On Secret Sharing Schemes, Matroids and Polymatroids

Jaume Martí-Farré and Carles Padró

Dept. of Applied Maths. IV, Technical University of Catalonia, Barcelona. *
{jaumem, matcpl}@ma4.upc.edu

Abstract. One of the main open problems in secret sharing is the characterization of the access structures of ideal secret sharing schemes. As a consequence of the results by Brickell and Davenport, every one of those access structures is related in a certain way to a unique matroid.
Matroid ports are combinatorial objects that are almost equivalent to matroid-related access structures. They were introduced in 1964 by Lehman and a forbidden minor characterization was given by Seymour in 1976. These and other subsequent works on that topic have not been noticed until now by the researchers interested on secret sharing.
By combining those results with some techniques in secret sharing, we obtain new characterizations of matroid-related access structures. As a consequence, we generalize the result by Brickell and Davenport by proving that, if the information rate of a secret sharing scheme is greater than 2/3, then its access structure is matroid-related. This generalizes several results that were obtained for particular families of access structures.
In addition, we study the use of polymatroids for obtaining upper bounds on the optimal information rate of access structures. We prove that all the bounds that are obtained by this technique for an access structure apply also to the dual structure.
Finally, we present lower bounds on the optimal information rate of the access structures that are related to two matroids that are not secret sharing representable: the Vamos matroid and the non-Desargues matroid.
Key words. Secret sharing, Ideal secret sharing schemes, Ideal access structures, Secret sharing representable matroids, Information rate.

1 Introduction

1.1 The Problems

A *secret sharing scheme* is a method to distribute a *secret value* into *shares* in such a way that only some *qualified subsets* of *participants* are able to recover the secret from their shares. Secret sharing schemes were independently introduced by Shamir [31] and Blakley [5]. Only *unconditionally secure perfect secret sharing schemes* will be considered in this paper. That is, the shares of the participants in a non-qualified subset must not contain any information about the secret value.

The family of the qualified subsets is the *access structure* of the scheme, which is supposed to be *monotone increasing*: every subset containing a qualified subset must be qualified. Then, an access structure is determined by its *minimal qualified subsets*.

The complexity of a secret sharing scheme can be measured by the length of the shares. In all secret sharing schemes, the length of every share is greater than or equal to the length

* This work was partially supported by the Spanish Ministry of Education and Science under project TIC 2003-00866. This work was done while the second author was in a sabbatical stay at CWI, Amsterdam. This stay was funded by the *Secretaría de Estado de Educación y Universidades* of the Spanish Ministry of Education.

of the secret [19]. A secret sharing scheme is said to be *ideal* if all shares have the same length as the secret.

The qualified subsets of a *threshold access structure* are those having at least a fixed number of participants. Shamir's construction [31] provides an ideal scheme for every threshold access structure. Even though there exists a secret sharing scheme for every access structure [17], in general some shares must be larger than the secret [12, 13].

This paper deals with the optimization of the complexity of secret sharing schemes for general access structures.

The characterization of the *ideal access structures*, that is, the access structures of ideal secret sharing schemes, is one of the main open problems in that direction. Brickell and Davenport [10] discovered important connections of this problem with Matroid Theory. Specifically, they proved that every ideal secret sharing scheme on a set of participants P defines a unique matroid $\mathcal{M}$ on the set $Q = P \cup \{D\}$, where $D \notin P$ is a special participant, usually called *dealer*. The access structure of the scheme is determined by the matroid $\mathcal{M}$. Actually, for every $A \subset P$, the set $A \cup \{D\}$ is a circuit of the matroid if and only if A is a minimal qualified subset. Therefore, if Γ is an ideal access structure, there must exist a matroid $\mathcal{M}$ with that property. In this case, we say that the access structure is *matroid-related*.

The matroids that are obtained in this way from ideal secret sharing schemes are generally called *secret sharing matroids*, but we prefer to call them *secret sharing representable matroids* or *ss-representable matroids*. This is due to the fact that the ideal secret sharing scheme can be seen as a representation of its associated matroid. Actually, this is a generalization of the linear representation of matroids, because the *vector space secret sharing schemes* introduced by Brickell [9] correspond exactly to the linear representations and, hence, their associated matroids are precisely the representable ones. The access structures that are related to representable matroids are called *vector space access structures*. Secret sharing representable matroids have been studied under different points of view by Simonis and Ashikhmin [32] and by Matúš [25], and are known under different names: *almost affinely representable matroids* in [32] and *partition representable matroids* in [25].

The results by Brickell and Davenport [10] reduce the open problem of characterizing the access structures of ideal secret sharing schemes to the following two open problems.

Problem 1. To characterize the matroid-related access structures.

Problem 2. To characterize the secret sharing representable matroids.

A more general open problem is to determine the complexity of the best secret sharing scheme for any given access structure. For instance, we can try to maximize the *information rate* or the *average information rate*, which are the ratios between the length in bits of the secret and, respectively, the maximum or the average length of the shares.

The *optimal information rate* of an access structure Γ, which is denoted by $\rho(\Gamma)$, is defined as the supremum of the information rates of all secret sharing schemes with access structure Γ. Clearly, $0 < \rho(\Gamma) \leq 1$. The *optimal average information rate* $\tilde{\rho}(\Gamma)$ is defined analogously. In this paper we consider only the first parameter.

Problem 3. To determine the value of $\rho(\Gamma)$ or, at least, to improve the known bounds on this function.

The concepts of *duality* that have been defined for matroids, for access structures and for linear codes are closely related and play an important role in the study of these problems. For instance, the dual of a matroid-related access structure is related to the dual matroid, and the dual of a linear secret sharing scheme for Γ (linear schemes can be seen as linear codes) is a scheme for the dual access structure.

1.2 Related Work

As a sequel of the results by Brickell and Davenport [10], there is a number of works dealing with Problem 2. The Vamos matroid was the first matroid that was proved to be non-ss-representable. This was done by Seymour [30] and a shorter proof was given later by Simonis and Ashikhmin [32]. All representable matroids are ss-representable. The first example of a ss-representable matroid that is not representable, the non-Pappus matroid, was presented in [32]. This matroid can be represented by an ideal *linear* secret sharing scheme. The matroids with this property are said to be *multilinearly representable*, a class that includes the representable matroids. The existence of ss-representable matroids that are not multilinearly representable is an open question. The dual of a multilinearly representable matroid is also multilinearly representable, but it is not known whether the dual of a ss-representable matroid is equally ss-representable. Some arguments towards a negative answer to this question were given in [25].

A number of important results and interesting ideas for future research on Problem 2 can be found in the works by Simonis and Ashikhmin [32] and Matúš [25]. The first one deals with the geometric structure that lies behind ss-representations of matroids. The second one analyzes the algebraic properties that the matroid induces in all its ss-representations. These properties make it possible to find some restrictions on the ss-representations of a given matroid and, in some cases, to exclude the existence of such representations. By using these tools, Matúš [25] presented an infinite family of non-ss-representable matroids with rank three.

One of the most important results on the optimization of the complexity of secret sharing schemes for general access structures is the fact that nonlinear secret sharing schemes are in general more efficient than the linear ones. By using the results and techniques in [1, 16], Beimel and Weinreb [4] presented families of access structures for which there exist nonlinear secret sharing schemes whose complexity is polynomial on the number of participants while the complexity of the best linear schemes is not polynomial.

Lower bounds on the optimal information rate of wide families of access structures can be found by applying the different techniques to construct secret sharing schemes with high information rate given in [8, 11, 28, 34, 35]. Upper bounds on this parameter have been found by using Information Theory [6, 7, 12]. Csirmaz [13] proved that every secret sharing scheme defines a polymatroid that is related to the access structure and he observed that those upper bounds on the optimal information rate could be derived from this fact. A general combinatorial method to find upper bounds, the *independent sequence method*, was given in [6] and was improved in [27]. However, there exists a wide gap between the best known upper and lower bounds on the optimal information rate for most access structures.

Due to the difficulty of finding general results on the three open problems we are considering, they have been studied in several particular classes of access structures: the access structures on sets of four [33] and five [18] participants, the access structures defined by

graphs [6–8, 10–12, 35], the bipartite access structures [27], the access structures with three or four minimal qualified subsets [23], the access structures with intersection number equal to one [24], the sparse homogeneous access structures with rank three [22], and the weighted threshold access structures [3]. There exist remarkable coincidences in the results obtained for all these classes of access structures. Namely, in every one of those 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 and, more precisely, with the vector space ones. Another interesting result has been proved for all those families except the weighted threshold access structures, for which it has not been disproved. Namely, the optimal information rate of all non-matroid-related access structures in those families is at most $2/3$ and, hence, there is no access structure Γ in those families whose optimal information rate is such that $2/3 < \rho(\Gamma) < 1$. A natural question that arises at this point is to determine to which extent these results can be generalized to other families of access structures.

The only known results on the optimal information rate of non-ideal matroid-related access structures have been presented in a recent work by Beimel and Livne [2]. They have given lower bounds on the length of the shares in secret sharing schemes for the access structures related to the Vamos matroid.

We have surveyed here the main results on the considered problems by the authors interested on secret sharing. Surprisingly enough, almost all these authors, including the ones of this paper, have been unaware that matroid-related access structures were studied before secret sharing was invented. Of course, a different name was used: *matroid ports*. We said *almost* because some of the main results on matroid ports were obtained in 1976 by Seymour [29], who later worked on secret sharing and, as we said before, proved that the Vamos matroid is not ss-representable [30].

Because of their important implications to the problems we are considering here, one of the main goals of this paper is to point out those old results on matroid ports to Cryptology researchers, specially to those interested on secret sharing.

A matroid port is exactly the family of minimal qualified subsets of a matroid-related access structure. Matroid ports were introduced by Lehman [20] in 1964 to solve a problem in Game Theory: the Shannon switching game. Seymour [29] presented a characterization of matroid ports by excluded minors that is based on a previous characterization of matroid ports by Lehman [21]. As a consequence, an answer to Problem 1 is obtained. Namely, matroid-related access structures are exactly those avoiding certain structures as minors. This characterization will be very useful to obtain new general results on the considered problems and to solve them for other particular families of access structures.

1.3 Our Results

Our main result consists of several new characterizations of matroid-related access structures that are obtained by combining the results by Seymour [29] with the fact that the Shannon entropy defines a polymatroid over a set of random variables [14, 15] and the combinatorial techniques to obtain upper bounds on the optimal information rate that were introduced in [6, 13, 27]. This is done in Section 4.

As a consequence, we generalize the result by Brickell and Davenport [10] by proving that, if the information rate of a secret sharing scheme is greater than $2/3$, then its access

structure is matroid-related. Let us recall that they proved that the access structure of every ideal secret sharing scheme is matroid-related. The proof of our result, as well as the ones for the results we apply in it, do not rely on the result by Brickell and Davenport [10]. In addition, except for the relation between entropy and polymatroids, those proofs use only combinatorial techniques. Therefore, we can say that we present here a new, almost purely combinatorial proof for that important result. Moreover, our result provides an explanation for a phenomenon that have been observed in several families of access structures: the gap between 2/3 and 1 in the values of the optimal information rate.

In addition, we present in Section 3 a new result about the use of polymatroids to obtain upper bounds on the information rate, a technique that was introduced by Csirmaz [13]. Specifically, we prove that every bound on the optimal information rate of a given access structure that can be obtained by using polymatroids applies also to the dual access structure. In order to do that, we define in a suitable way the *dual* of a polymatroid.

Finally, Section 5 is devoted to present lower bounds on the optimal information rate of the access structures related to the Vamos matroid and the non-Desargues matroid. Since these matroids are not ss-representable, the related access structures are not ideal. We prove that the optimal information rate of the access structures related to the Vamos matroid is at least 2/3, while this parameter is at least 3/4 for the structures related to the non-Desargues matroid.

2 Basics on Secret Sharing, Matroids and Polymatroids

The reader is referred to [33] for an introduction to secret sharing and to [26, 37] for general references on Matroid Theory. The book by Welsh [37] contains a chapter about polymatroids.

Let Q be a finite set of *participants* and $D \in Q$ a special participant called *dealer*. Let us consider a finite set E with a probability distribution on it. For every $i \in Q$, let us consider a finite set E_i and a surjective mapping $\pi_i \colon E \to E_i$. Those mappings induce random variables on the sets E_i. We notate $H(E_i)$ for the Shannon entropy of those random variables. For a subset $A = \{i_1, \ldots, i_r\} \subset Q$, we write $H(A)$ for the joint entropy $H(E_{i_1} \ldots E_{i_r})$, and a similar convention is used for conditional entropies: for instance, $H(E_j|A) = H(E_j|E_{i_1} \ldots E_{i_r})$.

The mappings π_i define a *secret sharing scheme* Σ with *access structure* Γ on the set of participants $P = Q - \{D\}$ if $H(E_D) > 0$ and $H(E_D|A) = 0$ if $A \in \Gamma$ while $H(E_D|A) = H(E_D)$ if $A \notin \Gamma$. In that situation, every random choice of an element $\mathbf{x} \in E$, according to the given probability distribution, results in a *distribution of shares* $((s_i)_{i \in P}, s)$, where $s_i = \pi_i(\mathbf{x}) \in E_i$ is the *share* of the participant $i \in P$ and $s = \pi_D(\mathbf{x}) \in E_D$ is the *shared secret value*.

From now on, we are going to suppose that every participant in P is at least in a minimal qualified subset, that is, the access structure is *connected*.

The ratio $\rho(\Sigma) = H(E_D)/(\max_{i \in P} H(E_i))$ is called the *information rate* of the scheme Σ, and the *optimal information rate* $\rho(\Gamma)$ of the access structure Γ is the supremum of the information rates of all secret sharing schemes with access structure Γ. It is not difficult to check that $H(E_i) \geq H(E_D)$ for every $i \in P$ and, hence, $\rho(\Sigma) \leq 1$. Secret sharing schemes with $\rho(\Sigma) = 1$ are said to be *ideal* and their access structures are called *ideal* as well. Of course, $\rho(\Gamma) = 1$ for every ideal access structure Γ.

If the sets E and E_i are vector spaces over some finite field $\mathbb{K}$, the uniform probability distribution is considered in E, and the mappings π_i are linear mappings, we say that Σ is a $\mathbb{K}$*-linear secret sharing scheme*. The linear schemes in which $E_i = \mathbb{K}$ for every $i \in Q$ are ideal and they are called $\mathbb{K}$*-vector space secret sharing scheme*. Their access structures are called $\mathbb{K}$*-vector space access structures*.

We notate $\mathcal{P}(Q)$ for the power set of Q. Given a secret sharing scheme Σ, let us consider the mapping $h\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(X) = H(X)/H(E_D)$. This mapping verifies the following properties [13]:

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

A *polymatroid* is any pair $\mathcal{S} = (Q, h)$ verifying those properties. Therefore, every secret sharing scheme Σ defines a polymatroid $\mathcal{S} = \mathcal{S}(\Sigma) = (Q, h)$ that has an additional property. Namely, $h(\{D\}) = 1$ and, for every subset $X \subset Q$, either $h(X \cup \{D\}) = h(X) + 1$ or $h(X \cup \{D\}) = h(X)$. Polymatroids with this additional property will be called here *D-secret sharing polymatroids* or *D-ss-polymatroids*.

Observe that $A \in \Gamma$ if and only if $h(A \cup \{D\}) = h(A)$. Therefore, the access structure of the scheme Σ is determined by the polymatroid $\mathcal{S}(\Sigma)$. In this situation, we say that the access structure Γ is related to the D-ss-polymatroid $\mathcal{S}$ and we write $\Gamma = \Gamma_D(\mathcal{S})$. Since there exists a secret sharing scheme for every access structure Γ, all access structures are related to some D-ss-polymatroid. Different D-ss-polymatroids can define the same access structure.

A *matroid* can be defined as a polymatroid $\mathcal{M} = (Q, r)$ with the additional property:

4. $r(X) \in \mathbb{Z}$ and $0 \leq r(X) \leq |X|$ for every $X \subset Q$, or, equivalently, for every $X \subset Q$ and $x \in Q$, either $r(X \cup \{x\}) = r(X) + 1$ or $r(X \cup \{x\}) = r(X)$.

As a consequence of the results by Brickell and Davenport [10], if Σ is an ideal scheme, then the polymatroid $\mathcal{S} = \mathcal{S}(\Sigma)$ is a matroid and, hence, $\mathcal{S}$ is a j-ss-polymatroid for every $j \in Q$. Moreover, by considering $(\pi_i(\mathbf{x}))_{i \in Q - \{j\}}$ as shares of the secret value $\pi_j(\mathbf{x})$, the scheme Σ defines an ideal secret sharing scheme with access structure $\Gamma_j(\mathcal{S})$ on the set of participants $Q - \{j\}$. We say that Γ is a *matroid-related* access structure if $\Gamma = \Gamma_D(\mathcal{M})$ for some matroid $\mathcal{M}$. Observe that all ideal access structures are matroid-related.

We need to recall now some terminology and basic facts about matroids. The set Q and the mapping r are called, respectively, the *set of points* and the *rank function* of the matroid $\mathcal{M}$. The value $r(X)$ is called the *rank* of the subset X while the *rank of the matroid* $\mathcal{M}$ is defined to be $r(\mathcal{M}) = r(Q)$.

A subset $X \subset Q$ is said to be *independent* if $r(X) = |X|$. The *dependent* subsets are those that are not independent. A *circuit* is a minimally dependent subset while a *basis* is a maximally independent subset. All bases have the same number of elements, which coincide with the rank of the matroid.

Let $\mathbb{K}$ be a finite field and let M be a $r_0 \times n$ matrix with entries in $\mathbb{K}$. If $|Q| = n$ and the points in Q are put in a one-to-one correspondence with the columns of M, a matroid $\mathcal{M}$ on the set Q is obtained by considering that the rank of a subset $X \subset Q$ is equal to the rank of the corresponding columns of M. In this situation, we say that the matrix M is a $\mathbb{K}$*-representation* of the matroid $\mathcal{M}$. The matroids that can be defined in this way are

called *representable*. Observe that representable matroids coincide with the ones that are obtained from vector space secret sharing schemes and their related access structures are precisely the vector space access structures.

The matroid $\mathcal{M}$ is said to be *connected* if, for every two different points $i, j \in Q$, there exists a circuit C with $i, j \in C$. As a consequence of [26, Proposition 4.1.2], the matroid $\mathcal{M}$ is connected if and only if the access structure $\Gamma_D(\mathcal{M})$ is connected. A connected matroid is determined by the circuits that contain some given point [20]. Therefore, if Γ is a matroid-related connected access structure, there exists a unique matroid $\mathcal{M}$ with $\Gamma = \Gamma_D(\mathcal{M})$.

If $\mathcal{M} = (Q, r)$ is a matroid, the mapping $r^*\colon \mathcal{P}(Q) \to \mathbb{Z}$ defined by $r^*(X) = |X| - r(Q) + r(Q - X)$ is the rank function of a matroid $\mathcal{M}^* = (Q, r^*)$, which is called the *dual* of the matroid $\mathcal{M}$. The dual of the access structure Γ on the set P is defined as the access structure $\Gamma^* = \{A \subset P : P - A \notin \Gamma\}$. Since $\Gamma_D(\mathcal{M}^*) = (\Gamma_D(\mathcal{M}))^*$, the dual of a matroid-related access structure is matroid-related.

3 Polymatroids and Optimal Information Rate

Most of the upper bounds on the optimal information rate that have been given until now were obtained by information-theoretical arguments. Specifically, by using basic properties of the Shannon entropy function. Csirmaz [13] pointed out that all those results are based solely on the fact that every secret sharing scheme defines a D-ss-polymatroid related to the access structure.

If $\mathcal{S} = (Q, h)$ is a polymatroid, we define $\sigma(\mathcal{S}) = \max\{h(\{x\}) : x \in Q\}$. For every access structure Γ, we consider the value $\kappa(\Gamma) = \inf \sigma(\mathcal{S})$, where the infimum is taken over all D-ss-polymatroids $\mathcal{S}$ with $\Gamma = \Gamma_D(\mathcal{S})$. The upper bounds on the optimal information rate that can be obtained by using polymatroids are based on the following proposition.

Proposition 4. *The optimal information rate of every access structure Γ is upper bounded by $\rho(\Gamma) \leq 1/\kappa(\Gamma)$.*

Proof. Let Σ be a secret sharing scheme with access structure Γ and let $\mathcal{S} = (Q, h)$ be the D-ss-polymatroid defined by Σ. Then, $\rho(\Sigma) = 1/\sigma(\mathcal{S}) \leq 1/\kappa(\Gamma)$. □

Therefore, upper bounds on $\rho(\Gamma)$ can be found by deriving lower bounds on $\kappa(\Gamma)$ from combinatorial properties of the access structure. Actually, $1/\kappa(\Gamma)$ is the best upper bound that can be obtained by this technique. Of course, $\kappa(\Gamma) = 1$ if Γ is matroid-related.

As far as we now, the only known upper bounds that do not fit this pattern are the one given by Gál [16] and the one presented by Beimel and Livne [2]. The first one applies only to linear secret sharing schemes and is the basis for proving the separation between the complexities of linear and nonlinear schemes [1, 4]. The second one applies to the access structures related to the Vamos matroid.

As an example of the kind of results that are obtained by using polymatroids, we present the *independent sequence method*, which was introduced in [6] and was improved in [27]. Let Γ be an access structure on a set of participants P. Let us consider $A \subset P$ and an increasing sequence of subsets $B_1 \subset \cdots \subset B_m \subset P$. We say that $(B_1, \ldots, B_m \,|\, A)$ is an *independent sequence* in Γ with *length* m and *size* s if $|A| = s$ and, for every $i = 1, \ldots, m$, there exists $X_i \subset A$ such that $B_i \cup X_i \in \Gamma$, while $B_m \notin \Gamma$ and, if $i \geq 2$, $B_{i-1} \cup X_i \notin \Gamma$. The independent sequence method is based on the following result.

Theorem 5. ([6, 27]) *Let Γ be an access structure on the set P. Let $\mathcal{S} = (Q, h)$ be a D-ss-polymatroid such that $\Gamma = \Gamma_D(\mathcal{S})$. If there exists in Γ an independent sequence $(B_1, \ldots, B_m \,|\, A)$ with length m and size s, then $h(A) \geq m$. As a consequence, $\kappa(\Gamma) \geq m/s$ and $\rho(\Gamma) \leq s/m$.*

We notice that this theorem was not stated in [6, 27] in terms of polymatroids, but in terms of the entropy function. The proof in [6] is easily adapted to this new statement. The following corollary of that theorem points out that independent sequences can be used in the characterization of matroid-related access structures. Actually, the converse of this result will be proved in Section 4.

Corollary 6. *An access structure Γ is not matroid-related if there exists an independent sequence with $s < m$.*

The next result by Csirmaz [13] points out the limitations of the use of polymatroids to find upper bounds on the optimal information rate.

Theorem 7. ([13]) *If Γ is an access structure on a set of participants P with $|P| = n$, then $\kappa(\Gamma) \leq n$.*

Proof. It is not difficult to prove that there exists a D-ss-polymatroid $\mathcal{S} = (Q, h)$ with $\Gamma = \Gamma_D(\mathcal{S})$ such that $h(X) = n + (n-1) + \cdots + (n-(k-1))$ for every subset of participants $X \subset P$ with $|X| = k$. □

By taking into account the known methods to construct secret sharing schemes, it is against intuition to suppose that there can exist, for every access structure, a secret sharing scheme such that the length of the shares is around n times the length of the secret. Therefore, as a consequence of Theorem 7, it seems that the optimal information rate of an access structure will be in general much smaller than $1/\kappa(\Gamma)$, the best upper bound that can be obtained by using polymatroids.

Nevertheless, the polymatroid technique has proved to be very useful when studying some particular families of access structures. In some cases the obtained upper bounds are tight or, at least, close to the best known lower bounds. In the following we prove a positive result for the polymatroid technique: the bounds that are obtained for Γ apply also to the dual access structure Γ^*. Let us recall that we are supposing that all access structures are connected. In particular, $\Gamma \neq \emptyset$ and $\emptyset \notin \Gamma$.

Theorem 8. *Let Γ be an access structure and let Γ^* be its dual. Then, $\kappa(\Gamma) = \kappa(\Gamma^*)$.*

The proof of this theorem is divided into several partial results. There exist several inequivalent ways to define the dual of a polymatroid [37] and we have to choose the suitable one to prove Theorem 8. Specifically, if $\mathcal{S} = (Q, h)$ is a polymatroid, we consider the *dual polymatroid* $\mathcal{S}^* = (Q, h^*)$, where $h^* \colon \mathcal{P}(Q) \to \mathbb{R}$ is defined by $h^*(X) = \sum_{x \in X} h(\{x\}) - h(Q) + h(Q - X)$. We prove in the next lemma that $\mathcal{S}^*$ is actually a polymatroid.

Lemma 9. *$\mathcal{S}^* = (Q, h^*)$ is a polymatroid.*

Proof. Obviously, $h^*(\emptyset) = 0$. Let us take a subset $X \subset Q$ and a point $y \notin X$. Then, $h^*(X \cup \{y\}) = h(\{y\}) + \sum_{x \in X} h(\{x\}) - h(Q) + h(Q - (X \cup \{y\}))$. Since $h(\{y\}) + h(Q - (X \cup \{y\})) \geq h(Q - X)$, we get that $h^*(X \cup \{y\}) \geq h^*(X)$. Therefore, h^* is monotone increasing. Finally, let us consider two arbitrary subsets $X, Y \subset Q$. Then, from the definition of h^* and the submodularity of h,

$$h^*(X) + h^*(Y) - h^*(X \cup Y) - h^*(X \cap Y) =$$

$$= h(Q - X) + h(Q - Y) - h(Q - (X \cup Y)) - h(Q - (X \cap Y)) \geq 0.$$

This proves that h^* is submodular. □

To be precise, the polymatroid $\mathcal{S}^*$ is properly a dual of $\mathcal{S}$, in the sense that $\mathcal{S}^{**} = \mathcal{S}$, if and only if $h(Q - \{x\}) = h(Q)$ for every $x \in Q$. The polymatroids verifying this property will be said to be *normalized*. To prove the next lemma is an easy exercise.

Lemma 10. *Let $\mathcal{S} = (Q, h)$ be a polymatroid. Then, the following properties hold.*

1. *The polymatroid $\mathcal{S}^* = (Q, h^*)$ is normalized.*
2. *$h^{**}(X) \leq h(X)$ for every $X \subset Q$.*
3. *$\mathcal{S}$ is normalized if and only if $\mathcal{S}^{**} = \mathcal{S}$.*
4. *If $\mathcal{S}$ is normalized, then $h^*(\{x\}) = h(\{x\})$ for every $x \in Q$.*

Lemma 11. *Let $\mathcal{S} = (Q, h)$ be a D-ss-polymatroid. Then, $\mathcal{S}^* = (Q, h^*)$ is also a D-ss-polymatroid and, moreover, $\Gamma_D(\mathcal{S}^*) = (\Gamma_D(\mathcal{S}))^*$.*

Proof. Let us take $\Gamma = \Gamma_D(\mathcal{S})$. Since $P = Q - \{D\} \in \Gamma$, we have that $h(Q - \{D\}) = h(Q)$ and, hence, $h^*(\{D\}) = h(\{D\}) = 1$. Let us consider a subset $X \subset P = Q - \{D\}$. Then,

$$h^*(X \cup \{D\}) = h(\{D\}) + \sum_{x \in X} h(\{x\}) - h(Q) + h(P - X).$$

If $X \in \Gamma^*$, then $P - X \notin \Gamma$ and $h(P - X) = h(Q - X) - 1$. In this case, $h^*(X \cup \{D\}) = h^*(X)$. Analogously, if $X \notin \Gamma^*$ then $h(P - X) = h(Q - X)$ and, hence, $h^*(X \cup \{D\}) = h^*(X) + 1$. □

Proof of Theorem 8. Let Γ be an access structure. Let us consider the subsets of $\mathbb{R}$

$$\Omega(\Gamma) = \{\sigma(\mathcal{S}) : \Gamma = \Gamma_D(\mathcal{S})\} \quad \text{and} \quad \widehat{\Omega}(\Gamma) = \{\sigma(\mathcal{S}) : \mathcal{S} \text{ is normalized, } \Gamma = \Gamma_D(\mathcal{S})\}.$$

If $\mathcal{S}$ is a D-ss-polymatroid such that $\Gamma = \Gamma_D(\mathcal{S})$, then $\mathcal{S}^{**}$ is normalized, $\Gamma = \Gamma_D(\mathcal{S}^{**})$ and $\sigma(\mathcal{S}^{**}) \leq \sigma(\mathcal{S})$. Therefore, $\kappa(\Gamma) = \inf \Omega(\Gamma) = \inf \widehat{\Omega}(\Gamma)$. The proof is concluded by taking into account that $\widehat{\Omega}(\Gamma) = \widehat{\Omega}(\Gamma^*)$. □

4 On the Characterization of Matroid-Related Access Structures

4.1 A Theorem by Seymour

Let Γ be an access structure on a set P and let us take a subset $Z \subset P$. We define the access structures $\Gamma \setminus Z$ and Γ / Z on the set $P - Z$ by $\Gamma \setminus Z = \{A \subset P - Z : A \in \Gamma\}$ and $\Gamma / Z = \{A \subset P - Z : A \cup Z \in \Gamma\}$. Every access structure that can be obtained from Γ by

repeatedly applying the operations $\setminus$ and $/$ is called a *minor of the access structure* Γ. If Z_1 and Z_2 are disjoint subsets then $(\Gamma \setminus Z_1)/Z_2 = (\Gamma/Z_2) \setminus Z_1$, and $(\Gamma \setminus Z_1) \setminus Z_2 = \Gamma \setminus (Z_1 \cup Z_2)$, and $(\Gamma/Z_1)/Z_2 = \Gamma/(Z_1 \cup Z_2)$. Therefore, every minor of Γ is in the form $(\Gamma \setminus Z_1)/Z_2$ for some disjoint subsets $Z_1, Z_2 \subset P$. In addition, $(\Gamma \setminus Z)^* = \Gamma^*/Z$ and $(\Gamma/Z)^* = \Gamma^* \setminus Z$.

We introduce now the forbidden minors in the characterization by Seymour. The set of participants or the access structures Φ and $\widehat{\Phi}$ is $P = \{p_1, p_2, p_3, p_4\}$. The minimal qualified subsets of Φ are $\{p_1, p_2\}$, $\{p_2, p_3\}$ and $\{p_3, p_4\}$, while the minimal qualified subsets $\widehat{\Phi}$ are $\{p_1, p_2\}$, $\{p_2, p_3\}$, $\{p_2, p_4\}$ and $\{p_3, p_4\}$. For every $s \geq 3$, the set of participants of the access structure Ψ_s is $P = \{p_1, \ldots, p_s, p_{s+1}\}$ and its minimal qualified subsets are $\{p_1, \ldots, p_s\}$ and $\{p_i, p_{s+1}\}$ for every $i = 1, \ldots, s$. Observe that $\Phi^* \cong \Phi$ and $\Psi_s^* = \Psi_s$. The minimal qualified subsets of $\widehat{\Phi}^*$ are $\{p_1, p_3, p_4\}$, $\{p_2, p_3\}$ and $\{p_2, p_4\}$.

The forbidden minor characterization of matroid ports by Seymour is stated here in our terminology.

Theorem 12. (Seymour [29]) *An access structure is matroid-related if and only if it has no minor isomorphic to Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s with $s \geq 3$.*

4.2 Generalizing the Result by Brickell and Davenport

New characterizations of matroid-related access structures are given in Theorem 13. They are obtained by combining Theorem 12 with the results in Section 3. As a consequence, we generalize in Corollary 17 the result by Brickell and Davenport [10] by proving that not only the access structures of ideal secret sharing schemes are matroid-related, but the access structures of all schemes with information rate greater than 2/3.

Theorem 13. *Let Γ be an access structure on a set of participants P. Then, the following statements are equivalent.*

1. *Γ is matroid-related.*
2. *Γ has no minor isomorphic to Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s with $s \geq 3$.*
3. *$\kappa(\Gamma) < 3/2$.*
4. *There does not exist in Γ any independent sequence with length $m = 3$ and size $s = 2$.*
5. *There does not exist in Γ any independent sequence with length m and size s such that $m > s$.*

Observe that, in particular, Theorem 13 implies that there is a gap in the values of $\kappa(\Gamma)$. Namely, there does not exist any access structure Γ with $1 < \kappa(\Gamma) < 3/2$.

In order to prove this theorem we need to introduce some new concepts and to present some partial results.

As we did before with access structure, we can consider as well *minors* of matroids and polymatroids. Let $\mathcal{S} = (Q, h)$ be a polymatroid. Given a subset $Z \subset Q$, we define the polymatroids $\mathcal{S} \setminus Z = (Q - Z, h_{\setminus Z})$ and $\mathcal{S}/Z = (Q - Z, h_{/Z})$, where $h_{\setminus Z}(X) = h(X)$ and $h_{/Z}(X) = h(X \cup Z) - h(Z)$. Clearly, $\sigma(\mathcal{S} \setminus Z) \leq \sigma(\mathcal{S})$ and $\sigma(\mathcal{S}/Z) \leq \sigma(\mathcal{S})$. It is not difficult to prove that, if $\mathcal{S}$ is a D-ss-polymatroid and $\Gamma = \Gamma_D(\mathcal{S})$, then, for every $Z \subset P$, both $\mathcal{S} \setminus Z$ and $\mathcal{S}/Z$ are D-ss-polymatroids and $\Gamma \setminus Z = \Gamma_D(\mathcal{S} \setminus Z)$ and $\Gamma/Z = \Gamma_D(\mathcal{S}/Z)$. If $\mathcal{M} = (Q, r)$ is a matroid, then $\mathcal{M} \setminus Z$ and $\mathcal{M}/Z$ are matroids as well. The following lemma is a direct consequence of all these considerations.

Lemma 14. *The following statements hold.*

1. *Every minor of a matroid-related access structure is matroid-related.*
2. *If Γ' is a minor of the access structure Γ, then $\kappa(\Gamma') \leq \kappa(\Gamma)$.*

The independent sequence method we have described in Section 3 has a good behavior with respect to minors.

Lemma 15. *Let Γ' be a minor of an access structure Γ. If there exists in Γ' an independent sequences with length m and size s, then the same occurs for Γ.*

Proof. Let us consider disjoint subsets $Z_1, Z_2 \subset P$ such that $\Gamma' = (\Gamma \backslash Z_1)/Z_2$. Let us suppose that $(B_1, \ldots, B_m \,|\, A)$ is an an independent sequence with length m and size $s = |A|$ in Γ'. Then, $(B_1 \cup Z_2, \ldots, B_m \cup Z_2 \,|\, A)$ is an independent sequence in Γ. □

Proposition 16. *Every one of the access structures Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ and Ψ_s, with $s \geq 3$, admits an independent sequence with length $m = 3$ and size $s = 2$. In particular, $\kappa(\Gamma) \geq 3/2$ if Γ is any of these structures.*

Proof. We are going to consider sequences $(B_1, B_2, B_3 \,|\, a_1 a_2)$ with $B_1 \subset B_2 \subset B_3 \subset P$ and $a_1, a_2 \in P$. Such a sequence will be independent in the access structure Γ if the subsets $B_1 \cup \{a_1, a_2\}$, $B_2 \cup \{a_1\}$ and $B_3 \cup \{a_2\}$ are in Γ while $B_1 \cup \{a_1\}$, $B_2 \cup \{a_2\}$ and B_3 are not qualified. The sequence $(\emptyset, \{p_1\}, \{p_1, p_4\} \,|\, p_2 p_3)$ is independent for both Φ and $\widehat{\Phi}$, while an independent sequence for $\widehat{\Phi}^*$ is $(\emptyset, \{p_4\}, \{p_1, p_4\} \,|\, p_2 p_3)$. Finally, $(\emptyset, \{p_s\}, \{p_2, \ldots, p_s\} \,|\, p_{s+1} p_1)$ is an independent sequence in Ψ_s. □

Proof of Theorem 13. The equivalence between 1 and 2 is Theorem 12. By combining this result with Corollary 6, Lemmas 14 and 15, and Proposition 16, we get the other equivalences. □

Brickell and Davenport [10] proved that the access structure of every ideal secret sharing scheme is matroid-related. As a corollary of Theorem 13, we obtain a generalization of that important result. Moreover, since it has not been used in the proof of Theorem 13, we have presented here an alternative proof to the result by Brickell and Davenport.

Corollary 17. *If the access structure Γ can be realized by a secret sharing scheme with information rate greater than $2/3$, then Γ is matroid-related.*

This result had been observed in most of the families for which the characterization of ideal access structures were studied. Since in all these families the matroid-related access structures coincide with the ideal ones, we cannot find in them any access structure with $2/3 < \rho(\Gamma) < 1$. Of course, this result can be now extended now to other familes such as the weighted threshold access structures that were studied in [3].

5 On Non-Ideal Matroid-Related Access Structures

Since there exist matroids that are not ss-representable, there are matroid-related access structures that are not ideal. Very little is known about the optimal information rate of these structures. We cannot find upper bounds by the techniques in Section 3 because $\kappa(\Gamma) = 1$ if

Γ is matroid-related. By using other techniques, upper bounds have been given by Beimel and Livne [2]. We present here some lower bounds on the optimal information rate of the access structures related to the Vamos matroid and the non-Desargues matroid.

The Vamos matroid $\mathcal{V}$ is the matroid on the set $Q_1 = \{v_1, \ldots, v_8\}$ such that its bases are all sets with cardinality 4 except the following five: $\{v_1, v_2, v_3, v_4\}$, $\{v_1, v_2, v_5, v_6\}$, $\{v_3, v_4, v_5, v_6\}$, $\{v_3, v_4, v_7, v_8\}$ and $\{v_5, v_6, v_7, v_8\}$. The Vamos matroid is not ss-representable [30] and, hence, the access structures related to it are not ideal. In a recent work, Beimel and Livne [2] prove that, for every secret sharing scheme realizing one of these access structures with domain of the secrets of size k, the size of the domain of the shares is at least $k + \Omega(\sqrt{k})$. Observe that this bound does not exclude that the optimal information rate of these structures may be equal to one, because $\rho(\Gamma)$ is the *supremum* of the information rates of the schemes realizing Γ.

The non-Desargues matroid $\mathcal{D}$ is the matroid with rank 3 on the set with 10 points that is determined by a non-Desargues configuration on a projective plane. That is, let us take three different lines L_1, L_2, L_3 that meet in a point p_0 and, on the line L_i, two different points $q_i, r_i \neq p_0$. Finally, let us consider the points s_{12}, s_{23} and s_{31}, where s_{ij} is the intersection of the lines q_iq_j and r_ir_j. If such a configuration has been taken on a projective plane over a field, the points s_{12}, s_{23} and s_{31} must be collinear by the Desargues Theorem. The non-Desargues matroid is defined by this configuration but considering that the three points s_{ij} are not collinear. That is, the set of points is $Q_2 = \{p_0, q_1, q_2, q_3, r_1, r_2, r_3, s_{12}, s_{23}, s_{31}\}$ and the bases are all subsets with three points that are not supposed to be collinear. As a consequence of the Desargues Theorem, this matroid is not representable. Moreover, Matúš [25] proved that $\mathcal{D}$ is not ss-representable.

Lower bounds on the optimal information rate of the access structures related to those matroids are given in the next theorem. We just present here a sketch of the proof. All details will be discussed in the full version.

Theorem 18. *Let us consider two arbitrary points $D_1 \in Q_1$ and $D_2 \in Q_2$ and the access structures $\Gamma_1 = \Gamma_{D_1}(\mathcal{V})$ and $\Gamma_2 = \Gamma_{D_2}(\mathcal{D})$. Then, $\rho(\Gamma_1) \geq 2/3$ and $\rho(\Gamma_2) \geq 3/4$.*

Proof. There exists a finite field $\mathbb{K}$ such that, for every $x \in P_2 = Q_2 - \{D_2\}$, the matroid $\mathcal{D} \setminus \{x\}$ is $\mathbb{K}$-representable and, hence, $\Gamma_2 \setminus \{x\}$ is a $\mathbb{K}$-vector space access structure. Therefore, we can apply the λ-decomposition technique by Stinson [35] to the nine access structures $(\Gamma_2 \setminus \{x\})_{x \in P_2}$. By doing that, a secret sharing scheme for Γ_2 with information rate equal to $3/4$ is obtained.

Let us suppose that $D_1 = v_1$. For every $2 \leq i < j \leq 8$, let $\Gamma^{(i,j)}$ be the access structure on P_1 whose minimal qualified subsets are the minimal qualified subsets A of Γ_1 such that $\{v_i, v_j\} \not\subset A$. It can be proved that $\Gamma^{(3,4)}$, $\Gamma^{(5,6)}$ and $\Gamma^{(7,8)}$ are $\mathbb{K}$-vector space access structures for some finite field $\mathbb{K}$. By applying the λ-decomposition technique to these substructures, we get that $\rho(\Gamma_1) \geq 2/3$. A similar construction can be obtained for other values of $D_1 \in Q_1$. □

Acknowledgments

The second author thanks Ronald Cramer, Bert Gerards, Robbert de Haan and Lex Schrijver for useful discussions, comments, and suggestions. Thanks to Lex Schrijver who pointed out

the existence of the paper by P.D. Seymour on matroid ports [29] and to Bert Gerards who independently found the construction in Theorem 7.

References

1. A. Beimel, Y. Ishai. On the power of nonlinear secret sharing schemes. *SIAM J. Discrete Math.* **19** (2005) 258–280.
2. A. Beimel, N. Livne. On Matroids and Non-ideal Secret Sharing. *Second Theory of Cryptography Conference, TCC 2006. Lecture Notes in Comput. Sci.*, to appear.
3. 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.
4. A. Beimel, E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.* **34** (2005) 1196–1215.
5. G.R. Blakley, Safeguarding cryptographic keys. *AFIPS Conference Proceedings*. **48** (1979) 313–317.
6. 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.
7. 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.
8. C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.
9. E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.
10. E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.
11. E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology* **5** (1992), 153–166.
12. 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.
13. L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.
14. S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* **39** (1978) 55–72.
15. S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18.
16. A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Proceedings of 30th ACM Symposium on the Theory of Computing, STOC 1998*, 1998, 429–437.
17. M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.* (1987) 99–102.
18. W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286.
19. E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.
20. A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725.
21. A. Lehman. Matroids and Ports. *Notices Amer. Math. Soc.* **12** (1976) 356–360.
22. J.Martí-Farré, C. Padró. Secret sharing schemes on sparse homogeneous access structures with rank three. *Electronic Journal of Combinatorics* **11(1)** (2004) Research Paper 72, 16 pp. (electronic).
23. J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes Cryptogr.* **34** (2005) 17–34.
24. J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics* **154** (2006) 552–563.
25. F. Matúš. Matroid representations by partitions. *Discrete Math.* **203** (1999) 169–194.
26. J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
27. C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604.
28. C. Padró, G. Sáez. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. *Inform. Process. Lett.* **83** (2002) 345–351.

29. P.D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.
30. P.D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B*, **56** (1992) pp. 69–73.
31. A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.
32. J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) pp. 179–197.
33. D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.
34. D.R. Stinson. New general lower bounds on the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92, Lecture Notes in Comput. Sci.* **740** (1993) 168-182.
35. D.R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory* **40** (1994) 118–125.
36. T. Tassa. Hierarchical Threshold Secret Sharing. *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004. Lecture Notes in Comput. Sci.* **2951** (2004) 473–490.
37. D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.