On Non-representable Secret Sharing Matroids

Qi Cheng[1,*], Yong Yin[1], Kun Xiao[1], and Ching-Fang Hsu[2]

[1] Engineering Department, Wuhan Digital Engineering Institute, Wuhan, China
[2] College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, China
cherryjingfang@gmail.com

Abstract. The characterization of the access structures of ideal secret sharing schemes is one of the main open problems in secret sharing and has important connections with matroid theory. Because of its difficulty, it has been studied for several particular families of access structures. Multipartite access structures, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role, have been studied in seminal works on secret sharing by Shamir, Simmons, and Brickell, and also recently by several authors.. In the EUROCRYPT'07, Farras made a important contribution to this work: By using discrete polymatroids, they obtained a necessary condition and a sufficient condition for a multipartite access structure to be ideal respectively. In particular, they further gave a very difficult open problem, that is, characterizing the representable discrete polymatroids, i.e., which discrete polymatroids are representable and which ones are non-representable. In this paper, by dealing with a family of matroids derived from the Vamos matroid, which was the first matroid that was proved to be non-representable, we obtain a family of non-representable matroids. As a consequence, we extend it to the general case and obtain a sufficient condition for a discrete polymatroid to be non-representable, which is a new contribution to the open problem given by Farras.

Keywords: Ideal secret sharing schemes, Ideal access structures, Multipartite access structures, Discrete polymatroids, Vamos matroid.

1 Introduction

Secret sharing schemes were introduced independently by Shamir [2] and Blakley [1] in 1979. In a secret sharing scheme, every participant receives a share of a secret value. Only the qualified sets of participants, which form the access structure of the scheme, can recover the secret value from their shares. This paper deals exclusively with unconditionally secure perfect secret sharing schemes, that is, the shares of the participants in a non-qualified set do not provide any information about the secret value.

The length of the shares is the main measure of the complexity of secret sharing schemes. In general, the shares must be much larger than the secret. An access structure is said to be ideal if it admits an ideal secret sharing scheme. The characterization

[*] Corresponding author.

F. Bao, H. Li, and G. Wang (Eds.): ISPEC 2009, LNCS 5451, pp. 124–135, 2009.

of ideal access structures is one of the main open problems in secret sharing and has important connections with matroid theory.

A necessary condition for an access structure to be ideal was given by Brickell and Davenport [4], who proved that every ideal access structure is matroid-related. Matroids that are obtained from ideal secret sharing schemes are said to be secret sharing representable (or ss-representable for short). Vamos matroid was the first matroid that was proved to be non-ss-representable. Nevertheless, as a consequence of the results in [3], all representable matroids (that is, matroid that can be represented by a matrix over some finite field) are ss-representable. This implies a sufficient condition for an access structure to be ideal. Namely, an access structure is ideal if it is related to a representable matroid.

Due to the difficulty of finding general results, the characterization of ideal access structures has been studied for several particular classes of access structures. 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. More accurately, we can consider in any access structure the partition that is derived from a suitable equivalence relation on the set of participants. Because of its practical interest, secret sharing for multipartite access structures has been studied by several authors[2,3,5,6,7,8].

Recently, in the EUROCRYPT'07, Farras[9] made a important contribution to this work by using discrete polymatroids. In particular, for solving the main open problems in secret sharing, they further gave a very difficult open problem, that is, characterizing the representable discrete polymatroids, i.e., which discrete polymatroids are representable and which ones are non-representable. In this paper, by dealing with a family of matroids derived from the Vamos matroid, which was the first matroid that was proved to be non-representable, we obtain a family of non-representable matroids. As a consequence, we extend it to the general case and obtain a sufficient condition for a discrete polymatroid to be non-representable, which is a new contribution to the open problem given by Farras.

2 Definitions and Preliminaries

In this section we review some basic definitions and notations that will be used through the paper.

2.1 Matroids and Ideal Secret Sharing

The reader is referred to [12] for an introduction to secret sharing and to [10, 11] 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. $\phi \in \mathcal{I}$, 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 $I_1 \bigcup \{x\} \in \mathcal{I}$.

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. The family $\mathcal{B}$ of the bases determines the matroid. Moreover, by [10, Theorem 1.2.5], $\mathcal{B} \subseteq \mathcal{P}(\mathcal{Q})$ is the family of bases of a matroid on $\mathcal{Q}$ if and only if

1. $\mathcal{B}$ is nonempty, and
2. for every $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, there exists $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \bigcup \{y\}$ is in $\mathcal{B}$.

All bases have the same number of elements, which is the rank of $\mathcal{M}$ and is denoted $r(\mathcal{M})$. The dependent sets are those that are not independent. A circuit is a minimally dependent subset. A matroid is said to be connected if, for every two points $x, y \in \mathcal{Q}$, there exists a circuit C with $x, y \in C$. The rank of $X \subseteq \mathcal{Q}$, which is denoted $r(X)$, is the maximum cardinality of the subsets of X that are independent. Observe that the rank of $\mathcal{Q}$ is the rank of the matroid $\mathcal{M}$ that was defined before. The rank function $r : \mathcal{P}(\mathcal{Q}) \to \mathbb{Z}$ of a matroid satisfies

1. $0 \leq r(X) \leq |X|$ for every $X \subseteq \mathcal{Q}$, and
2. r is monotone increasing: if $X \subseteq Y \subseteq \mathcal{Q}$, then $r(X) \leq r(Y)$, and
3. r is submodular: $r(X \bigcap Y) + r(X \bigcup Y) \leq r(X) + r(Y)$ for every $X, Y \subseteq \mathcal{Q}$.

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 $I = \{i_1, \ldots, i_k\} \subseteq \mathcal{Q}$ 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 $\mathcal{Q} = P \bigcup \{p_0\}$. For every $k \times (n+1)$ matrix M representing $\mathcal{M}$ over $\mathbb{K}$, let E be a vector space of finite dimention $\dim E = k$ over $\mathbb{K}$. For every $i \in \mathcal{Q}$, we define a surjective linear mapping: $\pi_i : E \to \mathbb{K}$, 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 $\Gamma_{p_0}(\mathcal{M})$. Therefore, the access structures that are related to representable matroids are ideal.

2.2 Multipartite Access Structures and Multipartite Matroids

We write $\mathcal{P}(P)$ for the power set of the set P. An m-partition $\Pi = \{P_1, \ldots, P_m\}$ of a set P is a disjoint family of m nonempty subsets of P with $P = P_1 \cup \ldots \cup P_m$. 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, which are actually families of subsets, and they can be applied as well to the family of independent sets of a matroid. A matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is Π-partite if $\mathcal{I} \subseteq \mathcal{P}(\mathcal{Q})$ is Π-partite.

Let $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ be a connected matroid and, for a point $p_0 \in \mathcal{Q}$, let $\Pi = \{P_1, \ldots, P_m\}$ and $\Pi_0 = \{\{p_0\}, P_1, \ldots, P_m\}$ be partitions of the sets $P = \mathcal{Q} - \{p_0\}$ and $\mathcal{Q}$ respectively. Then the access structure $\Gamma = \Gamma_{p_0}(\mathcal{M})$ is Π-partite if and only if the matroid $\mathcal{M}$ is Π_0-partite.

The partition Π' is a refinement of the partition Π if every set in Π' is a subset of some set in Π. Clearly, if $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite and Π' is a refinement of Π, then Λ is Π'-partite. Among all partitions Π for which a family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite, there exists a partition Π_Λ that is not a refinement of any other such partition. Following [13], we consider the following equivalence relation: two elements $p, q \in P$ are said to be equivalent according to Λ if the transposition τ_{pq} satisfies $\tau_{pq}(\Lambda) = \Lambda$. The partition Π_Λ is the one defined by this equivalence relation. It is not difficult to check that Λ is Π-partite if and only if Π is a refinement of Π_Λ.

For every integer $m \geq 1$, we consider the set $J_m = \{1, \ldots, m\}$. Let $\mathbb{Z}_+^m$ denote the set of vectors $u = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ with $u_i \geq 0$ for every $i \in J_m$. For a partition $\Pi = \{P_1, \ldots, P_m\}$ 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 $\Pi : \mathcal{P}(P) \to \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A), \ldots, \Pi_m(A))$. 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 [13], 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 $u \le v$ if $u_i \le v_i$ for every $i \in J_m$, and we write $u < v$ if $u \le v$ and $u \ne v$. 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 $|u| = u_1 + \cdots + u_m$. 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 $v \le u$, then $v \in D$, and
2. for every pair of vectors $u, v \in D$ with $|u| < |v|$, there exists $w \in D$ with $u < w \le u \vee v$.

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 [13, 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 $h : \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \max\{|u(X)| : u \in D\}$. The next proposition is a consequence of [13, Theorem 3.4].

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

1. $h(\phi) = 0$, and
2. h is monotone increasing: if $X \subseteq Y \subseteq J_m$, then $h(X) \le h(Y)$, and
3. h is submodular: if $X, Y \subseteq J_m$, then $h(X \bigcup Y) + h(X \bigcap Y) \le h(X) + h(Y)$.

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

For a discrete polymatroid D with ground set J_m and for every $X \subseteq J_m$, we define the discrete polymatroid $D(X)$ with ground set X by $D(X) = \{u(X) : u \in D\} \subset \mathbb{Z}_+^{|X|}$. This concept will be very useful in this paper.

Let $\mathbb{K}$ be a field, E a $\mathbb{K}$-vector space, and $V_1, \ldots, V_m$ subspaces of E. It is not difficult to check that the mapping $h : \mathcal{P}(J_m) \to \mathbb{Z}$ 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 $V_1, \ldots, V_m$ are a $\mathbb{K}$-representation of D. The next proposition is proved in [9, 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 Family of Non-representable Secret Sharing Matroids

In this section, we give a family of non-representable matroids derived from the Vamos matroid. Firstly, we introduce the Vamos matroid and give the proof of Vamos matroid being a non-representable multipartite matroid. Afterwards, through combining the partition of the ground set of Vamos matroid, we construct three "matroids", which are proved to be non-representable. However, according to the definition of matroid, we obtain these three "matroids" are pseudo matroids. Finally, from the concept of $D(X)$ defined above, a family of non-representable matroids derived from the Vamos matroid is obtained, which we call Vamos Family.

3.1 Vamos Matroid

The definition of Vamos matroid is as follows:

Definition 3.1. The Vamos matroid 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: $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,2,7,8\}$,$\{3,4,5,6\}$,$\{3,4,7,8\}$.

The following proposition gives a new proof of the Vamos matroid being a non-representable multipartite matroid.

Proposition 3.1. The Vamos matroid is non-representable.

Proof. For a partition $\Pi_0 = \{P_1, P_2, P_3, P_4\}$ ($P_1 = \{1,2\}, P_2 = \{3,4\}, P_3 = \{5,6,\}, P_4 = \{7,8\}$) of the ground set $\mathcal{Q}$, the partition Π_0 defines a mapping $\Pi_0 : \mathcal{P}(\mathcal{Q}) \to \mathbb{Z}_+^4$. For every non-basis 4-set A, we compute $\Pi_0(A)$ and obtain $(2,2,0,0),(2,0,2,0),(2,0,0,2),(0,2,2,0),(0,2,0,2)$. Similarly, for every basis B , we compute $\Pi_0(B)$ and obtain $(1,1,1,1),(1,1,2,0),(1,1,0,2),(1,2,1,0),(1,2,0,1),(1,0,1,2),$ $(1,0,2,1),$ $(0,1,1,2),$ $(0,1,2,1),$ $(0,2,1,1),$ $(2,1,0,1),(2,1,1,0),(2,0,1,1),(0,0,2,2)$. We can verify that for every 3-set C, there must exist a basis B such that $\Pi_0(C) < \Pi_0(B)$ and $C \subset B$. Therefore, all 3-sets are independent.

Suppose that over some finite field $\mathbb{K}$ there exists a matrix M which is a representation of the Vamos matroid, and every element $i \in \mathcal{Q}$ correspond to the column vector v_i of M . Apparently, all vectors of M are non-zero vectors. Arbitrary four column vectors of M are linearly independent except (v_1,v_2,v_3,v_4) , (v_1,v_2,v_5,v_6) , (v_1,v_2,v_7,v_8) , (v_3,v_4,v_5,v_6) , (v_3,v_4,v_7,v_8) . Because all 3-sets are independent, for every one of these five vector groups, its rank is 3 and every vector in it can be uniquely represented by the other three vectors over $\mathbb{K}$. The following operations are over the finite field $\mathbb{K}$:

For the vector group (v_1,v_2,v_7,v_8), let $v_8 = a_1v_1 + a_2v_2 + a_7v_7$ (1)

For the vector group (v_3,v_4,v_7,v_8), let $v_8 = a_3v_3 + a_4v_4 + a_7{}'v_7$. (2)

where $a_1,a_2,a_7,a_3,a_4,a_7{}' \in \mathbb{K}$ and $a_1,a_2,a_7,a_3,a_4,a_7{}' \neq 0$.
Simultaneous equations (1)(2), then

$$(a_7{}' - a_7)v_7 = a_1v_1 + a_2v_2 - a_3v_3 - a_4v_4 \tag{3}$$

For the vector group (v_1, v_2, v_3, v_4), let $v_4 = b_1v_1 + b_2v_2 + b_3v_3$ (4)

where $b_1, b_2, b_3 \in \mathbb{K}$ and $b_1, b_2, b_3 \neq 0$.

If $(a_7 '- a_7) \neq 0$, then simultaneous equations (3)(4) and we obtain (v_1, v_2, v_3, v_7) are linearly dependent. Since $\{1,2,3,7\}$ is a basis of the Vamos matroid, a contradiction. Hence, there must be $(a_7 '- a_7) = 0$, that is $a_7 ' = a_7$, then from equation (3) we obtain:

$$a_1v_1 + a_2v_2 = a_3v_3 + a_4v_4 \quad (5)$$

For the vector group (v_1, v_2, v_5, v_6), let $v_6 = c_1v_1 + c_2v_2 + c_5v_5$ (6)

For the vector group (v_3, v_4, v_5, v_6), let $v_6 = c_3v_3 + c_4v_4 + c_5 'v_5$ (7)

Similarly, we can obtain $c_5 = c_5 '$ and $c_1v_1 + c_2v_2 = c_3v_3 + c_4v_4$ (8)

Computing equation $c_1(5) - a_1(8)$, then:

$$(a_2c_1 - a_1c_2)v_2 = (a_3c_1 - a_1c_3)v_3 + (a_4c_1 - a_1c_4)v_4 \quad (9)$$

Because (v_2, v_3, v_4) are linearly independent, then $a_2c_1 - a_1c_2 = 0$ (10)

Computing equation $c_1(1) - a_1(6)$, then:

$$c_1v_8 - a_1v_6 = (a_2c_1 - a_1c_2)v_2 + a_7c_1v_7 - a_1c_5v_5 \quad (11)$$

Simultaneous equations (10)(11), then $c_1v_8 - a_1v_6 = a_7c_1v_7 - a_1c_5v_5$ (12)

Due to $a_1, c_1, a_7, c_5 \neq 0$, from equation (12) we can obtain (v_5, v_6, v_7, v_8) are linearly dependent. Since $\{5,6,7,8\}$ is a basis of the Vamos matroid, a contradiction. Therefore, it is impossible that there exists a matrix M over some finite field $\mathbb{K}$ which is a representation of the Vamos matroid, that is, the Vamos matroid is non-representable.

3.2 Three Non-representable Pseudo Matroids

Through combining the partition of the ground set of Vamos matroid, we construct three "matroids" as follow:

Definition 3.2. The Pseudo-1 matroid is defined on $\mathcal{Q} = \{1,2,3,4,5,6,7,8\}$ with bases all 4-sets except the thirteen 4-sets which are: $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,2,5,7\}$, $\{1,2,5,8\}$, $\{1,2,6,7\}$, $\{1,2,6,8\}$, $\{1,2,7,8\}$, $\{3,4,5,6\}$, $\{3,4,5,7\}$, $\{3,4,5,8\}$, $\{3,4,6,7\}$, $\{3,4,6,8\}$, $\{3,4,7,8\}$.

Definition 3.3. The Pseudo-2 matroid is defined on $\mathcal{Q} = \{1,2,3,4,5,6,7,8\}$ with bases all 4-sets except the thirteen 4-sets which are: $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,3,5,6\}$, $\{1,4,5,6\}$, $\{2,3,5,6\}$, $\{2,4,5,6\}$, $\{3,4,5,6\}$, $\{1,2,7,8\}$, $\{1,3,7,8\}$, $\{1,4,7,8\}$, $\{2,3,7,8\}$, $\{2,4,7,8\}$, $\{3,4,7,8\}$.

Definition 3.4. The Pseudo-3 matroid is defined on $\mathcal{Q} = \{1,2,3,4,5,6,7,8\}$ with bases all 4-sets except the thirty-seven 4-sets which are: $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,3,5,6\}$, $\{1,4,5,6\}$, $\{2,3,5,6\}$, $\{2,4,5,6\}$, $\{3,4,5,6\}$, $\{1,2,5,7\}$, $\{1,3,5,7\}$, $\{1,4,5,7\}$, $\{2,3,5,7\}$, $\{2,4,5,7\}$, $\{3,4,5,7\}$, $\{1,2,5,8\}$, $\{1,3,5,8\}$, $\{1,4,5,8\}$, $\{2,3,5,8\}$, $\{2,4,5,8\}$, $\{3,4,5,8\}$, $\{1,2,6,7\}$, $\{1,3,6,7\}$, $\{1,4,6,7\}$, $\{2,3,6,7\}$, $\{2,4,6,7\}$, $\{3,4,6,7\}$, $\{1,2,6,8\}$, $\{1,3,6,8\}$, $\{1,4,6,8\}$, $\{2,3,6,8\}$, $\{2,4,6,8\}$, $\{3,4,6,8\}$, $\{1,2,7,8\}$, $\{1,3,7,8\}$, $\{1,4,7,8\}$, $\{2,3,7,8\}$, $\{2,4,7,8\}$, $\{3,4,7,8\}$.

In the following propositions, we prove that these three "matroids" stated above are all non-representable.

Proposition 3.2. The Pseudo-1 matroid is non-representable.

Proof. For a partition $\Pi_1 = \{P_1, P_2, P_3\}$ ($P_1 = \{1,2\}, P_2 = \{3,4\}, P_3 = \{5,6,7,8\}$) of the ground set $\mathcal{Q}$, the partition Π_1 defines a mapping $\Pi_1 : \mathcal{P}(\mathcal{Q}) \to \mathbb{Z}_+^3$. For every non-basis 4-set A, we compute $\Pi_1(A)$ and obtain $(2,2,0), (2,0,2), (0,2,2)$. Similarly, for every basis B, we compute $\Pi_1(B)$ and obtain $(1,1,2), (1,2,1), (1,0,3), (0,1,3), (2,1,1), (0,0,4)$. We can verify that for every 3-set C, there must exist a basis B such that $\Pi_1(C) < \Pi_1(B)$ and $C \subset B$. Therefore, all 3-sets are independent.

Suppose that over some finite field $\mathbb{K}$ there exists a matrix M which is a representation of the Pseudo-1 matroid, and every element $i \in \mathcal{Q}$ correspond to the column vector v_i of M. Apparently, all vectors of M are non-zero vectors. Arbitrary four column vectors of M are linearly independent except (v_1, v_2, v_3, v_4), (v_1, v_2, v_5, v_6), (v_1, v_2, v_5, v_7), (v_1, v_2, v_5, v_8), (v_1, v_2, v_6, v_7), (v_1, v_2, v_6, v_8), (v_1, v_2, v_7, v_8), (v_3, v_4, v_5, v_6), (v_3, v_4, v_5, v_7), (v_3, v_4, v_5, v_8), (v_3, v_4, v_6, v_7), (v_3, v_4, v_6, v_8), (v_3, v_4, v_7, v_8). Because all

3-sets are independent, for every one of these thirteen vector groups, its rank is 3 and every vector in it can be uniquely represented by the other three vectors over $\mathbb{K}$. The following proof is the same to the proof of Proposion 3.1.

Proposition 3.3. The Pseudo-2 matroid is non-representable.

Proof. For a partition $\Pi_2 = \{P_1, P_2, P_3\}$ ($P_1 = \{1,2,3,4\}, P_2 = \{5,6\}, P_3 = \{7,8\}$) of the ground set $\mathcal{Q}$, the partition Π_2 defines a mapping $\Pi_2 : \mathcal{P}(\mathcal{Q}) \to \mathbb{Z}_+^3$. For every non-basis 4-set A, we compute $\Pi_2(A)$ and obtain $(4,0,0),(2,0,2),(2,2,0)$. Similarly, for every basis B, we compute $\Pi_2(B)$ and obtain $(2,1,1),(3,1,0),(3,0,1),(1,1,2),(1,2,1),(0,2,2)$. We can verify that for every 3-set C, there must exist a basis B such that $\Pi_2(C) < \Pi_2(B)$ and $C \subset B$. Therefore, all 3-sets are independent. The following proof is the same to the proof of Proposion 3.1.

Proposition 3.4. The Pseudo-3 matroid is non-representable.

Proof. For a partition $\Pi_3 = \{P_1, P_2\}$ ($P_1 = \{1,2,3,4\}, P_2 = \{5,6,7,8\}$) of the ground set $\mathcal{Q}$, the partition Π_3 defines a mapping $\Pi_3 : \mathcal{P}(\mathcal{Q}) \to \mathbb{Z}_+^2$. For every non-basis 4-set A, we compute $\Pi_3(A)$ and obtain $(4,0),(2,2)$. Similarly, for every basis B, we compute $\Pi_3(B)$ and obtain $(1,3),(3,1),(0,4)$. We can verify that for every 3-set C, there must exist a basis B such that $\Pi_3(C) < \Pi_3(B)$ and $C \subset B$. Therefore, all 3-sets are independent. The following proof is the same to the proof of Proposion 3.1.

If these three non-representable "matroids" accord with the definition of matroid, it means there exist non-representable bipartite and tripartite matroids. However, we will show these three non-representable "matroids" are pseudo matroids.

From Proposition 2.2, 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 $\mathbb{Z}^m$. In Pseudo-1 matroid, for $u = (2,1,1)$ and $v = (0,0,4)$ with $u_2 > v_2$, there only exists $u_3 < v_3$ but $(2,0,2)$ is not a basis. Therefore, Pseudo-1 matroid is not a matroid, namely, a pseudo matroid. Similarly, in Pseudo-2 matroid, for $u = (1,2,1)$ and $v = (3,1,0)$ with $u_3 > v_3$, there only exists $u_1 < v_1$ but $(2,2,0)$ is not a basis. Therefore, Pseudo-2 matroid is a pseudo matroid. In Pseudo-3 matroid, for $u = (3,1)$ and $v = (0,4)$ with $u_1 > v_1$, there only exists $u_2 < v_2$ but $(2,2)$ is not a basis. Therefore, Pseudo-3 matroid is a pseudo matroid. As a consequence, these three non-representable "matroids" are all pseudo matroids.

3.3 Vamos Family

For the Vamos matroid $\mathcal{M}=(\mathcal{Q},\mathcal{I})$, there exists a partition $\Pi_0=\{P_1,P_2,P_3,P_4\}$ ($P_1=\{1,2\},P_2=\{3,4\},P_3=\{5,6,\},P_4=\{7,8\}$) of the ground set $\mathcal{Q}$, and the partition Π_0 defines a mapping $\Pi_0:\mathcal{P}(\mathcal{Q})\to\mathbb{Z}_+^4$ and, hence, we obtain a discrete polymatroid $D_V=\Pi_0(\mathcal{I})$ corresponding to the Vamos matroid.

Proposition 3.5. For a discrete polymatroid D with ground set J_m, if there exists $X\subseteq J_m$, where $|X|=4$, such that $D(X)=D_V$, then D must be a non-representable discrete polymatroid, and hence, the multipartite matroid corresponding to D must be non-representable. All of these discrete polymatroids construct a family of non-representable matroids, that is, $F_{D_V}=\left\{D\subset\mathbb{Z}_+^m:\ D(X)=D_V, X\subset J_m且|X|=4\right\}$, which we call Vamos Family.

The proof of Proposition 3.5 is very simple, which is a special case of the proof of Theorem 4.1. Suppose a discrete polymatroid D in Vamos Family is representable. We will obtain the Vamos matroid is representable, contradiction. Therefore, the discrete polymatroids in Vamos Family is non-representable.

4 A Sufficient Condition for a Discrete Polymatroid to Be Non-representable

In this section, we extend the Vamos Family to the general case and obtain a sufficient condition for a discrete polymatroid to be non-representable.

Theorem 4.1. Let $D\subset\mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m, if there exists $X\subseteq J_m$ such that $D(X)=\{u(X):u\in D\}\subset\mathbb{Z}_+^{|X|}$ is a non-representable discrete polymatroid, then D must be a non-representable discrete polymatroid and, hence, the multipartite matroid corresponding to D must be non-representable.

Proof. Let $D\subset\mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m. There exists $X\subseteq J_m$ such that $D(X)=\{u(X):u\in D\}\subset\mathbb{Z}_+^{|X|}$ is a non-representable discrete polymatroid. Suppose D is representable over some finite field $\mathbb{K}$, i.e., there exists a vector space $E=\mathbb{K}^s$ over $\mathbb{K}$, where $s=h(J_m)$, such that m subspaces $V_1,\ldots,V_m$ of E are a $\mathbb{K}$-representation of D. Let $X=\{x_1,\ldots,x_r\}$, where $\left|X\right|=r$ and, hence, the subspaces corresponding to the elements of $X\subseteq J_m$ are

$V_{x_1},\dots,V_{x_r}$. Since $D(X)=\{u(X):u\in D\}\subset\mathbb{Z}_{+}^{|X|}$, it means r subspaces $V_{x_1},\dots,V_{x_r}$ of $E=\mathbb{K}^s$ are a $\mathbb{K}$-representation of $D(X)$, namely, $D(X)$ is a $\mathbb{K}$-representable discrete polymatroid, contradiction. Therefore, D is a non-representable discrete polymatroid and, hence, the multipartite matroid corresponding to D must be non-representable.

As a consequence, Theorem 4.1 gives a sufficient condition for a discrete polymatroid to be non-representable.

5 Conclusion

In this paper, by dealing with a family of matroids derived from the Vamos matroid, which was the first matroid that was proved to be non-representable, we obtain a family of non-representable matroids. As a consequence, we extend it to the general case and obtain a sufficient condition for a discrete polymatroid to be non-representable, which is a new contribution to the open problem given by Farras.

References

1. Shamir, A.: How to share a secret. Commun. of the ACM 22, 612–613 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS Conference Proceedings, vol. 48, pp. 313–317 (1979)
3. Matus, F.: Matroid representations by partitions. Discrete Math. 203, 169–194 (1999)
4. Seymour, P.D.: On secret-sharing matroids. J. Combin. Theory Ser. B 56, 69–73 (1992)
5. Marti-Farre, J., Padro, C.: On Secret Sharing Schemes, Matroids and Polymatroids. Cryptology ePrint Archive, Report 2006/077, `http://eprint.iacr.org/2006/077`
6. Tassa, T.: Hierarchical threshold secret sharing. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 473–490. Springer, Heidelberg (2004)
7. Ng, S.-L., Walker, M.: On the composition of matroids and ideal secret sharing schemes. Des. Codes Cryptogr. 24, 49–67 (2001)
8. Collins, M.J.: A Note on Ideal Tripartite Access Structures. Cryptology ePrint Archive, Report 2002/193, `http://eprint.iacr.org/2002/193`
9. Farràs, O., Martí-Farré, J., Padró, C.: Ideal multipartite secret sharing schemes. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 448–465. Springer, Heidelberg (2007)
10. Oxley, J.G.: Matroid theory. Oxford Science Publications/ The Clarendon Press/ Oxford University Press, New York (1992)
11. Welsh, D.J.A.: Matroid Theory. Academic Press, London (1976)
12. Ng, S.-L.: Ideal secret sharing schemes with multipartite access structures. IEE Proc.-Commun. 153, 165–168 (2006)
13. Herzog, J., Hibi, T.: Discrete polymatroids. J. Algebraic Combin. 16, 239–268 (2002)