Applied Mathematical Sciences, Vol. 11, 2017, no. 48, 2351 - 2365
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ams.2017.78251

On the Linear Shareability of Matroids

Arley Gómez

Departamento de Matemáticas
Universidad Nacional de Colombia
Bogotá, Colombia

Carolina Mejia

Departamento de Matemáticas
Universidad Nacional de Colombia
Bogotá, Colombia

J. Andres Montoya

Departamento de Matemáticas
Universidad Nacional de Colombia
Bogotá, Colombia

Abstract

We partially solve an important open problem in secret sharing: The characterization of the access structures admitting ideal secret sharing schemes. As our main result we prove that all the weakly linear matroids are ideal.

Mathematics Subject Classification: 68P30

Keywords: Secret Sharing, Matroids, Polymatroids, Linear Polymatroids, Linear Rank Inequalities

1 Introduction

In this work we give a partial solution to an important theoretical question coming from secret sharing: We prove that all the access structures coming from weakly linear matroids are realized by linear ideal secret sharing schemes.

Recall that matroids are combinatorial structures that are supposed to encode the abstract notion of dimension and which have found its way into Cryptography [11]. The study of the access structures coming from matroids is an old important topic in secret sharing [4]. *Ideal access structures* are the structures that admit optimal solutions to the secret sharing problem, those optimal solutions are called *ideal secret sharing schemes*. It is an important open problem to characterize the ideal structures. It is known that there exists access structures that cannot be realized by ideal schemes [3]. It is worth to remark that the known examples of non-ideal structures are obtained from special matroids as for example The Vamos Matroid [3]. Thus, it seems that matroids are a rich source of access structures. Actually, most access structures come from matroids. Then, it makes a lot of sense to consider the following question: Which are the matroids that give place to ideal access structures? We conjectured that representable matroids give place to access structures that can be realized by linear ideal secret sharing schemes. We prove that all the weakly linear matroids are ideal. To prove the later we use some elementary tools of the linear algebra of finite vector spaces.

Organization of the work, relations to previous work and contributions. This work is organized into three sections. In section 1 we review some facts of the linear algebra of finite vector spaces. In section 2 we prove that linear polymatroids and linear rank functions are the same. In section 3 we prove that weakly linear matroids can be realized by linear ideal secret sharing schemes.

Proviso. This work concerns the shareability of matroids, and it is related to all those works that are devoted to the same issue. The study of matroid-shareability began with Brikell and Davenport [4], who introduced a notion of shareability that is completely different to our notion: The access structures that Brikell-Davenport construct from a matroid M are very different to the access structure we construct with the generators of M. Brikell and Davenport construct access structures using the different ports of M (see [5]), and it happens that in those access structures the dealer belongs to the ground set of M. We, in turn, construct a single access structure from M, and it happens that in our construction the dealer does not belong to the ground set of M. We think that our construction is more natural than Brikell-Davenport construction. Most works on matroid shareability are related to the later construction,

and their results do not refer to our construction. Beimel et al [2] proved that weakly linear matroids admit linear ideal secret sharing schemes. However, it is important to remark that the aforementioned result refers the ports of M and not the access structure that is constituted by the generators of M. Thus, it cannot be said that our main result reduces to the aforementioned result.

2 The Orthogonal Complement in Finite Vector Spaces

Let us begin this section with the definition of *direct sum*

Definition 2.1 *Let $\mathcal{V}$ be a vector space, and let $\mathcal{W}$,$\mathcal{U}$ be subspaces of $\mathcal{V}$. We have that $\mathcal{V}$ is equal to $\mathcal{W} \oplus \mathcal{U}$, if and only if, the following two conditions are satisfied.*

1. For all $v \in \mathcal{V}$ there exist $w \in \mathcal{W}$ and $u \in \mathcal{U}$ such that $v = w + u$.
2. $\mathcal{W} \cap \mathcal{U} = \{0\}$, where 0 denotes the zero-vector of $\mathcal{V}$.

The *standard scalar product* is defined by

$$\langle (v_1, ..., v_n) \mid (w_1, ..., w_n) \rangle = v_1 w_1 + \cdots + v_n w_n$$

It is well known that the standard scalar product behaves well over the real field: A non-null vector is non-orthogonal to itself, since any sum of non-null real squares is different of zero. Moreover, we have that $\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^{\perp}$,where the set $\mathcal{W}^{\perp}$ is defined as

$$\mathcal{W}^{\perp} = \{v \in \mathcal{V} : (\forall w \in \mathcal{W}) \, (\langle v \mid w \rangle = 0)\} .$$

Then, it makes full sense to say that $\mathcal{W}^{\perp}$ is the (orthogonal) *complement* of $\mathcal{W}$.

Notice that the standard scalar product does not behave as well over the complex field: A non-null complex vector can be orthogonal to itself. However, it is easy to remedy the later problem by defining the complex scalar product as

$$\langle (z_1, ..., z_n) \mid ((w_1, ..., w_n)) \rangle = z_1 \overline{w_1} + \cdots + z_n \overline{w_n},$$

where the symbol $\overline{z}$ denotes complex conjugation. What about finite fields?

Let $\mathbb{F}$ be a finite field of characteristic k, and let $\mathcal{V}$ be a vector space over $\mathbb{F}$. Suppose that $\dim(\mathcal{V}) \geq 4$. Recall that k can be written as the sum of four squares. Thus, there exist $0 \leq a, b, c, d < k$, such that $k = a^2 + b^2 + c^2 + d^2$.

Set $v = (a, b, c, d, 0, ..., 0)$, and set $\mathcal{W} = \langle v \rangle$, that is: $\mathcal{W}$ is the linear span of v. We have that

$$\langle v \mid v \rangle = a^2 + b^2 + c^2 + d^2 = k = 0 \pmod{k},$$

and it implies that $v \in \mathcal{W}^{\perp}$. Thus, we have that $\mathcal{W} \cap \mathcal{W}^{\perp} \neq \{0\}$. Moreover, as we prove below, there exists $v \in \mathcal{V}$ which cannot be expressed as the sum of an element of $\mathcal{W}$ and an element of $\mathcal{W}^{\perp}$.

The above facts indicate that the notion of orthogonal complement does not work for n-dimensional finite vector spaces (provided that $n \geq 4$). However, we think that it is a so valuable notion that it is worth to rescue as much as possible of it.

Suppose that $\mathcal{V}$ is a real vector space and $\mathcal{W}$ is a subspace of $\mathcal{V}$. We have that $\mathcal{V}$ is equal to $\mathcal{W} \oplus \mathcal{W}^{\perp}$. Then, we easily get as a corollary that the equality $\dim(\mathcal{V}) = \dim(\mathcal{W}) + \dim\left(\mathcal{W}^{\perp}\right)$ holds. We notice that for some applications it suffices with the later equality. Therefore, we ask: Does the later identity hold for any finite vector space?

By an abuse of language, we will use the term *orthogonal complement of* $\mathcal{W}$ to denote the subspace $\mathcal{W}^{\perp}$. Next proposition partially justifies the use of this term.

Proposition 2.2 *Let $\mathcal{V}$ be a vector space over the finite field $\mathbb{F}$, and let $\mathcal{W}$ be a subspace of $\mathcal{V}$, we have that*

$$\dim(\mathcal{V}) = \dim\left(\mathcal{W}^{\perp}\right) + \dim(\mathcal{W}).$$

Proof. Let $w_1, ..., w_k$ be a basis of $\mathcal{W}$ and let $T : \mathcal{V} \to \mathbb{F}^k$ be the linear map defined by

$$T(v) = (\langle v, w_1 \rangle, ..., \langle v, w_k \rangle)^{\top}.$$

It is easy to check that $\ker(T) = \mathcal{W}^{\perp}$. On the other hand, we notice that $T(v)$ is given by right-multiplying v by the matrix $\begin{pmatrix} w_1 & ... & w_k \end{pmatrix}$. By definition, this matrix has column span of dimension k. The Rank Nullity Theorem, which holds true for any vector space, asserts that $\dim(\mathcal{V}) = \dim(\ker(T)) + \dim(\mathrm{Im}(T))$. Then, we have that

$$\dim(\mathcal{V}) = \dim\left(\mathcal{W}^{\perp}\right) + k = \dim\left(\mathcal{W}^{\perp}\right) + \dim(\mathcal{W}),$$

and the theorem is proved. ■

We can get the following interesting corollaries

Corollary 2.3 *For all subspace $\mathcal{W}$ the equality $\left(\mathcal{W}^{\perp}\right)^{\perp} = \mathcal{W}$ holds.*

Proof. Let $w \in \mathcal{W}$. We have that the equality $\langle w, u\rangle = 0$ holds for all $u \in \mathcal{W}^{\perp}$. Then, we get that $w \in \left(\mathcal{W}^{\perp}\right)^{\perp}$. The later fact implies that $\mathcal{W} \subseteq \left(\mathcal{W}^{\perp}\right)^{\perp}$. It follows from the above proposition that

$$\dim\left(\left(\mathcal{W}^{\perp}\right)^{\perp}\right) = \dim\left(\mathcal{V}\right) - \dim\left(\left(\mathcal{W}^{\perp}\right)\right) = \dim\left(\mathcal{W}\right).$$

Then, we have that $\mathcal{W} = \left(\mathcal{W}^{\perp}\right)^{\perp}$. ■

Corollary 2.4 *Let $w \in \mathcal{V}$ be a non-null vector such that $\langle w \mid w\rangle = 0$, and let $\mathcal{W}$ be equal to $\langle w\rangle$, there exists $v \in \mathcal{V}$ which cannot be expressed as the sum of an element of $\mathcal{W}$ and an element of $\mathcal{W}^{\perp}$.*

Proof. First we notice that $\mathcal{W} \subset \mathcal{W}^{\perp}$. It implies that the set of vectors that can be expressed as the sum of an element of $\mathcal{W}$ and an element of $\mathcal{W}^{\perp}$ is equal to $\mathcal{W}^{\perp}$. Then, it is enough to prove that $\mathcal{W}^{\perp}$ is strictly contained in $\mathcal{V}$. Set $n = \dim\left(\mathcal{V}\right)$, recall that

$$n = \dim\left(\mathcal{W}\right) + \dim\left(\mathcal{W}^{\perp}\right) = 1 + \dim\left(\mathcal{W}^{\perp}\right).$$

Then, we have that $\dim\left(\mathcal{W}^{\perp}\right) = n - 1 < \dim\left(\mathcal{V}\right)$, and the corollary is proved. ■

We study in the next sections some applications of Proposition 2.2.

3 Linear Polymatroids

The first application concerns the theory of *linear polymatroids*, a theory that has found important applications in discrete optimization (see reference [7]), secret sharing and network coding (see reference [10] and the references therein). We prove that the class of linear polymatroids is essentially the same as the class of *linear rank functions* studied in *matroid* theory (see [11] and the references therein). First, some definitions.

Notation 3.1 *We use the symbol $[n]$ to denote the set $\{1, ..., n\}$.*

Definition 3.2 (Polymatroid) *We say that a function $f : (\wp([n]) - \emptyset) \to \mathbb{R}^{+}$ is a polymatroid of order n, if and only if:*

1. *Given $I, J \in (\wp([n]) - \emptyset)$, if $I \subseteq J$ then $f(I) \leq f(J)$.*
2. *For all $I, J \in (\wp([n]) - \emptyset)$, we have that $f(I \cup J) + f(I \cap J) \leq f(I) + f(J)$.*

An important class of polymatroids is constituted by the linear polymatroids.

Definition 3.3 (Linear polymatroid) *A linear polymatroid of order n is a polymatroid $h : (\wp([n]) - \emptyset) \to \mathbb{R}^+$ for which there exists a tuple $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$, such that $\mathcal{V}$ is a finite vector space; $\mathcal{V}_1, ..., \mathcal{V}_n$ are subspaces of $\mathcal{V}$, and for all $I \in (\wp([n]) - \emptyset)$ the equality*

$$h(I) = \log\left(\left|\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right|\right),$$

holds

A better known notion is the notion of linear rank function that comes from matroid theory.

Definition 3.4 (Linear rank function) *A linear rank function of order n is a function $r : (\wp([n]) - \emptyset) \to \mathbb{R}^+$, which is determined by a tuple $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$, such that $\mathcal{V}$ is a finite vector space, $\mathcal{V}_1, ..., \mathcal{V}_n$ are subspaces of $\mathcal{V}$, and for all $I \in (\wp([n]) - \emptyset)$ the equality*

$$r(I) = \dim\left(\left\langle\bigcup_{i\in I}\mathcal{V}_i\right\rangle\right),$$

holds

We prove that those two sets of functions are essentially equal. First a technical lemma.

Lemma 3.5 *Let $\mathcal{V}$ be a finite vector space, and let $\{\mathcal{V}_i : i \in I\}$ be a family of subspaces of $\mathcal{V}$, we have that*

$$\dim\left(\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right) = \dim\left(\left\langle\bigcup_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle\right).$$

Proof. We have from definition that

$$\dim\left(\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right) = \dim(\mathcal{V}) - \dim\left(\bigcap_{i\in I}\mathcal{V}_i\right),$$

then

$$\dim\left(\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right)=\dim\left(\left(\bigcap_{i\in I}\mathcal{V}_i\right)^{\perp}\right).$$

Thus, it suffices to prove that $\left(\bigcap\limits_{i\in I}\mathcal{V}_i\right)^{\perp}$ is equal to $\left\langle\bigcup\limits_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle$. To this end, we prove that

$$\bigcap_{i\in I}\mathcal{V}_i=\left(\left\langle\bigcup_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle\right)^{\perp}$$

First, we suppose that $v\in\bigcap\limits_{i\in I}\mathcal{V}_i$. Given $w\in\left\langle\bigcup\limits_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle$, the vector w can be expressed as $\sum\limits_{i\in I}\alpha_i v_i$, where for all $i\in I$ we have that $v_i\in\mathcal{V}_i$ and α_i is a scalar. Notice that

$$\langle v\mid w\rangle=\sum_{i\in I}\alpha_i\langle v\mid v_i\rangle=0$$

Then, $v\in\left(\left\langle\bigcup\limits_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle\right)^{\perp}$ and

$$\bigcap_{i\in I}\mathcal{V}_i\subseteq\left(\left\langle\bigcup_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle\right)^{\perp}.$$

Now, we suppose that $v\in\left(\left\langle\bigcup\limits_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle\right)^{\perp}$. Given $i\in I$, and given $w\in(\mathcal{V}_i)^{\perp}$, we have that $\langle v\mid w\rangle=0$. It means that for all $i\in I$ the vector v belongs to $\left((\mathcal{V}_i)^{\perp}\right)^{\perp}$. Then, we have that $v\in\left(\bigcap\limits_{i\in I}\left((\mathcal{V}_i)^{\perp}\right)^{\perp}\right)$. Recall that

$$\left(\bigcap_{i\in I}\left((\mathcal{V}_i)^{\perp}\right)^{\perp}\right)=\bigcap_{i\in I}\mathcal{V}_i.$$

Thus, we have that

$$\left(\left\langle\bigcup_{i\in I}(\mathcal{V}_i)^{\perp}\right\rangle\right)^{\perp}\subseteq\bigcap_{i\in I}\mathcal{V}_i,$$

and the lemma is proved. ■

Now, we are ready to prove that linear rank functions and linear polymatroids are one and the same thing.

Theorem 3.6 *For all linear polymatroid h there exists a linear rank function r and there exists $c > 0$ such that $h = c \cdot r$. On the other hand, for all linear rank function r there exist a linear polymatroid h and a constant $d > 0$ such that $r = d \cdot h$.*

Proof. Let h be a linear polymatroid determined by a tuple $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$, where $\mathcal{V}$ is a finite vector space over the finite field $\mathbb{F}$. Let I be non-empty subset of $[n]$, we have that

$$\begin{aligned} h(I) &= \log\left(\left|\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right|\right) = \frac{1}{\log_{|\mathbb{F}|}(2)}\log_{|\mathbb{F}|}\left(\left|\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right|\right) \\ &= \frac{1}{\log_{|\mathbb{F}|}(2)}\dim\left(\frac{\mathcal{V}}{\bigcap\limits_{i\in I}\mathcal{V}_i}\right) = \frac{1}{\log_{|\mathbb{F}|}(2)}\dim\left(\left\langle\bigcup_{i\in I}\mathcal{V}_i^{\perp}\right\rangle\right). \end{aligned}$$

Let $c = \frac{1}{\log_{|\mathbb{F}|}(2)}$, let $R = \left(\mathcal{V}, \mathcal{V}_1^{\perp}, ..., \mathcal{V}_n^{\perp}\right)$ and let r be equal to the linear rank function determined by the tuple R. We have that $h = c \cdot r$. The proof of the other claim is similar. ■

We study in next section an application of Theorem 3.6, the application is related to secret sharing.

4 Linear Secret Sharing

Secret sharing is an important cryptographic primitive that plays a key role in secure multiparty computation [6]. Let us introduce some of the main definitions related to linear secret sharing.

Definition 4.1 (Access structure) *An access structure is a pair $(n, \mathcal{C})$, such that $\mathcal{C}$ is a non-empty family of subsets of $[n]$ that is upward closed (closed for supersets).*

Let $(n, \mathcal{C})$ be an access structure, it determines a notion of largeness: Given $A \subset [n]$, we have that A is large, if and only if, the set A belongs to $\mathcal{C}$.

One can use the later notion of largeness to define *The Secret Sharing Problem*:

To break a secret into n pieces (shares), in such a way that the secret can be reconstructed from any large set of pieces, but such that no information about it can be drawn from the small sets.

The reader can imagine the following situation. There are n parties, an access structure $(n, \mathcal{C})$ has been fixed, and someone wants to privately communicate a share of a secret to each one of the n parties. Moreover, the shares

must be chosen in such a way that given $I \in \mathcal{C}$ the secret can be perfectly reconstructed from the shares that were communicated to the parties in I. We also suppose that there is an eavesdropper who wants to know the secret. If the eavesdropper has the possibility of infiltrating the small sets of parties (the unqualified sets that do not belong to the access structure $(n, \mathcal{C})$), then the shares must be chosen in such a way that given $J \notin \mathcal{C}$, no information about the secret can be obtained from the shares that were communicated to the parties in J.

A solution to the above problem is a *perfect secret sharing scheme for* $(n, \mathcal{C})$. We are interested in *linear secret sharing schemes,* which are the perfect distribution schemes that can be realized by linear functions.

Definition 4.2 (Linear secret sharing scheme) *Let $(n, \mathcal{C})$ be an access structure and let h be a linear polymatroid of order $n+1$, we say that h is a linear secret sharing scheme for $(n, \mathcal{C})$ (h realizes $(n, \mathcal{C})$), if and only if, the following conditions are satisfied:*

1. Correctness*: $h(I \cup \{n+1\}) - h(I) = 0$, for all $I \in \mathcal{C}$.*
2. Privacy*: $h(J \cup \{n+1\}) - h(J) = h(\{n+1\})$, for all $J \notin \mathcal{C}$.*

Any linear secret sharing scheme for $(n, \mathcal{C})$ encodes a perfect secret sharing scheme for the same access structure. Let h be linear secret sharing scheme for $(n, \mathcal{C})$, and let $(\mathcal{V}, \mathcal{V}_1, .., \mathcal{V}_{n+1})$ be a vector space representation of h, we can use this representation to construct a perfect secret sharing scheme:

We suppose that the secret is a vector s that belongs to $\frac{\mathcal{V}}{\mathcal{V}_{n+1}}$, the perfect secret sharing scheme works as follows:

1. The secret dealer randomly chooses $w \in \mathcal{V}_{n+1}$.
2. Given $i \in [n]$, the share assigned to party i is equal to $\pi_i(s + w)$, where π_i is the projection of $\mathcal{V}$ onto the quotient $\frac{\mathcal{V}}{\mathcal{V}_i}$.

It is easy to check that the above distribution scheme meets the conditions imposed in the definition of perfect secret sharing schemes (which can be formalized using the notion of Shannon entropy, see [10]). Notice also that the functions that are used to compute the shares are linear projections.

Ito et al [8] proved that for any access structure there exists a linear secret sharing scheme realizing it. Unfortunately, the schemes that can be obtained form Ito's construction exhibit an unpleasant feature: The size of the shares is exponential with respect to the size of the secret. Given a secret sharing scheme, the ratio between the size of the shares and the size of the secret is a measure of the efficiency and applicability of the scheme. If the ratio is large, computing and communication times could become prohibitive. Moreover, if

the ratio is large and the shares are huge, the security provided by the scheme can be corrupted for practical reasons: It could happens that the parties do not have enough internal memory to store such a huge shares, and then, they can become forced to store those shares in an unsafe external memory (as the cloud) that could be infiltrated by the eavesdropper.

Definition 4.3 (Linear information ratio) *Given an access structure $(n, \mathcal{C})$ and given a linear secret sharing scheme h, the linear information ratio of h is equal to $\frac{h([n])}{h(\{n+1\})}$, and it is denoted by $\sigma^*(h)$.*

It is important to remark that the linear information ratio of h is usually defined as

$$\rho(h) = \frac{\max_{i \leq n}(h(\{i\}))}{h(\{n+1\})}.$$

We have preferred to introduce our definition of $\sigma^*(h)$, which is very similar to the standard one, and which has some important advantages: Our definition does not use the operator max. Next lemma ensures that our notion and the classical one are closely related. The proof of the lemma is straightforward and we omit it.

Lemma 4.4 *Let $n \geq 1$, and let h be a linear secret sharing scheme for n parties, it happens that $\rho(h) \leq \sigma^*(h) \leq n \cdot \rho(h)$.*

Definition 4.5 (Optimal linear information ratio) *Given an access structure $(n, \mathcal{C})$, the optimal linear information ratio $\sigma(\mathcal{C})$ is defined by*

$$\sigma(\mathcal{C}) = \inf\{\sigma^*(h) : h \text{ is a linear secret sharing scheme for } (n, \mathcal{C})\}.$$

Let $(n, \mathcal{C})$ be an access structure, and let $\alpha_{\mathcal{C}}$ be equal to $\min\{|I| : I \in \mathcal{C}\}$. It is known that the optimal linear information ratio of $(n, \mathcal{C})$ cannot be smaller than $\alpha_{\mathcal{C}}$ (see [10]). If the equality $\sigma(\mathcal{C}) = \alpha_{\mathcal{C}}$ holds, we say that $(n, \mathcal{C})$ is an *ideal access structure*. Observe that ideal access structures are those structures for which the secret sharing problem can be optimally solved by means of linear functions. The question about the characterization of the ideal access structures is an important open problem in linear secret sharing. We wont solve the later problem, but we will present some results related to it. It is important to remark that all those results are obtained thanks to the notion of orthogonal complement in finite vector spaces and one of its corollaries: The connection between linear polymatroids and linear rank functions established in the previous section.

4.1 Ideal access structures and matroids.

Matroids are combinatorial structures encoding the abstract notion of dimension. Those structures have found their way into cryptography (see for example [4]).

Definition 4.6 (Matroid) *Given $n \geq 1$, a matroid of order n is a set $M \subseteq \wp([n])$ such that:*

1. $\emptyset \in M$.
2. *Given $A \subseteq B \subseteq [n]$, if $B \in M$, then $A \in M$.*
3. *Given $A, B \in M$, if $|A| < |B|$ there exists $b \in B$ such that $A \cup \{b\} \in M$.*

The dimension encoded by a matroid M is given by its *rank function*, which is defined as follows

Definition 4.7 (Rank function) *Let M be a matroid of order n and let $I \subseteq [n]$, the rank function of M is the function $rk_M : \wp([n]) \to \mathbb{N}$ given by*

$$rk_M(I) = \max\{|J| : J \in M \text{ and } J \subseteq I\}.$$

A matroid of order n determines an access structure (n, S_M), where S_M is equal to

$$\{J \subseteq [n] : rk_M(J) = rk_M([n])\}.$$

We say that matroid M is an *ideal matroid*, if and only if, (n, S_M) is an ideal access structure.

Remark 4.8 *From now on, we will denote the access structure (n, S_M) with the symbol M.*

It happens that most access structures come from matroids. It is easy to check that given a *threshold access structure* $(n, \mathcal{C})$ there exists a matroid of order n, say M, such that $(n, \mathcal{C})$ is equal to M. The same is true of most of the different types of access structures that have been considered in the literature. The later facts suggest that it is a good idea to focus on the following question: Which are the ideal matroids? Observe that the notion of ideal matroid corresponds to a new notion of representability for matroids. Then, to begin with, it could be a good idea to investigate the relations of this new notion with some classical notions of representability.

Definition 4.9 *A matroid M is a linear matroid, if and only if, there exists a vector space arrangement $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$ such that for all $i \leq n$ the equality $\dim(\mathcal{V}_i) = 1$ holds, and such that rk_M is equal to the linear rank function determined by $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$. We say, in the later case, that $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$ is a linear representation of M.*

We prove, as a warm up for our main result (Theorem 4.12), that any linear matroid is ideal.

Theorem 4.10 *Linear matroids are ideal.*

Proof. Let M be a linear matroid of order n, and let $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$ be a linear representation of M. We want to prove that M is ideal, it means that we have to construct a linear polymatroid of order $n+1$ satisfying the correctness and privacy constraints imposed by S_M. We use the connection between linear polymatroids and linear rank functions. Therefore, we focus on constructing a subspace $\mathcal{V}_{n+1} \subset \mathcal{V}$ that satisfies the following constraints:

1. $\dim\left(\left\langle\left(\bigcup_{i\in I}\mathcal{V}_i\right)\cup\mathcal{V}_{n+1}\right\rangle\right) = \dim\left(\left\langle\bigcup_{i\in I}\mathcal{V}_i\right\rangle\right)$, for all $I \in S_M$.
2. $\dim\left(\left\langle\left(\bigcup_{i\in J}\mathcal{V}_i\right)\cup\mathcal{V}_{n+1}\right\rangle\right) = \dim\left(\left\langle\bigcup_{i\in J}\mathcal{V}_i\right\rangle\right) + 1$, for all $J \notin S_M$.

We can suppose (without loss of generality) that $\mathcal{V} = \left\langle\bigcup_{i\in[n]}\mathcal{V}_i\right\rangle$. Let $\dim(\mathcal{V}) = m$, if $I \notin S_M$ we get that $\dim\left(\left\langle\bigcup_{i\in I}\mathcal{V}_i\right\rangle\right) \leq m-1$, and hence $\left|\left\langle\bigcup_{i\in I}\mathcal{V}_i\right\rangle\right| \leq |\mathbb{F}|^{m-1}$, where $\mathbb{F}$ is the ground field of $\mathcal{V}$. Then,we have that

$$\left|\bigcup_{I\notin S_M}\left(\left\langle\bigcup_{i\in I}V_i^{\perp}\right\rangle\right)\right| \leq 2^n\cdot|\mathbb{F}|^{m-1}.$$

We can suppose that the size of $\mathbb{F}$ is larger than 2^n, and then we get that

$$\left|\bigcup_{I\notin S_M}\left(\left\langle\bigcup_{i\in I}V_i^{\perp}\right\rangle\right)\right| < |\mathbb{F}|^m = |\mathcal{V}|.$$

Thus, if we suppose $|\mathbb{F}| > 2^n$, we ensure the existence of a vector $v \in \mathcal{V}$ such that $v \notin \bigcup_{I\notin S_M}\left(\left\langle\bigcup_{i\in I}V_i^{\perp}\right\rangle\right)$. We set $\mathcal{V}_{n+1} = \langle v\rangle$, it is easy to check that the above two constraints are satisfied. Then, if we set

$$\mathcal{V}^+ = \left(\mathcal{V}, \mathcal{V}_1^{\perp}, ..., \mathcal{V}_n^{\perp}, \mathcal{V}_{n+1}^{\perp}\right),$$

we get that the linear polymatroid determined by $\mathcal{V}^+$, which we denote with the symbol $h_{\mathcal{V}^+}$, is a linear secret sharing scheme for M. Moreover, we have that

$$\frac{h_{\mathcal{V}^+}([n])}{h_{\mathcal{V}^+}(\{n+1\})} = \dim(\mathcal{V}) = \alpha_M = rk_M([n]).$$

Then, we can conclude that M is ideal. ■

Now, we prove the main result of this section, we prove that the any *weakly linear matroid* is ideal.

Definition 4.11 *A matroid M is a weakly linear matroid, if and only if, there exists a vector space arrangement $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$ such that for all $i \leq n$ the equality $\dim(\mathcal{V}_i) = \dim(\mathcal{V}_1)$ holds, and such that $\dim(\mathcal{V}_1) \cdot rk_M$ is equal to the linear rank function determined by $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$. We say, in the later case, that $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$ is a weakly linear representation of M.*

Notice that any linear matroid is weakly linear. On the other hand, it is known that there exist weakly linear matroids that are not linear, an important example is the non-Pappus matroid (see [1]).

Theorem 4.12 *Let M be a weakly linear matroid, we have that M is ideal.*

Proof. We use, once again, the connection between linear polymatroids and linear rank functions.

Suppose that rk_M is weakly linear, there exists a subspace arrangement $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_n)$ with ground field $\mathbb{F}$ and such that:

1. For all $I \subseteq [n]$, the equality $rk_M(I) = \frac{\dim\left(\left\langle \bigcup_{i \in I} \mathcal{V}_i \right\rangle\right)}{\dim(\mathcal{V}_1)}$ holds.
2. $\mathcal{V} = \left\langle \bigcup_{i \leq n} \mathcal{V}_i \right\rangle$.

Recall that we are trying to construct an ideal linear secret sharing scheme for M, to this end we have to construct a subspace $\mathcal{V}_{n+1} \subset \mathcal{V}$ such that:

1. $\dim(\mathcal{V}_{n+1}) = \dim(\mathcal{V}_1)$.
2. $\dim\left(\left(\left\langle \bigcup_{i \in I} \mathcal{V}_i \right\rangle\right) \cup \mathcal{V}_{n+1}\right) = \dim\left(\left\langle \bigcup_{i \in I} \mathcal{V}_i \right\rangle\right)$, for all $I \in S_M$.
3. $\dim\left(\left(\left\langle \bigcup_{i \in J} \mathcal{V}_i \right\rangle\right) \cup \mathcal{V}_{n+1}\right) = \dim\left(\left\langle \bigcup_{i \in J} \mathcal{V}_i \right\rangle\right) + \dim(\mathcal{V}_{n+1})$, for all $J \notin S_M$.

Let $PB(M)$ be the set

$$\{I \subset [n] : rk_M(I) = rk_M([n]) - 1\},$$

and let $\mathcal{W}$ be equal to $\bigcup_{I \in PB(M)} \left\langle \bigcup_{i \in I} \mathcal{V}_i \right\rangle$. If we set $K_M = |PB(M)|$ (notice that $K_M \leq 2^n$), we get that $\mathcal{W}$ is equal to the union of K_M subspaces of $\mathcal{V}$ each of dimension $\dim(\mathcal{V}_1) \cdot (m-1)$, where m is equal to $rk_M([n])$.

We say that a family $\{W_j\}_{j \in J}$ of subspaces of V is a *non-intersecting family*, if and only if, for all $s, l \in J$, *if* $s \neq l$ then $W_s \cap W_l = \{0\}$. Set $d = \dim(\mathcal{V}_1)$, it can be proved (see [5]) that there exists a non-intersecting family of d-dimensional subspaces of $\mathcal{V}$ whose size is equal to $\frac{|\mathbb{F}|^{d \cdot m} - 1}{|\mathbb{F}|^d - 1}$. Let $\{W_j\}_{j \in J}$ be such a family and suppose that for all $j \in J$, it happens that $\mathcal{W} \cap W_j \neq \{0\}$. Then we have that

$$\begin{aligned} K_M\left(|\mathbb{F}|^{d \cdot (m-1)}\right) &\geq |\mathcal{W}| \\ &\geq \left(\frac{|\mathbb{F}|^{d \cdot m} - 1}{|\mathbb{F}|^d - 1}\right)(|\mathbb{F}| - 1) \end{aligned}$$

We can suppose that the size of $\mathbb{F}$ is as large as we want, and then if we suppose that $|\mathbb{F}|$ is very much larger than 2^n we get that the inequality

$$K_M\left(|\mathbb{F}|^{d \cdot (m-1)}\right) \geq \left(\frac{|\mathbb{F}|^{d \cdot m} - 1}{|\mathbb{F}|^d - 1}\right)(|\mathbb{F}| - 1)$$

cannot be satisfied. The later fact means that if $|\mathbb{F}|$ is large, there must exist a subspace $\mathcal{U} \subset \mathcal{V}$, such $\dim(\mathcal{U}) = d$ and $\mathcal{U} \cap \mathcal{W} = \{0\}$.

Thus, we suppose $|\mathbb{F}|$ large and we pick $\mathcal{U}$ as above. If we set $\mathcal{V}_{n+1} = \mathcal{U}$, we get a vector space arrangement, the arrangement $(\mathcal{V}, \mathcal{V}_1, ..., \mathcal{V}_{n+1})$, that satisfies the three conditions we wanted to fulfill with our construction. If we set

$$\mathcal{V}^+ = \left(\mathcal{V}, \mathcal{V}_1^\perp, ..., \mathcal{V}_n^\perp, \mathcal{V}_{n+1}^\perp\right),$$

we get that the linear polymatroid determined by $\mathcal{V}^+$, which we denote with the symbol $h_{\mathcal{V}^+}$, is a linear secret sharing scheme for M. Moreover, we have that

$$\frac{h_{\mathcal{V}^+}([n])}{h_{\mathcal{V}^+}(\{n+1\})} = \frac{\dim(\mathcal{V})}{\dim(\mathcal{V}_1)} = \alpha_M = rk_M([n]).$$

Then, we can conclude that M is ideal and the theorem is proved. ■

References

[1] A. Ashikhmin, J. Simonis, Almost Affine Codes, *Designs, Codes and Cryptography*, **14** (1998), no. 2, 179-197.
https://doi.org/10.1023/a:1008244215660

[2] A. Beimel, A. Ben-Efraim, C. Padró, I. Tyomkin, Multi-linear Secret-Sharing Schemes, Chapter in *TCC 2014: Theory of Cryptography*, 2014, 394-418. https://doi.org/10.1007/978-3-642-54242-8_17

[3] A. Beimel, N. Livne, C. Padró, Matroids Can Be Far from Ideal Secret Sharing, Chapter in *TCC 2008: Theory of Cryptography*, 2008, 194-212. https://doi.org/10.1007/978-3-540-78524-8_12

[4] E. Brickell, D. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptol.*, **4** (1991), 123-134. https://doi.org/10.1007/bf00196772

[5] A. Calderbank, S. Diggavi, F. Oggier, N. Sloane, Nonintersecting subspaces based on finite alphabets, *IEEE Transactions on Information Theory*, **51** (2005), no. 12, 4320-4325. https://doi.org/10.1109/tit.2005.858946

[6] R. Cramer, I. Damgård, J. Nielsen, *Secure Multiparty Computation and Secret Sharing*, Cambridge University Press, N.Y., 2015. https://doi.org/10.1017/cbo9781107337756

[7] S. Fujishige, *Submodular Functions and Optimization,* Elsevier, Amsterdam, 2005.

[8] M. Ito, A. Saito and T. Nishizeki, Secret Sharing Scheme Realizing General Access Structure, *Proceedings of Globecom*, (1987), 99-102.

[9] A. M. Legendre, *Essai Sur la Théorie Des Nombres*, Paris, An VI (1797-1798), 202 and 398-399.

[10] C. Mejia, *On the Theory of Linear Rank Functions*, Ph.D Thesis, Universidad Nacional de Colombia, Bogota, 2016.

[11] J. Oxley, *Matroid Theory*, Oxford University Press, Oxford U.K., 1992.

Received: August 23, 2017; Published: September 17, 2017