) \in \mathbb{K}$ is the share of the participant $i \in P$ and $s = \pi_{p_0}(x) \in \mathbb{K}$ is the shared secret value. Hence, by the columns of M , we define an ideal secret sharing scheme with access structure $\Gamma_{p_0}(\mathcal{M})$, where $\min \Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\}$. Therefore, the access structures induced by representable matroids are ideal.

We write $\mathcal{P}(P)$ for the power set of the set P . An m -partition $\Pi = \{P_1, \dots, P_m\}$ of a set P is a disjoint family of m nonempty subsets of P with $P = P_1 \cup \dots \cup P_m$. Let $\Lambda \subseteq \mathcal{P}(P)$ be a family of subsets of P . For a permutation σ on P , we define $\sigma(\Lambda) = \{\sigma(A) : A \in \Lambda\} \subseteq \mathcal{P}(P)$. A family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is said to be Π -partite if $\sigma(\Lambda) = \Lambda$ for every permutation σ such

that $\sigma(P_i) = P_i$ for every $P_i \in \Pi$. We say that Λ is m -partite if it is Π -partite for some m -partition Π . These concepts can be applied to access structures and matroids.

For every integer $m \geq 1$, we consider the set $J_m = \{1, \dots, m\}$. Let \mathbb{Z}_+^m denote the set of vectors $u = (u_1, \dots, u_m) \in \mathbb{Z}^m$ with $u_i \geq 0$ for every $i \in J_m$. For a partition $\Pi = \{P_1, \dots, P_m\}$ of a set P and for every $A \subseteq P$ and $i \in J_m$, we define $\Pi_i(A) = |A \cap P_i|$. Then the partition Π defines a mapping $\Pi: \mathcal{P}(P) \rightarrow \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A), \dots, \Pi_m(A))$. If $\Lambda \subseteq \mathcal{P}(P)$ is Π -partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda)$. That is, Λ is completely determined by the partition Π and the set of vectors $\Pi(\Lambda) \subset \mathbb{Z}_+^m$.

Discrete polymatroids, a combinatorial object introduced by Herzog and Hibi [32], are closely related to multipartite matroids and, because of that, they play an important role in the characterization of ideal multipartite access structures. Before giving the definition of discrete polymatroid, we need to introduce some notation. If $u, v \in \mathbb{Z}_+^m$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J_m$, and we write $u < v$ if $u \leq v$ and $u \neq v$. The vector $w = u \vee v$ is defined by $w_i = \max(u_i, v_i)$. The modulus of a vector $u \in \mathbb{Z}_+^m$ is $|u| = u_1 + \dots + u_m$. For every subset $X \subseteq J_m$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^{|X|}$ and $|u(X)| = \sum_{i \in X} u_i$.

A discrete polymatroid on the ground set J_m is a nonempty finite set of vectors $D \subset \mathbb{Z}_+^m$ satisfying:

1. if $u \in D$ and $v \in \mathbb{Z}_+^m$ is such that $v \leq u$, then $v \in D$, and
2. for every pair of vectors $u, v \in D$ with $|u| < |v|$, there exists $w \in D$ with $u < w \leq u \vee v$.

The next proposition, which is easily proved from the axioms of the independent sets of a matroid, shows the relation between multipartite matroids and discrete polymatroids.

Proposition 2.1. Let Π be a partition of a set \mathcal{Q} and let $\mathcal{I} \subseteq \mathcal{P}(\mathcal{Q})$ be a Π -partite family of subsets. Then \mathcal{I} is the family of the independent sets of a Π -partite matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ if and only if $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is a discrete polymatroid.

A basis of a discrete polymatroid D is a maximal element in D , that is, a vector $u \in D$ such that there does not exist any $v \in D$ with $u < v$. Similarly to matroids, a discrete polymatroid is determined by its bases. Specifically, the following result is proved in [32, Theorem 2.3].

Proposition 2.2. A nonempty subset $\mathcal{B} \subset \mathbb{Z}_+^m$ is the family of bases of a discrete polymatroid if and only if it satisfies:

1. all elements in \mathcal{B} have the same modulus, and
2. for every $u \in \mathcal{B}$ and $v \in \mathcal{B}$ with $u_i > v_i$, there exists $j \in J_m$ such that $u_j < v_j$ and $u - e_i + e_j \in \mathcal{B}$, where e_i denotes the i -th vector of the canonical basis of \mathbb{Z}^m .

The rank function of a discrete polymatroid D with ground set J_m is the function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ defined by $h(X) = \max \{|u(X)| : u \in D\}$. The next proposition is a consequence of [32, Theorem 3.4].

Proposition 2.3. A function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ is the rank function of a discrete polymatroid with ground set J_m if and only if it satisfies

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

Moreover, a polymatroid D is completely determined by its rank function. Specifically, $D = \{u \in \mathbb{Z}_+^m : |u(X)| \leq h(X) \text{ for all } X \subseteq J_m\}$.

Let \mathbb{K} be a field, E a \mathbb{K} -vector space, and V_1, \dots, V_m subspaces of E . It is not difficult to check that the mapping $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of a discrete polymatroid $D \subset \mathbb{Z}_+^m$. In this situation, we say that D is \mathbb{K} -representable and the subspaces V_1, \dots, V_m are a \mathbb{K} -representation of D . The next proposition is proved in [30, Theorem 7.1]

Proposition 2.4. Let $\mathcal{M}=(\mathcal{Q},\mathcal{I})$ be a Π -partite matroid and let $D=\Pi(\mathcal{I})$ be its associated discrete polymatroid. If \mathcal{M} is \mathbb{K} -representable, then so is D . In addition, if D is \mathbb{K} -representable, then \mathcal{M} is representable over some finite extension of \mathbb{K} .

3 A Characterization of A Family of Representable Matroids

In this section, by using a group of inequalities related to the rank functions of the associated discrete polymatroids, a characterization of a family of representable multipartite matroids is present, and hence, all access structures related to this family of representable multipartite matroids are the ideal ones.

We firstly define the associated discrete polymatroids of this family of multipartite matroids as follow.

Definition 3.1. Let $D \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m and rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. We say that D is a normalized discrete polymatroid if the rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ of D is such that $h(X) = h(J_m)$, where $X \subseteq J_m$ and $|X| \geq 3$.

It is not difficult to check that for all unipartite, bipartite and tripartite matroids, the associated discrete polymatroids are normalized ones.

The main goal of this section is to obtain the following theorem, which is proved in the appendix.

Theorem 3.2. Let $D \subset \mathbb{Z}_+^m$ be a normalized discrete polymatroid with ground set J_m and rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. D is \mathbb{K} -representable if and only if there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ such that for every $i, j, k \in J_m$,

$$\sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_m}} r(A) = h(\{i\}), \quad (3-1)$$

$$\sum_{\substack{A \cap \{i,j\} \neq \emptyset \\ A \subseteq J_m}} r(A) = h(\{i, j\}), \quad (3-2)$$

$$\sum_{\substack{A \cap \{i,j,k\} \neq \emptyset \\ A \subseteq J_m}} r(A) \geq h(\{i, j, k\}) = h(J_m), \quad (3-3)$$

where every element of R is a nonnegative integer and $|R| = C_m^1 + C_m^2 + \dots + C_m^m$.

As a consequence, from Proposition 2.4, Theorem 3.2 provides a characterization of a family of representable multipartite matroids, the associated discrete polymatroids of which are the normalized ones.

The further importance of Theorem 3.2 is that it provides a sufficient condition for a multipartite access structure to be ideal. Namely, a multipartite access structure is ideal if it is of the form $\Gamma_{p_0}(\mathcal{M})$, where $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is a Π -partite matroid and $\Pi(\mathcal{I})$ is the associated discrete polymatroid D which is a normalized one and there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied.

In addition, the interest of Theorem 3.2 goes beyond its implications to secret sharing. The characterization of the representable discrete polymatroids was until now an open problem. By using Theorem 3.2, this problem will be smoothly solved if the representability of a discrete polymatroid can be characterized by the representability of a normalized discrete polymatroid. Therefore, Theorem 3.2 is an interesting new result about representability of matroids.

4 Operations on Discrete Polymatroids

In this section, by dealing with the rank function of a discrete polymatroid, we introduce the definitions on the ΔH -set of a discrete polymatroid and the reduced discrete polymatroid respectively, which will be very useful in the characterization of quadripartite representable matroids.

Definition 4.1. Let $D \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m and rank function $h : \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. We say that an integer set $\Delta H = \{\Delta h(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ defined by

$$\begin{aligned} \Delta h(\{i\}) &= h(J_m) - h(J_m \setminus \{i\}), \\ \Delta h(\{i, j\}) &= h(J_m) - h(J_m \setminus \{i, j\}) - \Delta h(\{i\}) - \Delta h(\{j\}), \\ \Delta h(\{i, j, k\}) &= h(J_m) - h(J_m \setminus \{i, j, k\}) - \sum_{\substack{A \subseteq \{i, j, k\} \\ A \neq \emptyset}} \Delta h(A), \\ &\dots, \end{aligned}$$

$$\Delta h(J_m \setminus \{j\}) = h(J_m) - h(\{j\}) - \sum_{\substack{A \subseteq J_m \setminus \{j\} \\ A \neq \emptyset}} \Delta h(A), \text{ and}$$

$$\Delta h(J_m) = h(J_m) - \sum_{\substack{A \subseteq J_m \\ A \neq \emptyset}} \Delta h(A),$$

is the ΔH -set of D , where $i, j, k \in J_m$ and $|\Delta H| = C_m^1 + C_m^2 + \dots + C_m^m$.

In this situation, it is not difficult to check that

$$h(\{i\}) = \sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_m}} \Delta h(A),$$

$$h(\{i, j\}) = \sum_{\substack{A \cap \{i, j\} \neq \emptyset \\ A \subseteq J_m}} \Delta h(A),$$

...

$$h(J_m) = \sum_{\substack{A \subseteq J_m \\ A \neq \emptyset}} \Delta h(A).$$

Lemma 4.2. From Proposition 2.3 and Definition 4.1, observe that for all $i, j \in J_m$,

$$\Delta h(\{i\}) = h(J_m) - h(J_m - \{i\}) \geq 0,$$

$$\Delta h(\{i, j\}) = h(J_m - \{i\}) + h(J_m - \{j\}) - h(J_m - \{i, j\}) - h(J_m) \geq 0.$$

These imply that for $m \leq 2$ all elements of ΔH -set of a discrete polymatroid are bound to nonnegative integers, but for $m \geq 3$ one or more negative integers may be present.

Definition 4.3. Let $D \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m and rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. We say that a discrete polymatroid D_r with ground set J_m is the reduced discrete polymatroid of D if the rank function $h_r: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ of D_r is such that $h_r(X) = h(X) - \sum_{i \in X} \Delta h(i)$ for every $X \subseteq J_m$, where $\Delta h(i) = h(J_m) - h(J_m - \{i\})$.

It is not difficult to check that for every $j \in J_m$, $h_r(J_m \setminus \{j\}) = h_r(J_m) = \sum_{i \in J_m} h(J_m - \{i\}) - (m-1)h(J_m)$, which is an important property of the reduced discrete polymatroids. In the appendix, the next proposition is proved.

Proposition 4.4. Let D be a discrete polymatroid with ground set J_m and rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. Let D_r be the associated reduced discrete polymatroid with ground set J_m and rank function $h_r: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. If D is \mathbb{K} -representable, then so is D_r . In addition, if D_r is \mathbb{K} -representable, then D is \mathbb{K} -representable.

As a consequence, the representability of a discrete polymatroid can be completely characterized by the representability of the associated reduced discrete polymatroid.

5 A Characterization of Quadripartite Representable Matroids

In this section, by using the ΔH -set of discrete polymatroids and the associated reduced discrete polymatroids of quadripartite matroids, we obtain a complete characterization of quadripartite representable matroids, which was until now an open problem, and hence, all access structures related to quadripartite representable matroids are the ideal ones.

Since the associated discrete polymatroids are the normalized ones, by using Theorem 3.2, we firstly give the complete characterizations of unipartite, bipartite and tripartite representable matroids respectively.

Example 5.1. Consider a discrete polymatroid D with ground set J_m and rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$.

For $m \leq 2$, from Lemma 4.2, all elements of ΔH -set of D are bound to nonnegative integers. We can construct a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ such that $R = \Delta H$. Hence, from Theorem 3.2, D is representable over some finite field.

As a consequence, all unipartite and bipartite matroids are representable, then access structures induced by unipartite and bipartite matroids are ideal ones, which has been done in [18], and also in [30].

Example 5.2. (Following Example 5.1)

For $m = 3$, $J_3 = \{1, 2, 3\}$ and from Definition 4.1, the ΔH -set of D is $\Delta H = \{\Delta h(A) : \text{for all } A \subseteq J_3 \text{ and } A \neq \emptyset\}$ defined by

$$\Delta h(\{i\}) = h(J_3) - h(J_3 \setminus \{i\}), \quad (5-1)$$

$$\Delta h(\{i, j\}) = h(J_3) - h(J_3 \setminus \{i, j\}) - \Delta h(\{i\}) - \Delta h(\{j\}), \quad (5-2)$$

$$\Delta h(J_3) = h(J_3) - \sum_{\substack{A \subseteq J_3 \\ A \neq \emptyset}} \Delta h(A). \quad (5-3)$$

From Lemma 4.2, it is easily seen that all elements of ΔH -set of D except $\Delta h(J_3)$ are nonnegative integers.

If $\Delta h(J_3) \geq 0$, we can construct a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_3 \text{ and } A \neq \emptyset\}$ such that $R = \Delta H$. From Theorem 3.2, D is representable over some finite field.

If $\Delta h(J_3) < 0$, from Theorem 3.2, D is \mathbb{K} -representable if and only if there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_3 \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied. We can suppose that there exist $h'(J_3) > h(J_3)$ and a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_3 \text{ and } A \neq \emptyset\}$ such that for every $i, j \in J_3$,

$$\sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_3}} r(A) = h(\{i\}), \quad (5-4)$$

$$\sum_{\substack{A \cap \{i, j\} \neq \emptyset \\ A \subseteq J_3}} r(A) = h(\{i, j\}), \quad (5-5)$$

$$\sum_{\substack{A \neq \emptyset \\ A \subseteq J_3}} r(A) = h'(J_3). \quad (5-6)$$

Together with (5-1)-(5-6), we obtain that for every $i, j \in J_3$,

$$r(\{i\}) = h'(J_3) - h(J_3 \setminus \{i\}) \geq 0,$$

$$r(\{i, j\}) = \Delta h(\{i, j\}) + h(J_3) - h'(J_3) \geq 0,$$

$$r(J_3) = \Delta h(J_3) - h(J_3) + h'(J_3) \geq 0.$$

The above inequalities can be merged into $h(J_3) - \Delta h(J_3) \leq h'(J_3) \leq h(J_3) + \Delta h(\{i, j\})$ since from $\Delta h(J_3) < 0$ and $\Delta h(J_3) + \Delta h(\{i, j\}) = h(\{i\}) + h(\{j\}) - h(\{i, j\}) \geq 0$, we obtain that

$h(J_3 \setminus \{i\}) \leq h(J_3) \leq h(J_3) - \Delta h(J_3) \leq h(J_3) + \Delta h(\{i, j\})$. Hence, the value range of $h'(J_3)$ is $h(J_3) - \Delta h(J_3) \leq h'(J_3) \leq h(J_3) + \min(\Delta h(\{i, j\}), \Delta h(\{i, k\}), \Delta h(\{j, k\}))$, where $i, j, k \in J_3$.

Namely, we can find a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_3 \text{ and } A \neq \emptyset\}$ such that (5-1)-(5-3) are satisfied. From Theorem 3.2, D is representable over some finite field.

As a consequence, all tripartite matroids are representable and all access structures induced by tripartite matroids are ideal ones, which has been done in [30].

Following this line of research, in order to characterize quadripartite representable matroids by using Theorem 3.2, we first need to deal with every quadripartite matroid such that the representability of the associated discrete polymatroid can be characterized by the representability of a normalized discrete polymatroid, that is, $h(J_4 \setminus \{i\}) = h(J_4)$ for every $i \in J_4$, which is exactly the property of the associated reduced discrete polymatroid.

Hence, to characterize quadripartite representable matroids is equivalent to characterize the representable reduced discrete polymatroids with ground set J_4 , which are equally the normalized discrete polymatroids. From Theorem 3.2, we need to determine whether there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied, which is the main goal of this section.

In the next theorem, we give the complete characterization of representable quadripartite matroids, which is proved in the appendix.

Theorem 5.3. A quadripartite matroid is representable if and only if for the associated reduced discrete polymatroid D_r there exist five nonnegative integers $h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\})$ and $h'(J_4)$ such that for every $i, j, k, g \in J_4$ the following inequalities are satisfied:

1. $h_r(J_4) \leq h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\}) \leq h'(J_4)$, and
2. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) - h'(J_4) \geq h_r(J_4) - \Delta h(\{i, j\})$, and
3. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) - h'(J_4) \leq 2h_r(J_4) + \Delta h(\{i, j, k\})$, and
4. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) + h'(J_4 \setminus \{g\}) - h'(J_4) \geq 3h_r(J_4) - \Delta h(J_4)$,

where $h_r(J_4), \Delta h(\{i, j\}), \Delta h(\{i, j, k\})$ and $\Delta h(J_4)$ are the values of the rank function and ΔH -set of D_r respectively.

According to Theorem 5.3, if a quadripartite matroid is representable, the values of $h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\})$ and $h'(J_4)$ can be calculated, and then we can determine a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied, from which we can construct a \mathbb{K} -representation of the associated discrete polymatroid according to the proof of Theorem 3.2.

Therefore, after all representable quadripartite matroids are characterized, all access structures related to quadripartite representable matroids are the ideal ones.

We need to highlight that since there exist ideal access structures related to non-representable matroids, to characterize representable quadripartite matroids is not equivalent to characterize the ideal access structures related to quadripartite matroids.

Example 5.4. The Vamos matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is a known non-representable matroid, which is defined on $\mathcal{Q} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ with bases all 4-sets except the five 4-sets which are: $\{1, 2, 3, 4\}, \{1, 2, 5, 6\}, \{1, 2, 7, 8\}, \{3, 4, 5, 6\}, \{3, 4, 7, 8\}$.

For the Vamos matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$, we consider a partition $\Pi = \{P_1, P_2, P_3, P_4\}$ of the ground set \mathcal{Q} with $P_1 = \{1, 2\}, P_2 = \{3, 4\}, P_3 = \{5, 6\}, P_4 = \{7, 8\}$, and then, the partition Π defines a mapping $\Pi: \mathcal{P}(\mathcal{Q}) \rightarrow \mathbb{Z}_+^4$, from which we obtain the associated discrete polymatroid $D = \Pi(\mathcal{I})$ with ground set $J_4 = \{1, 2, 3, 4\}$. The rank function $h: \mathcal{P}(J_4) \rightarrow \mathbb{Z}$ of $D = \Pi(\mathcal{I})$ are as following:

$$\begin{aligned} h(\{1\}) &= h(\{2\}) = h(\{3\}) = h(\{4\}) = 2, \\ h(\{1, 2\}) &= h(\{1, 3\}) = h(\{1, 4\}) = h(\{2, 3\}) = h(\{2, 4\}) = 3, \quad h(\{3, 4\}) = 4, \\ h(\{1, 2, 3\}) &= h(\{1, 2, 4\}) = h(\{1, 3, 4\}) = h(\{2, 3, 4\}) = 4, \\ h(\{1, 2, 3, 4\}) &= 4. \end{aligned}$$

From Definition 3.1, the associated discrete polymatroid D of the Vamos matroid is a normalized discrete polymatroid. Namely, the associated reduced discrete polymatroid $D_r = D$. All elements of the ΔH -set of D_r are calculated as follow:

$$\begin{aligned}\Delta h(\{1\}) &= \Delta h(\{2\}) = \Delta h(\{3\}) = \Delta h(\{4\}) = 0, \\ \Delta h(\{1,3\}) &= \Delta h(\{1,4\}) = \Delta h(\{2,3\}) = \Delta h(\{2,4\}) = \Delta h(\{3,4\}) = 1, \quad \Delta h(\{1,2\}) = 0, \\ \Delta h(\{1,2,3\}) &= \Delta h(\{1,2,4\}) = 0, \quad \Delta h(\{1,3,4\}) = \Delta h(\{2,3,4\}) = -1, \\ \Delta h(\{1,2,3,4\}) &= 1.\end{aligned}$$

According to Theorem 5.3, suppose that there exist five nonnegative integers $h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\})$ and $h'(J_4)$ such that

1. $4 \leq h'(J_4 \setminus \{1\}), h'(J_4 \setminus \{2\}), h'(J_4 \setminus \{3\}), h'(J_4 \setminus \{4\}) \leq h'(J_4)$, and
2. $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{2\}) - h'(J_4) \geq 4 - \Delta h(\{1,2\}) = 4$, and
 $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{3\}) - h'(J_4) \geq 4 - \Delta h(\{1,3\}) = 3$, and
 $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \geq 4 - \Delta h(\{1,4\}) = 3$, and
 $h'(J_4 \setminus \{2\}) + h'(J_4 \setminus \{3\}) - h'(J_4) \geq 4 - \Delta h(\{2,3\}) = 3$, and
 $h'(J_4 \setminus \{2\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \geq 4 - \Delta h(\{2,4\}) = 3$, and
 $h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \geq 4 - \Delta h(\{3,4\}) = 3$, and
3. $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{2\}) + h'(J_4 \setminus \{3\}) - h'(J_4) \leq 8 + \Delta h(\{1,2,3\}) = 8$, and
 $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{2\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \leq 8 + \Delta h(\{1,2,4\}) = 8$, and
 $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \leq 8 + \Delta h(\{1,3,4\}) = 7$, and
 $h'(J_4 \setminus \{2\}) + h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \leq 8 + \Delta h(\{2,3,4\}) = 7$, and
4. $h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{2\}) + h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) - h'(J_4) \geq 12 - \Delta h(J_4) = 11$,

From the above inequalities, we obtain that

$$\begin{aligned}h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{2\}) + 2h'(J_4 \setminus \{3\}) + 2h'(J_4 \setminus \{4\}) - 2h'(J_4) &= 14, \text{ and} \\ h'(J_4 \setminus \{1\}) + h'(J_4 \setminus \{2\}) &= 8, \text{ and}\end{aligned}$$

$$h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) - h'(J_4) = 3, \text{ and}$$

$$h'(J_4) = 4, \text{ and}$$

$$h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) = 7.$$

Obviously, $h'(J_4 \setminus \{3\}) + h'(J_4 \setminus \{4\}) = 7$ is contradictory to the inequality $4 \leq h'(J_4 \setminus \{1\}), h'(J_4 \setminus \{2\}), h'(J_4 \setminus \{3\}), h'(J_4 \setminus \{4\}) \leq h'(J_4)$. This is a contradiction. It implies that there does not exist five nonnegative integers $h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\})$ and $h'(J_4)$ such that the above inequalities are satisfied. Therefore, the Vamos matroid is non-representable over any field.

6 Conclusions

In this paper, by introducing the normalized discrete polymatroids, we obtain a characterization of a family of representable multipartite matroids, which implies a sufficient condition for an access structure to be ideal. Further, using this result and introducing the reduced discrete polymatroids, we provide a complete characterization of quadripartite representable matroids, which was until now an open problem, and hence, all access structures related to quadripartite representable matroids are the ideal ones. By the way, using our results, we give a new and simple proof that all access structures related to unipartite, bipartite and tripartite matroids coincide with the ideal ones. Our results are potentially interesting to solve the open problem, that is, which matroids induce ideal access structures?

Appendix

Theorem 3.2. Let $D \subset \mathbb{Z}_+^m$ be a normalized discrete polymatroid with ground set J_m and rank function $h : \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. D is \mathbb{K} -representable if and only if there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ such that for every $i, j, k \in J_m$,

$$\sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_m}} r(A) = h(\{i\}), \quad (3-1)$$

$$\sum_{\substack{A \cap \{i,j\} \neq \emptyset \\ A \subseteq J_m}} r(A) = h(\{i, j\}), \quad (3-2)$$

$$\sum_{\substack{A \cap \{i,j,k\} \neq \emptyset \\ A \subseteq J_m}} r(A) \geq h(\{i, j, k\}) = h(J_m), \quad (3-3)$$

where every element of R is a nonnegative integer and $|R| = C_m^1 + C_m^2 + \dots + C_m^m$.

Proof: We begin by proving the necessary condition in the statement of Theorem 3.2. Suppose that D is \mathbb{K} -representable. Then there exists a \mathbb{K} -representation of D consisting of subspaces V_1, \dots, V_m of the \mathbb{K} -vector space $E = \mathbb{K}^s$, where $s = h(J_m)$. It implies that for every $X \subseteq J_m$, $h(X) = \dim(\sum_{i \in X} V_i)$. Consider a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ defined by

$$\begin{aligned} r(J_m) &= \dim(\bigcap_{i \in J_m} V_i), \\ r(J_m \setminus \{j\}) &= \dim(\bigcap_{i \in J_m \setminus \{j\}} V_i) - r(J_m), \\ &\dots, \\ r(A) &= \dim(\bigcap_{i \in A} V_i) - \sum_{\substack{A \subset X \\ X \subseteq J_m}} r(X), \end{aligned}$$

where $j \in J_m$, $A \subseteq J_m$ and $A \neq \emptyset$. Then we obtain that for every $i, j, k \in J_m$,

$$\begin{aligned} \sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_m}} r(A) &= \dim(V_i) = h(\{i\}), \\ \sum_{\substack{A \cap \{i,j\} \neq \emptyset \\ A \subseteq J_m}} r(A) &= \dim(V_i + V_j) = h(\{i, j\}), \text{ and} \\ \sum_{\substack{A \cap \{i,j,k\} \neq \emptyset \\ A \subseteq J_m}} r(A) &= \dim(V_i + V_j + V_k) = h(\{i, j, k\}) = h(J_m). \end{aligned}$$

Hence, there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied.

The proof for the sufficient condition in the theorem is much more involved. Assume now that there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_m \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied. Naturally, we obtain that for every $i, j, k, g \in J_m$,

$$\begin{aligned} \sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_m}} r(A) &= h(\{i\}), \\ \sum_{\substack{A \cap \{i, j\} \neq \emptyset \\ A \subseteq J_m}} r(A) &= h(\{i, j\}), \\ \sum_{\substack{A \cap \{i, j, k\} \neq \emptyset \\ A \subseteq J_m}} r(A) &\geq h(\{i, j, k\}) = h(J_m), \\ \sum_{\substack{A \cap \{i, j, k, g\} \neq \emptyset \\ A \subseteq J_m}} r(A) &\geq h(\{i, j, k, g\}) = h(J_m), \quad (3-4) \\ &\dots, \quad (\dots) \\ \sum_{\substack{A \neq \emptyset \\ A \subseteq J_m}} r(A) &\geq h(J_m). \quad (3-m) \end{aligned}$$

Let $s = h(J_m)$ and $E = \mathbb{K}^s$ be a s -dimensional vector space over some finite field \mathbb{K} with $|\mathbb{K}| \geq \sum_{\substack{A \neq \emptyset \\ A \subseteq J_m}} r(A)$. Given a basis $\{v_1, \dots, v_s\}$ of E , consider the mapping $\mathbf{v} : \mathbb{K} \rightarrow E$ defined by

$\mathbf{v}(x) = \sum_{i=1}^s x^{i-1} v_i$. Observe that the vectors $\mathbf{v}(x)$ have Vandermonde coordinates with respect to the given basis of E . This implies that every set of at most s vectors of the form $\mathbf{v}(x)$ is independent (this property is very important to the following proof).

Consider $t = |R|$ disjoint sets $S_1, \dots, S_t \subseteq \{\mathbf{v}(x) : x \in \mathbb{K}\} \subset E$ with $|S_i| = f(i)$ ($1 \leq i \leq t$), where $f : \{1, \dots, t\} \rightarrow R$ is a bijection which associates each i ($1 \leq i \leq t$) with an element of R .

From (3-m), we obtain that $\sum_{i=1}^t |S_i| = \sum_{\substack{A \neq \emptyset \\ A \subseteq J_m}} r(A) \geq s$, where every set of at most s vectors in

S_1, \dots, S_t are independent.

According to (3-1), we construct m subspaces $V_1, \dots, V_m \subseteq E$ such that for every $j \in J_m$, V_j is spanned by $\bigcup_{\sum |S_i|=h(\{j\})} S_i$ respectively. In this situation, from (3-1) and (3-2), we obtain that for every $i, j \in J_m$, the dimensions $\dim(V_i) = h(\{i\})$ and $\dim(V_i + V_j) = h(\{i, j\})$. From (3-3)-(3-m), there hold that for $|A| \geq 3$ and $A \subseteq J_m$, the dimensions $\dim(\sum_{j \in A} V_j) = h(A) = h(J_m)$ since every set of at most $s = h(J_m)$ vectors in S_1, \dots, S_t are independent. Hence, for all $A \subseteq J_m$, the dimensions $\dim(\sum_{j \in A} V_j) = h(A)$ hold. These imply that m subspaces V_1, \dots, V_m of the vector space $E = \mathbb{K}^s$ is a \mathbb{K} -representation of D . Namely, D is representable over \mathbb{K} .

Proposition 4.4. Let D be a discrete polymatroid with ground set J_m and rank function $h: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. Let D_r be the associated reduced discrete polymatroid with ground set J_m and rank function $h_r: \mathcal{P}(J_m) \rightarrow \mathbb{Z}$. If D is \mathbb{K} -representable, then so is D_r . In addition, if D_r is \mathbb{K} -representable, then D is \mathbb{K} -representable.

Proof: We begin by proving the first claim in the statement of Proposition 4.1. Suppose that D is \mathbb{K} -representable. Then there exists a \mathbb{K} -representation of D consisting of subspaces V_1, \dots, V_m of the \mathbb{K} -vector space $E = \mathbb{K}^s$, where $s = h(J_m)$. For every $i \in J_m$, consider two subspaces $U_i, W_i \subseteq E$ such that $U_i = \sum_{j \in J_m - \{i\}} V_j$ and $E = U_i \oplus W_i$. Since $s = h(J_m) = \dim(E)$ and $h(J_m - \{i\}) = \dim(\sum_{j \in J_m - \{i\}} V_j)$, we deduce that $\Delta r(i) = \dim(W_i)$. On the other hand, $W_i \subseteq V_i$ because $E = U_i + V_i$ and $E = U_i \oplus W_i$. Consider two subspaces $R_i, W_i \subseteq V_i$ such that $V_i = R_i \oplus W_i$. Since $E = U_i \oplus W_i$ and $V_i = R_i \oplus W_i$, we obtain that $\dim(\sum_{i \in X} V_i) = \dim(\sum_{i \in X} R_i \oplus W_i) = \dim(\sum_{i \in X} R_i) + \sum_{i \in X} \dim(W_i)$, where

$\dim(\sum_{i \in X} V_i) = h(X)$ and $\sum_{i \in X} \dim(W_i) = \sum_{i \in X} \Delta r(i)$, and hence, $\dim(\sum_{i \in X} R_i) = h_r(X)$. Therefore, the subspaces R_1, \dots, R_m of the \mathbb{K} -vector space $E' = \mathbb{K}^{s'}$ are a \mathbb{K} -representation of D_r , where $s' = h(J_m) - \sum_{i \in J_m} \Delta r(i)$.

The proof for the second claim in the theorem is similar to the first. Assume now that D_r is \mathbb{K} -representable. Then there exists a \mathbb{K} -representation of D_r consisting of subspaces R_1, \dots, R_m of the \mathbb{K} -vector space $E' = \mathbb{K}^{s'}$, where $s' = h(J_m) - \sum_{i \in J_m} \Delta r(i)$. Consider two subspaces $E', W \subseteq E = \mathbb{K}^s$ such that $E = E' \oplus W$, where $s = h(J_m)$. Then $\dim(W) = \sum_{i \in J_m} \Delta r(i)$. Consider the subspaces $W_1, \dots, W_m \subseteq W$ such that $W = W_1 \oplus \dots \oplus W_m$, where $\dim(W_i) = \Delta r(i)$. Let $V_i = R_i \oplus W_i$. Since $E = E' \oplus W$ and $E' = \sum_{i \in J_m} R_i$, we obtain that $\dim(\sum_{i \in X} V_i) = \dim(\sum_{i \in X} R_i) + \sum_{i \in X} \dim(W_i)$ and, hence, the subspaces V_1, \dots, V_m of the \mathbb{K} -vector space $E = \mathbb{K}^s$ are a \mathbb{K} -representation of D , where $s = h(J_m)$.

As a consequence, the representable reduced discrete polymatroids can characterize the representable discrete polymatroids.

Theorem 5.3. A quadripartite matroid is representable if and only if for the associated reduced discrete polymatroid D_r there exist five nonnegative integers $h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\})$ and $h'(J_4)$ such that for every $i, j, k, g \in J_4$ the following inequalities are satisfied:

1. $h_r(J_4) \leq h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\}) \leq h'(J_4)$, and
2. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) - h'(J_4) \geq h_r(J_4) - \Delta h(\{i, j\})$, and
3. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) - h'(J_4) \leq 2h_r(J_4) + \Delta h(\{i, j, k\})$, and
4. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) + h'(J_4 \setminus \{g\}) - h'(J_4) \geq 3h_r(J_4) - \Delta h(J_4)$,

where $h_r(J_4), \Delta h(\{i, j\}), \Delta h(\{i, j, k\})$ and $\Delta h(J_4)$ are the values of the rank function and ΔH -set of D_r , respectively.

Proof: For $m = 4$, $J_4 = \{1, 2, 3, 4\}$. According to Definition 4.3, the associated reduced discrete polymatroid D_r with rank function $h_r : \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ is obtained. From Proposition 4.4, in order to determine the representability of D , we just determine the representability of D_r .

From the rank function $h_r : \mathcal{P}(J_m) \rightarrow \mathbb{Z}$ of D_r , the ΔH -set of D_r is $\Delta H = \{\Delta h(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ defined by

$$\Delta h(\{i\}) = h_r(J_4) - h_r(J_4 \setminus \{i\}) = 0, \quad (5-7)$$

$$\Delta h(\{i, j\}) = h_r(J_4) - h_r(J_4 \setminus \{i, j\}) - \Delta h(\{i\}) - \Delta h(\{j\}), \quad (5-8)$$

$$\Delta h(\{i, j, k\}) = h_r(J_4) - h_r(J_4 \setminus \{i, j, k\}) - \sum_{\substack{A \subseteq \{i, j, k\} \\ A \neq \emptyset}} \Delta h(A), \quad (5-9)$$

$$\Delta h(J_4) = h_r(J_4) - \sum_{\substack{A \subseteq J_4 \\ A \neq \emptyset}} \Delta h(A). \quad (5-10)$$

From Lemma 4.2, it is easily seen that for all $i, j, k \in J_4$, all elements of ΔH -set of D_r except $\Delta h(\{i, j, k\})$ and $\Delta h(J_4)$ are nonnegative integers.

If $\Delta h(\{i, j, k\}) \geq 0$ and $\Delta h(J_4) \geq 0$ for all $i, j, k \in J_4$, we can construct a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ such that $R = \Delta H$. From Theorem 3.2, D_r is representable over some finite field.

If there exist one or more negative integers in the values of $\Delta h(\{i, j, k\})$ and $\Delta h(J_4)$ for all $i, j, k \in J_4$. From Theorem 3.2, D_r is \mathbb{K} -representable if and only if there exists a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ such that (3-1)-(3-3) are satisfied. Suppose that there exist $h'(\{i, j, k\}) \geq h_r(\{i, j, k\})$ for every $i, j, k \in J_4$, $h'(J_4) \geq h_r(J_4)$ and a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ such that for every $i, j, k \in J_4$,

$$\sum_{\substack{A \cap \{i\} \neq \emptyset \\ A \subseteq J_4}} r(A) = h_r(\{i\}), \quad (5-11)$$

$$\sum_{\substack{A \cap \{i, j\} \neq \emptyset \\ A \subseteq J_4}} r(A) = h_r(\{i, j\}), \quad (5-12)$$

$$\sum_{\substack{A \cap \{i,j,k\} \neq \emptyset \\ A \subseteq J_4}} r(A) = h'(\{i, j, k\}), \quad (5-13)$$

$$\sum_{\substack{A \neq \emptyset \\ A \subseteq J_4}} r(A) = h'(J_4). \quad (5-14)$$

Together with (5-7)-(5-14), we obtain that for every $i, j, k, g \in J_4$,

$$r(\{i\}) = h'(J_4) - h'(J_4 \setminus \{i\}) \geq 0,$$

$$r(\{i, j\}) = h'(J_4 \setminus \{j\}) - h_r(J_4) + \Delta h(\{i, j\}) + h'(J_4 \setminus \{i\}) - h'(J_4) \geq 0,$$

$$r(\{i, j, k\}) = h'(J_4) - h'(J_4 \setminus \{i\}) - h'(J_4 \setminus \{j\}) - h'(J_4 \setminus \{k\}) + 2h_r(J_4) + \Delta h(\{i, j, k\}) \geq 0,$$

$$r(J_4) = h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) + h'(J_4 \setminus \{g\}) - 3h_r(J_4) + \Delta h(J_4) + h'(J_4 \setminus \{i\}) - h'(J_4) \geq 0.$$

To sum up, a nonnegative integer set $R = \{r(A) : \text{for all } A \subseteq J_4 \text{ and } A \neq \emptyset\}$ can be found if there exist five nonnegative integers $h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\})$ and $h'(J_4)$ such that for every $i, j, k, g \in J_4$ the following inequalities are satisfied:

1. $0 \leq h'(J_4 \setminus \{i\}), h'(J_4 \setminus \{j\}), h'(J_4 \setminus \{k\}), h'(J_4 \setminus \{g\}) \leq h'(J_4)$, and
2. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) - h'(J_4) \geq h(J_4) - \Delta h(\{i, j\})$, and
3. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) - h'(J_4) \leq 2h(J_4) + \Delta h(\{i, j, k\})$, and
4. $h'(J_4 \setminus \{i\}) + h'(J_4 \setminus \{j\}) + h'(J_4 \setminus \{k\}) + h'(J_4 \setminus \{g\}) - h'(J_4) \geq 3h(J_4) - \Delta h(J_4)$.

Acknowledgment

The authors would like to express their gratitude to Prof. Keith Martin, Royal Holloway, University of London, for motivating discussions on the topic in October 2009. The final version of this paper is based on the inspiring discussion with Dr. Siaw-Lynn Ng, Royal Holloway, University of London, in the spring of 2010.

References

- [1] A. Shamir. How to share a secret. *Commun. of the ACM*, 22 (1979) pp. 612-613.
- [2] G.R. Blakley, Safeguarding cryptographic keys. *AFIPS Conference Proceedings*. 48 (1979) 313-317.
- [3] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, pages 99-102, 1987.
- [4] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35-41, 1983.
- [5] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123-134, 1991.
- [6] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. And Combin. Comput.*, 6:105-113, 1989.
- [7] P.D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B*, 56 (1992) pp. 69-73.
- [8] F. Matus. Matroid representations by partitions. *Discrete Math.* 203 (1999) 169-194.
- [9] J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179-197, 1998.
- [10] J. Marti-Farre, C. Padro. On Secret Sharing Schemes, Matroids and Polymatroids. *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Computer Science 4392 (2007) 273-290.*
- [11] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* 2 (1992) 357-390.
- [12] W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* 9 (1996) 267-286.
- [13] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptogr.* 11 (1997) 107-122.
- [14] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92, Lecture Notes in Comput. Sci.* 740 148-167.
- [15] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* 8 (1995) 39-64.
- [16] E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* 4 (1991) 123-134.
- [17] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. Cryptology* 6 (1993) 157-168.
- [18] C. Padro, G. Saez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* 46 (2000) 2596-2604.
- [19] J. Marti-Farre, C. Padro. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes*

- Cryptogr. 34 (2005) 17-34.
- [20] J. Marti-Farre, C. Padro. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics* 154 (2006) 552-563.
- [21] J. Marti-Farre, C. Padro. Secret sharing schemes on sparse homogeneous access structures with rank three. *Electronic Journal of Combinatorics* 11(1) (2004) Research Paper 72, 16 pp. (electronic).
- [22] J. Marti-Farre, C. Padro. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Fifth Conference on Security and Cryptography for Networks, SCN 2006, Lecture Notes in Comput. Sci.*, to appear.
- [23] A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Comput. Sci.* 3378 (2005) 600-619.
- [24] P. Morillo, C. Padro, G. Saez, J. L. Villar. Weighted Threshold Secret Sharing Schemes. *Inf. Process. Lett.* 70 (1999) 211-216.
- [25] A. Beimel, E. Weinreb. Monotone Circuits for Monotone Weighted Threshold Functions. *Information Processing Letters* 97 (2006) 12-18.
- [26] S.-L. Ng. A Representation of a Family of Secret Sharing Matroids. *Des. Codes Cryptogr.* 30 (2003) 5-19.
- [27] S.-L. Ng, M. Walker. On the composition of matroids and ideal secret sharing schemes. *Des. Codes Cryptogr.* 24 (2001) 49-67.
- [28] M.J. Collins. A Note on Ideal Tripartite Access Structures. *Cryptology ePrint Archive, Report 2002/193*, <http://eprint.iacr.org/2002/193>.
- [29] J. Herranz, G. Saez. New Results on Multipartite Access Structures. *IEE Proceedings of Information Security* 153 (2006) 153-162.
- [30] Oriol Farras, Jaume Martí Farré, Carles Padró. Ideal Multipartite Secret Sharing Schemes. *Advances in Cryptology, EUROCRYPT 2007, Lecture Notes in Comput. Sci.* 4515 (2007) 448-465.
- [31] Oriol Farras, Carles Padró. Ideal Hierarchical Secret Sharing Schemes. *7th Theory of Cryptography Conference, TCC 2010, Lecture Notes in Comput. Sci.* 5978 (2010) 219-236.
- [32] J. Herzog, T. Hibi. Discrete polymatroids. *J. Algebraic Combin.* 16 (2002) 239-268.
- [33] S.-L. Ng. Ideal secret sharing schemes with multipartite access structures *IEE Proc.-Commun.* 153 (2006) 165-168.
- [34] J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
- [35] D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.