On Secret Sharing Schemes, Matroids and Polymatroids*

Jaume Martí-Farré, Carles Padró
Dep. de Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, Barcelona, Spain
{jaumem,cpadro}@ma4.upc.edu

June 22, 2009

Abstract

The complexity of a secret sharing scheme is defined as the ratio between the maximum length of the shares and the length of the secret. The optimization of this parameter for general access structures is an important and very difficult open problem in secret sharing. We explore in this paper the connections of this open problem with matroids and polymatroids.

Matroid ports were introduced by Lehman in 1964. A forbidden minor characterization of matroid ports was given by Seymour in 1976. These results are previous to the invention of secret sharing by Shamir in 1979. Important connections between ideal secret sharing schemes and matroids were discovered by Brickell and Davenport in 1991. Their results can be restated as follows: every ideal secret sharing scheme defines a matroid, and its access structure is a port of that matroid. In spite of this, the results by Lehman and Seymour and other subsequent results on matroid ports have not been noticed until now by the researchers interested in secret sharing.

Lower bounds on the optimal complexity of access structures can be found by taking into account that the joint Shannon entropies of a set of random variables define a polymatroid. We introduce a new parameter, which is denoted by κ, to represent the best lower bound that can be obtained by this method. We prove that every bound that is obtained by this technique for an access structure applies to its dual structure as well.

By using the aforementioned result by Seymour we obtain two new characterizations of matroid ports. The first one refers to the existence of a certain combinatorial configuration in the access structure, while the second one involves the values of the parameter κ that is introduced in this paper. Both are related to bounds on the optimal complexity. As a consequence, we generalize the result by Brickell and Davenport by proving that, if the length of every share in a secret sharing scheme is less than $3/2$ times the length of the secret, then its access structure is a matroid port. This generalizes and explains a phenomenon that was observed in several families of access structures.

Finally, we present a construction of linear secret sharing schemes for the ports of the Vamos matroid and the non-Desargues matroid, which do not admit any ideal secret sharing scheme. We obtain in this way upper bounds on their optimal complexity. These new bounds are a contribution on the search of examples of access structures whose optimal complexity lies between 1 and $3/2$.

Key words. Secret sharing, Optimization of secret sharing schemes for general access structures, Ideal secret sharing schemes, Matroids, Polymatroids.

*This work was partially supported by the Spanish Ministry of Education and Science under projects TIC2003-00866 and TSI2006-02731. 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. A preliminary version of this work appeared in *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Computer Science* **4392** (2007) 273–290.

1 Introduction

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, which was independently introduced by Shamir [41] and Blakley [8] in 1979, is a very important cryptographic primitive and it is a fundamental building block for many different kinds of cryptographic protocols.

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. Because of that, no restriction on the computational power of the participants is assumed. The reader is referred to Stinson's *Explication of secret sharing schemes* [43] for an excellent introduction to the topic.

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

There exists a secret sharing scheme for every access structure. Constructive proofs for this fact are given in [7, 24]. The schemes that are obtained by these methods are inefficient because the size of the shares grows exponentially with the number of participants. Nevertheless, the existence of better general constructions is still unknown. The optimization of secret sharing schemes for general access structures is one of the main research topics on secret sharing.

The size of the shares, usually in relation to the size of the secret value, is the commonest way to measure the efficiency of a secret sharing scheme. To this end, we consider here the *complexity* of a secret sharing scheme, which is the ratio between the maximum length (in bits) of the shares and the length of the secret value. This is actually the inverse of the *information rate*, a parameter that has been widely considered in the literature. The *optimal complexity* $\sigma(\Gamma)$ of an access structure Γ is the infimum of the complexities of all secret sharing schemes for Γ. This paper deals with the open problem of determining the value of this parameter for every given access structure. Several techniques have been proposed to find bounds on the optimal complexity of an access structure. Nevertheless, there is a huge gap between the best known general lower and upper bounds.

A secret sharing scheme is said to be *linear* if the secret value and the shares are vectors over some finite field and they are the values of some given linear maps on a random vector. The infimum complexity of all linear secret sharing schemes for an access structure Γ is denoted by $\lambda(\Gamma)$. Clearly, $\sigma(\Gamma) \leq \lambda(\Gamma)$.

In all secret sharing schemes, the length of every share is at least the length of the secret [27]. A secret sharing scheme is said to be *ideal* if all shares have the same length as the secret. The access structures of ideal secret sharing schemes are called *ideal* as well. For example, the (t, n)-threshold access structure, which consists of all subsets with at least t participants out of a set of n, is ideal because it can be realized by the ideal scheme proposed by Shamir [41]. The characterization of the ideal access structures has attracted the attention of many researchers. Brickell and Davenport [13] discovered strong connections of this open problem with matroid theory. Specifically, every ideal secret sharing scheme defines a unique matroid, and hence ideal secret sharing schemes can be seen as representations of matroids that actually include linear representations because of the construction of ideal linear schemes proposed by Brickell [12].

Surprisingly enough, the authors interested on secret sharing have been unaware until recently that the result by Brickell and Davenport [13] can be stated in terms of *matroid ports*, a combinatorial object that was introduced by Lehman [28] in 1964 to solve the Shannon switching game. Actually, after a small change in the definition of matroid port to adapt it to our topic, the main result in [13] can be rewritten as follows: every ideal access structure is a matroid port.

This necessary condition for an access structure to be ideal is not sufficient because there exist matroids that can not be represented by any ideal secret sharing scheme, and hence there exist matroid ports that are not ideal access structures. The first example of such a matroid, the *Vamos matroid*, was presented by Seymour [40], and other examples, being the *non-Desargues matroid* among them, were given by Matúš [33].

Two techniques have been mostly used until now in the search for bounds on the optimal complexity of access structures. On one hand, upper bounds have been obtained from different decomposition methods by means of which several linear secret sharing schemes are combined into a new one [11, 14, 18, 26, 38, 44, 45]. Upper bounds on $\lambda(\Gamma)$ are obtained in this way. On the other hand, lower bounds on the optimal complexity have been derived by combining the basic inequalities of Shannon entropy with the requirements given by the access structure [9, 10, 15, 26]. Csirmaz [17] simplified and unified the techniques in those works by revealing the combinatorial nature of the method. More specifically, he pointed out that the previous lower bounds were solely based on the fact that every secret sharing scheme for a given access structure defines a polymatroid with certain properties.

In this paper we contribute to a better understanding of this combinatorial method. A new parameter, called $\kappa(\Gamma)$, is introduced in Section 3 to represent the best lower bound on the optimal complexity that can be obtained by using polymatroids. Obviously,

$$\kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma).$$

The parameters κ and λ mark the limits of the two aforementioned techniques for the search of bounds on the optimal complexity. This is due to the fact that the construction of linear secret sharing schemes for a given access structure by using decomposition methods provides upper bounds on $\lambda(\Gamma)$, and the lower bounds on $\sigma(\Gamma)$ that can be derived from the basic inequalities of Shannon entropy are actually lower bounds on $\kappa(\Gamma)$. Therefore, determining the values of the new parameter κ and finding out the separation between κ and σ are new open problems that have important implications. Some important results showing a separation between the parameters σ and λ have been given in [1, 6, 23]. They imply that linear schemes are not among the optimal schemes for every access structure.

We prove in Theorem 3.9, one of our main results, that $\kappa(\Gamma) = \kappa(\Gamma^*)$, that is, every lower bound that is obtained for Γ by using polymatroids applies also to the dual access structure Γ^*. The use of this result would greatly simplify, for instance, the computation in [26] of the lower bounds for the access structures on five participants. A similar behavior was known for the parameter $\lambda(\Gamma)$. Specifically, from every linear secret sharing scheme for an access structure Γ, a linear scheme with the same complexity can be obtained for the dual access structure Γ^* [20, 25], and hence $\lambda(\Gamma) = \lambda(\Gamma^*)$. The relation between $\sigma(\Gamma)$ and $\sigma(\Gamma^*)$ is still an open problem.

Seymour [39] presented in 1976 a characterization of matroid ports by excluded minors that is based on a previous characterization of matroid ports due to Lehman [29]. These results, which were presented before secret sharing was invented, were not noticed by the researchers in this topic, but they can be very useful for the open problems considered here. One example of this is our main result, Theorem 4.4, which has important consequences and enhances our understanding about the connections between secret sharing and matroid theory. Its proof mainly based on Seymour's characterization of matroid ports [39]. Theorem 4.4 provides two new characterizations of matroid ports. The first one refers to the existence of independent sequences, combinatorial configurations in the access structure that provide lower bounds on $\kappa(\Gamma)$. The independent sequence technique was introduced in [11] and it was improved in [37]. It is restated here in Theorem 3.4. The second one deals with the value of $\kappa(\Gamma)$. Namely, an access structure Γ is a matroid port if and only if $\kappa(\Gamma) < 3/2$. Because of that, our new characterizations of matroid ports have interesting implications in the open problem that is considered here.

One of the most remarkable consequences of Theorem 4.4 is related to a repeated phenomenon was observed in several families of access structures as, for instance, the ones defined by graphs [15], the ones on at most five participants [43, 26], the bipartite access structures [37], the structures with at most four minimal qualified subsets [31], or the ones with intersection number equal to one [32]. Namely, in all these families, the optimal complexity of every non-ideal access structure is at least 3/2. On one hand, this suggested the existence of a general result, namely, a gap in the values of the optimal complexity $\sigma(\Gamma)$. But, on the other hand, this common property was proved by methods that seemed to be specific to every one of those families, and hence it was not clear that there existed a common explanation.

Theorem 4.4 generalizes and explains this repeated behavior. Actually, in all those families the ideal access structures coincide with the matroid ports, and hence $\sigma(\Gamma) \geq \kappa(\Gamma) \geq 3/2$ if Γ is a non-ideal access structure. Therefore, our new characterization of matroid ports provides a unified explanation for the gap in the values of $\sigma(\Gamma)$ that was observed in those families. Our result can be also seen as a generalization of the result by Brickell and Davenport [13], who proved that all ideal access structures are matroid ports. As a direct consequence of Theorem 4.4, if the complexity of a secret sharing scheme is less than 3/2, then its access structure is a matroid port.

The existence of access structures with $1 < \sigma(\Gamma) < 3/2$ has been an open problem until recently. As a consequence of our main result, such access structures must be matroid ports. Actually, Theorem 4.4 implies that such a gap exists on the values of the parameter κ, that is, there is no access structure Γ with $1 < \kappa(\Gamma) < 3/2$. We contribute here to the solution of this open problem by proving in Section 5 that the optimal complexities of the ports of the Vamos matroid and the non-Desargues matroid are at most 4/3. Those matroid ports are known to be non-ideal [33, 40], but this does not imply that their optimal complexities are larger than 1. Nevertheless, it has been proved in [3], a paper that appeared during the preparation of this work, that the optimal complexities of the ports of the Vamos matroid are actually larger than 1. Therefore, these are the first known examples of access structures with $1 < \sigma(\Gamma) < 3/2$.

2 Preliminaries

2.1 On Access Structures Defined from Matroids and Polymatroids

In this section we present some definitions connecting access structures to matroids and polymatroids. The relevance of these definitions in secret sharing will be made clear in the following sections. The reader is referred to [36, 46] for general references on matroid theory. The book by Welsh [46] contains a chapter about polymatroids.

For a set P, we notate $\mathcal{P}(P)$ for the power set of P. An *access structure* on P is a monotone increasing family $\Gamma \subseteq \mathcal{P}(P)$ of subsets of P, that is, $Y \in \Gamma$ if $X \subseteq Y \subseteq P$ and $X \in \Gamma$. The elements in Γ are called the *qualified subsets* of the access structure. Obviously, an access structure Γ is determined by the family $\min \Gamma$ of its minimal qualified subsets. A participant is said to be *redundant* in an access structure if there is no minimal qualified set containing it. An access structure is *connected* if there is not any redundant participant in it. All participants are redundant in the two *trivial access structures* $\emptyset, \mathcal{P}(P) \subseteq \mathcal{P}(P)$.

A *polymatroid* is a pair $\mathcal{S} = (Q, h)$ formed by a finite set Q, called the *ground set*, and a *rank function* $h\colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

1. $h(\emptyset) = 0$.
2. h is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $h(X) \leq h(Y)$.

3. h is *submodular*: if $X, Y \subseteq Q$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$.

We say that $p_0 \in Q$ is an *atomic point* of the polymatroid $\mathcal{S} = (Q, h)$ if, for every $X \subseteq Q$, either $h(X \cup \{p_0\}) = h(X)$ or $h(X \cup \{p_0\}) = h(X) + 1$.

A *matroid* is a polymatroid $\mathcal{M} = (Q, h)$ such that $h(X) \in \mathbb{Z}$ and $0 \leq h(X) \leq |X|$ for every $X \subseteq Q$. A subset $X \subseteq Q$ is said to be an *independent set* of the matroid $\mathcal{M}$ if $h(X) = |X|$. 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 equals $h(Q)$, the *rank of the matroid* $\mathcal{M}$.

For a polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$ we define on the set $P = Q - \{p_0\}$ the access structure

$$\Gamma = \Gamma_{p_0}(\mathcal{S}) = \{X \subseteq P : h(X \cup \{p_0\}) = h(X)\}.$$

We have to check that Γ is monotone increasing. If $X \subseteq Y \subseteq P$ and $X \in \Gamma$, then the submodularity of h implies that $h(X) + h(Y) = h(X \cup \{p_0\}) + h(Y) \geq h(Y \cup \{p_0\}) + h(X)$, and hence $Y \in \Gamma$.

For an access structure Γ on $P = Q - \{p_0\}$, a polymatroid $\mathcal{S} = (Q, h)$ is said to be a Γ-*polymatroid* if p_0 is an atomic point of $\mathcal{S}$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$. There exist Γ-polymatroids for every access structure Γ. Observe that different polymatroids can define the same access structure.

If $h(\{x\}) = 0$ for every $x \in Q$, then $\Gamma_{p_0}(\mathcal{S}) = \mathcal{P}(P)$, and $\Gamma_{p_0}(\mathcal{S}) = \emptyset$ if $h(\{p_0\}) = 1$ and $h(\{x\}) = 0$ for every $x \in P$. If Γ is non-trivial and $\mathcal{S} = (Q, h)$ is a Γ-polymatroid, then $h(\{p_0\}) = 1$ and $h(P) = h(Q)$.

If $\mathcal{M} = (Q, r)$ is a matroid, then all its points are atomic and we can consider, for every $x \in Q$, the access structure $\Gamma_x(\mathcal{M})$ on the set $Q - \{x\}$. This access structure is called the *port of the matroid* $\mathcal{M}$ *at the point* x. With a slightly different definition, matroid ports were introduced in 1964 by Lehman [28] to solve the Shannon switching game. Seymour [39] presented in 1976 a characterization of matroid ports by excluded minors that is based on a previous characterization of matroid ports due to Lehman [29]. The minimal sets of a matroid port can be characterized by

$$\min \Gamma_x(\mathcal{M}) = \{A \subseteq Q - \{x\} : A \cup \{x\} \text{ is a circuit of } \mathcal{M}\}.$$

Actually, matroid ports were defined by Lehman as the families of subsets of this form. We changed here the definition in order to simplify the presentation.

A matroid $\mathcal{M} = (Q, r)$ is said to be *connected* if, for every two different points $x, y \in Q$, there exists a circuit C with $x, y \in C$. Clearly, all ports of a connected matroid are connected. Moreover, as a consequence of [36, Proposition 4.1.2], a matroid is connected if and only if at least one of its ports is connected. A connected matroid is determined by the circuits that contain some given point [28]. Therefore, if Γ is a connected matroid port, there exists a unique connected matroid $\mathcal{M}$ with $\Gamma = \Gamma_{p_0}(\mathcal{M})$.

2.2 Secret Sharing Schemes

Several different definitions for secret sharing have been proposed in the literature. We present here the most general one. Namely, a secret sharing scheme is defined as a set of random variables satisfying some properties in terms of their joint Shannon entropies. The reader is referred to [16] for a textbook containing more information about Shannon entropies.

Let Q be a finite set of *participants*. Consider a finite set E with a probability distribution on it. For every $i \in Q$, consider a finite set E_i and a map $\pi_i \colon E \to E_i$. Those maps induce random variables on the sets E_i. Let $H(E_i)$ denote the Shannon entropy of one of these random variables. For a subset $A = \{i_1, \ldots, i_r\} \subseteq Q$, we write $H(E_A)$ for the joint entropy

$H(E_{i_1} \dots E_{i_r})$, and a similar convention is used for conditional entropies as, for instance, in $H(E_j|E_A) = H(E_j|E_{i_1} \dots E_{i_r})$.

Consider a distinguished participant $p_0 \in Q$, which is usually called *dealer*, and an access structure Γ on the set $P = Q - \{p_0\}$. We write E_0 and π_0 for E_{p_0} and π_{p_0}, respectively. The maps π_i define an *unconditionally secure perfect secret sharing scheme* Σ with access structure Γ if the following properties are satisfied.

1. $H(E_0|E_A) = 0$ if $A \in \Gamma$.
2. $H(E_0|E_A) = H(E_0)$ if $A \notin \Gamma$.

In this 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 $s = \pi_0(\mathbf{x}) \in E_0$ is the *shared secret value*. Observe that the first requirement in the definition implies that the qualified subsets can recover the secret value from their shares and, by the second one, the shares of the participants in an unqualified subset do not provide any information at all about the secret value. Recall that only unconditionally secure perfect secret sharing schemes are considered in this paper.

The ratio

$$\sigma(\Sigma) = \frac{\max_{i\in P} H(E_i)}{H(E_0)}$$

is called the *complexity* of the scheme Σ, and the *optimal complexity* $\sigma(\Gamma)$ of the access structure Γ is the infimum of the complexities of all secret sharing schemes for Γ. It is not difficult to check that $H(E_i) \geq H(E_0)$ for every non-redundant participant $i \in P$, and hence $\sigma(\Sigma) \geq 1$ for every secret sharing scheme Σ with non-trivial access structure. Secret sharing schemes with $\sigma(\Sigma) = 1$ are said to be *ideal* and their access structures are called *ideal* as well.

If the sets E and E_i are vector spaces over some finite field $\mathbb{K}$, the maps π_i are linear, and the uniform probability distribution is considered in E, then Σ is said to be a $\mathbb{K}$*-linear secret sharing scheme*. The linear schemes in which $E_i = \mathbb{K}$ for every non-redundant participant $i \in P$ are ideal and they are called $\mathbb{K}$*-vector space secret sharing schemes*. Their access structures are called $\mathbb{K}$*-vector space access structures*. Observe that there exist ideal linear schemes that are not vector space secret sharing schemes. In such schemes, $\dim E_i = \dim E_0 > 1$ for every non-redundant participant $i \in P$. The complexity of a linear secret sharing scheme is

$$\sigma(\Sigma) = \frac{\max_{i\in P} \dim E_i}{\dim E_0}.$$

For an access structure Γ on P, we notate $\lambda(\Gamma)$ for the infimum of the complexities of the *linear* secret sharing schemes for Γ. Obviously, $\lambda(\Gamma) \geq \sigma(\Gamma)$ and, of course, every construction of a linear secret sharing scheme for Γ provides an upper bound for $\lambda(\Gamma)$, and hence for $\sigma(\Gamma)$. Efficient constructions can be obtained by using the existing methods to combine some given linear secret sharing schemes into a new one [14, 18, 26, 38, 44, 45].

In order to develop a fully formal exposition, specially when dealing with minors in Section 2.4, we consider that $\sigma(\Gamma) = \lambda(\Gamma) = 0$ if Γ is a trivial access structure. Clearly, trivial structures are matroid ports and, in addition, we consider them to be ideal and $\mathbb{K}$-vector space access structures for every finite field $\mathbb{K}$.

The connection between secret sharing and matroid theory is due to the fact that the joint entropies of a set of random variables define a polymatroid. Specifically, given the random variables defined by maps $(\pi_i)_{i\in Q}$, consider the function $h\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(X) = \alpha H(E_X)$, where α is a positive real number. Fujishige [22, 21] noticed that, from the basic

properties of the entropy function, the so-called *Shannon inequalities*, it follows that the pair (Q, h) is a polymatroid. This fact is central in our results.

Actually, a secret sharing scheme has been defined as a family of random variables, and hence it defines a polymatroid. Let Σ be a secret sharing scheme with access structure Γ on the set $P = Q - \{p_0\}$. Associated to Σ, we consider the polymatroid $\mathcal{S} = \mathcal{S}(\Sigma) = (Q, h)$, where $h(X) = H(E_X)/H(E_0)$. Clearly, $\mathcal{S}(\Sigma)$ is a Γ-polymatroid.

2.3 Ideal Secret Sharing Schemes and Matroid Ports

As a consequence of the results by Brickell and Davenport [13], the polymatroid $\mathcal{S}(\Sigma)$ is a matroid if Σ is an ideal secret sharing scheme. In particular all ideal access structures are matroid ports. An ideal secret sharing scheme Σ can be seen as a representation of the matroid $\mathcal{M} = (Q, h) = \mathcal{S}(\Sigma)$. The matroids of the form $\mathcal{S}(\Sigma)$ for some ideal secret sharing scheme Σ are called *secret sharing representable* or *ss-representable* for short. Seymour [40] presented the first example of a matroid that is not ss-representable, the Vamos matroid. Many more examples, being the non-Desargues matroid among them, were given by Matúš [33].

It is not difficult to check that a matroid is representable over a finite field $\mathbb{K}$ (see [36] for the definition of representable matroid) if and only if it is of the form $\mathcal{S}(\Sigma)$ for some $\mathbb{K}$-vector space secret sharing scheme Σ. Therefore, all representable matroids are ss-representable, and hence all ports of representable matroids are ideal access structures. We say that a matroid is *linearly representable* if it is represented by an ideal linear secret sharing scheme. All representable matroids are linearly representable, but there exist linearly representable matroids that are not representable, being the non-Pappus matroid an example [42]. The existence of ss-representable matroids that are not linearly representable is an open problem.

2.4 Minors and Duals

We recall some basic facts about dual access structures and dual matroids. The *dual* of the access structure Γ on the set P is defined as the access structure $\Gamma^* = \{A \subseteq P : P - A \notin \Gamma\}$. If $\mathcal{M} = (Q, r)$ is a matroid, the map $r^*\colon \mathcal{P}(Q) \to \mathbb{Z}$ 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 $\mathcal{M}$. Since $\Gamma_{p_0}(\mathcal{M}^*) = (\Gamma_{p_0}(\mathcal{M}))^*$, the dual of a matroid port is a matroid port. If Σ is a $\mathbb{K}$-linear secret sharing scheme with access structure Γ, then there exists a $\mathbb{K}$-linear scheme Σ^* with access structure Γ^* and complexity $\sigma(\Sigma^*) = \sigma(\Sigma)$ [20, 25]. This implies that $\lambda(\Gamma^*) = \lambda(\Gamma)$. Actually, Σ can be seen as a linear code, and the linear scheme Σ^* is the one constructed from the dual code. As a consequence, if a matroid is linearly representable, the same applies to the dual matroid. Nevertheless, it is not known whether the dual of an ss-representable matroid is ss-representable, and the relation between $\sigma(\Gamma)$ and $\sigma(\Gamma^*)$ is an open problem too.

Taking minors is another interesting operation on access structures, matroids, and polymatroids. Let Γ be an access structure on a set P and take a subset $Z \subseteq P$. We define the access structures $\Gamma \setminus Z$ and Γ/Z on the set $P - Z$ by $\Gamma \setminus Z = \{A \subseteq P - Z : A \in \Gamma\}$ and $\Gamma/Z = \{A \subseteq P - Z : A \cup Z \in \Gamma\}$. 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 of the form $(\Gamma \setminus Z_1)/Z_2$ for some disjoint subsets $Z_1, Z_2 \subseteq P$. In addition, $(\Gamma \setminus Z)^* = \Gamma^*/Z$ and $(\Gamma/Z)^* = \Gamma^* \setminus Z$.

We can consider as well *minors of matroids and polymatroids*. Let $\mathcal{S} = (Q, h)$ be a polymatroid. Given a subset $Z \subseteq Q$, 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 $h_{/Z}(X) = h(X \cup Z) - h(Z)$ for every $X \subseteq Q - Z$.

It is not difficult to prove that, if p_0 is an atomic point of $\mathcal{S}$ and and $\Gamma = \Gamma_{p_0}(\mathcal{S})$, then for every $Z \subseteq P$, the point p_0 is atomic in both minors $\mathcal{S} \setminus Z$ and $\mathcal{S}/Z$ and, moreover, $\Gamma \setminus Z = \Gamma_{p_0}(\mathcal{S} \setminus Z)$ and $\Gamma/Z = \Gamma_{p_0}(\mathcal{S}/Z)$. In addition, if $\mathcal{M} = (Q, r)$ is a matroid, then $\mathcal{M} \setminus Z$ and $\mathcal{M}/Z$ are matroids as well.

The two operations on access structures that are used to construct minors have a very natural interpretation in secret sharing. Suppose that the participants in $Z \subseteq P$ are removed from the scheme. If their shares are not revealed, only the subsets in $\Gamma \setminus Z$ are able to reconstruct the secret value, while the subsets that can recover the secret are exactly those in Γ/Z if the shares of the participants in Z are made public. Having this in mind, from any secret sharing scheme Σ for the access structure Γ, one can construct secret sharing schemes $\Sigma \setminus Z$ and Σ/Z for $\Gamma \setminus Z$ and Γ/Z, respectively, whose complexities are at most the complexity of Σ. Next proposition is a straightforward consequence of the previous arguments.

Proposition 2.1. *The following classes of access structures are closed by minors: the $\mathbb{K}$-vector space access structures, the ideal ones, and the matroid ports. In addition, if Γ' is a minor of Γ, then $\lambda(\Gamma') \leq \lambda(\Gamma)$ and $\sigma(\Gamma') \leq \sigma(\Gamma)$.*

3 Lower Bounds from Polymatroids

Most of the known lower bounds on the optimal complexity were obtained by information-theoretical arguments [9, 10, 15, 26]. Specifically, by using basic properties of the Shannon entropy function in combination with the requirements that must be satisfied by the random variables involved in a secret sharing scheme. Csirmaz [17] pointed out that all those results are based solely on the so-called *Shannon inequalities* on the joint entropies of a set of random variables, and hence they can be proved from the fact that every secret sharing scheme with access structure Γ defines a polymatroid $\mathcal{S}$ with $\Gamma = \Gamma_{p_0}(\mathcal{S})$. In order to simplify and clarify the discussion about the lower bounds on the optimal complexity that are obtained by this technique, we introduce here a new parameter, which we denote by $\kappa(\Gamma)$.

For a polymatroid $\mathcal{S} = (Q, h)$ and an atomic point $p_0 \in Q$, we define $\sigma_{p_0}(\mathcal{S}) = \max\{h(\{x\}) : x \in P\}$, where $P = Q - \{p_0\}$. Observe that $\sigma_{p_0}(\mathcal{S}) = \sigma(\Sigma)$ if $\mathcal{S}$ is the polymatroid associated to the secret sharing scheme Σ. For every access structure Γ, we consider the value

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) : \mathcal{S} \text{ is a } \Gamma\text{-polymatroid with } \Gamma = \Gamma_{p_0}(\mathcal{S})\}.$$

Clearly, $\kappa(\emptyset) = \kappa(\mathcal{P}(P)) = 0$ and $\kappa(\Gamma) \geq 1$ for every non-trivial access structure Γ. In addition, $\sigma_{p_0}(\mathcal{M}) \leq 1$ if $\mathcal{M}$ is a matroid and $\kappa(\Gamma) = 1$ if Γ ia a non-trivial matroid port.

The next result completes Proposition 2.1. Its proof is straightforward from the definition of κ and the discussion is Section 2.4.

Proposition 3.1. *If Γ' is a minor of the access structure Γ, then $\kappa(\Gamma') \leq \kappa(\Gamma)$.*

The lower bounds on the optimal complexity that can be obtained by using polymatroids (that is, by using Shannon inequalities) are based on the following proposition.

Proposition 3.2. *The optimal complexity of every access structure Γ is lower bounded by $\sigma(\Gamma) \geq \kappa(\Gamma)$.*

Proof. Let Σ be a secret sharing scheme with access structure Γ and let $\mathcal{S} = \mathcal{S}(\Sigma)$ be its associated polymatroid. Then $\sigma(\Sigma) = \sigma_{p_0}(\mathcal{S}) \geq \kappa(\Gamma)$. □

Therefore, lower bounds on $\sigma(\Gamma)$ can be found by deriving lower bounds on $\kappa(\Gamma)$ from combinatorial properties of the access structure. Of course, $\kappa(\Gamma)$ is the best lower bound that can be obtained by this technique. The best general lower bound that has been found by this method was given by Csirmaz [17], who presented an infinite family (Γ_n) of access structures such that $\kappa(\Gamma_n) \geq n/\log n$, where n is the number of participants. This is very far from the known general upper bounds, which are exponential in n.

Observe that $\kappa(\Gamma)$ deals only with the properties of the Γ-polymatroids. Every secret sharing scheme for Γ determines a Γ-polymatroid, but there exist Γ-polymatroids that are not associated to any secret sharing scheme for Γ. The Vamos matroid is an example of such a polymatroid, because its ports do not admit any ideal secret sharing scheme [40]. Because of that, $\kappa(\Gamma)$ may not be in general a tight lower bound for $\sigma(\Gamma)$. Another argument in this direction was given by Csirmaz [17], who realized that, for every access structure Γ on a set P with $|P| = n$, there exists a Γ-polymatroid $\mathcal{S} = (Q, h)$ such that $h(X) = n + (n-1) + \cdots + (n-(k-1))$ for every $X \subseteq P$ with $|X| = k$. The next result is a direct consequence of this fact.

Theorem 3.3. *If Γ is an access structure on a set of n participants, then $\kappa(\Gamma) \leq n$.*

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 whose complexity is linear in the number of participants. Therefore, it seems that the optimal complexity of an access structure will be in general much larger than $\kappa(\Gamma)$, the best lower bound that can be obtained by using polymatroids. Actually, some particular separation results between the parameters κ and σ have been presented very recently [3]. More details about them are given in Section 6. Stronger separation results are needed to prove the limitations of the polymatroid technique to find good asymptotic lower bounds for $\sigma(\Gamma)$ in the same way as the separation results between the parameters λ and σ [1, 6, 23] indicate the limits of the search of asymptotic upper bounds by constructing linear schemes.

Anyway, the polymatroid technique has proved to be very useful when studying some particular families of access structures. In some cases the obtained lower bounds are tight or, at least, close to the best known upper bounds.

As an example of the kind of results that are obtained by using polymatroids, we present the *independent sequence method*, which was introduced in [9] and was improved in [37]. Let Γ be an access structure on a set of participants P. Consider $A \subseteq P$ and an increasing sequence of subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$. 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 $X_i \subseteq A$ such that $B_i \cup X_i \in \Gamma$, while $B_m \notin \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$ if $i \geq 2$. The independent sequence method is based on Theorem 3.4. We notice that this result was not stated in [9, 37] in terms of polymatroids, but in terms of the entropy function.

Theorem 3.4 ([9, 37])**.** *Let Γ be an access structure on the set P and let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid. If there exists in Γ an independent sequence $(B_1, \ldots, B_m \,|\, A)$ with length m and size s, then $h(A) \geq m$ and consequently $\kappa(\Gamma) \geq m/s$.*

Since $\kappa(\Gamma) \leq 1$ if Γ is a matroid port, we obtain the following corollary of Theorem 3.4. The converse of this result will be proved in Section 4.

Corollary 3.5. *If an access structure admits an independent sequence with length m and size $s < m$, then it is not a matroid port.*

In the following we prove another positive result about the polymatroid technique. Namely, we prove in Theorem 3.9 that the bounds that are obtained by this technique for an access

structure apply also to its dual. Observe that, since $\lambda(\Gamma^*) = \lambda(\Gamma)$, this is also the case for the upper bounds that are derived from the constructions of linear schemes. The existence of a similar result for the parameter σ is still unknown.

There exist several inequivalent ways to define the dual of a polymatroid [46] and we have to choose the suitable one to prove our result. 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

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

Clearly, if $\mathcal{M} = (Q, r)$ is such that $r(\{x\}) = 1$ for every $x \in Q$, then the dual matroid of $\mathcal{M}$ coincides with the dual polymatroid. Then this definition generalizes the duality that is usually considered for matroids. We prove in the next lemma that $\mathcal{S}^*$ is actually a polymatroid, and we describe in Lemma 3.7 the relation between the dual of a Γ-polymatroid and the dual of the access structure Γ.

Lemma 3.6. *$\mathcal{S}^* = (Q, h^*)$ is a polymatroid.*

Proof. Obviously, $h^*(\emptyset) = 0$. Take a subset $X \subseteq Q$ and a point $y \notin X$. 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, consider two arbitrary subsets $X, Y \subseteq Q$. 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. □

Lemma 3.7. *Let Γ be a non-trivial access structure on $P = Q - \{p_0\}$ and let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid. Then $\mathcal{S}^* = (Q, h^*)$ is a Γ^*-polymatroid.*

Proof. Since Γ is non-trivial, $h(\{p_0\}) = 1$ and $h(P) = h(Q)$, and hence $h^*(\{p_0\}) = 1$. For every $X \subseteq P$,

$$h^*(X \cup \{p_0\}) = h(\{p_0\}) + \sum_{x \in X} h(\{x\}) - h(Q) + h(P - X).$$

If $X \in \Gamma^*$, then $P - X \notin \Gamma$ and $h(P - X) = h(Q - X) - 1$. In this case, $h^*(X \cup \{p_0\}) = h^*(X)$. Analogously, if $X \notin \Gamma^*$ then $h(P - X) = h(Q - X)$, and hence $h^*(X \cup \{p_0\}) = h^*(X) + 1$. □

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 satisfying this property will be said to be *normalized*. In addition, we need some technical results that are given in the next lemma, whose proof is an easy exercise.

Lemma 3.8. *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 $X \subseteq Q$.*
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 $x \in Q$.*

Theorem 3.9. *Let Γ be an access structure and let Γ^* be its dual. Then $\kappa(\Gamma^*) = \kappa(\Gamma)$.*

Proof. Clearly, $\kappa(\Gamma) = \kappa(\Gamma^*) = 0$ if Γ is a trivial access structure. Assume that Γ is non-trivial. Consider the sets of real numbers

$$\Omega(\Gamma) = \{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}$$

and

$$\widehat{\Omega}(\Gamma) = \{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a normalized } \Gamma\text{-polymatroid}\}.$$

If $\mathcal{S}$ is a Γ-polymatroid, then $\mathcal{S}^{**}$ is a normalized Γ-polymatroid with $\sigma(\mathcal{S}^{**}) \leq \sigma(\mathcal{S})$. 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 A New Result from an Old Theorem

Our main result, Theorem 4.4, is presented in this section. It consists of two new characterizations of matroid ports that have interesting consequences in secret sharing. Its proof is based on the forbidden minor characterization of matroid ports given by Seymour [39] in 1976, before the invention of secret sharing by Shamir [41] in 1979.

We begin by presenting Seymour's characterization. First, we define the access structures that are the forbidden minors of matroid ports. The set of participants of 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 $\{p_2, p_4\}$. At this point, we can state Seymour's result.

Theorem 4.1 (Seymour [39])**.** *An access structure is a matroid port if and only if it has no minor isomorphic to Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$, or Ψ_s with $s \geq 3$.*

We need to introduce two technical results that are used in the proof of Theorem 4.4. First, independent sequences have a good behavior with respect to minors, and second, all forbidden minors in Seymour's characterization admit an independent sequence with length $m = 3$ and size $s = 2$.

Lemma 4.2. *Let Γ' be a minor of an access structure Γ. If there exists in Γ' an independent sequence with length m and size s, then the same occurs for Γ.*

Proof. Consider disjoint subsets $Z_1, Z_2 \subseteq P$ such that $\Gamma' = (\Gamma \setminus Z_1)/Z_2$. Suppose that $(B_1, \ldots, B_m \,|\, A)$ is 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 4.3. *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 $s = 2$.*

Proof. We are going to consider independent sequences with length $m = 3$ and size $s = 2$ that will be denoted by $(B_1, B_2, B_3 \,|\, a_1, a_2)$, where $B_1 \subseteq B_2 \subseteq B_3 \subseteq P$ and $a_1, a_2 \in P$ are such that 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 in Γ. 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. □

We can now prove our main result. It provides new characterizations of matroid ports in terms of independent sequences and in terms of the parameter κ.

Theorem 4.4. *Let Γ be a non-trivial access structure. Then the following statements are equivalent.*

1. *Γ is a matroid port.*
2. *There does not exist in Γ any independent sequence with length m and size $s < m$.*
3. *There does not exist in Γ any independent sequence with length $m = 3$ and size $s = 2$.*
4. *$\kappa(\Gamma) = 1$.*
5. *$\kappa(\Gamma) < 3/2$.*

Proof. If Γ is a matroid port, then $\kappa(\Gamma) = 1$ and, by Corollary 3.5, there does not exist in Γ any independent sequence with length m and size $s < m$. In addition, by Theorem 3.4, there does not exist in Γ any independent sequence with length $m = 3$ and size $s = 2$ if $\kappa(\Gamma) < 3/2$. Finally, if Γ is not a matroid port, then there exists a minor Γ' of Γ that is isomorphic to one of the forbidden minors in Theorem 4.1. From Proposition 4.3, Γ' admits an independent sequence with length $m = 3$ and size $s = 2$ and, by Lemma 4.2, the same occurs with Γ. □

One of the applications of Theorem 4.4 to secret sharing is an interesting generalization of the important result by Brickell and Davenport [13], who proved that the access structure of every ideal secret sharing scheme is a matroid port.

Corollary 4.5. *Let Σ be a secret sharing scheme with complexity $\sigma(\Sigma) < 3/2$. Then the access structure of Σ is a matroid port.*

In particular, our result implies a gap in the values of $\kappa(\Gamma)$. Namely, there does not exist any access structure Γ with $1 < \kappa(\Gamma) < 3/2$. This gap provides a common explanation for a phenomenon that was separately observed in several particular families of access structures, in which the optimal complexity of every non-ideal access structure is at least $3/2$. Actually, since all matroid ports in those families are ideal access structures, the gap observed in the values of σ is a direct consequence of our result. Nevertheless, this gap does not hold in general. The existence of non-ideal matroid ports with $1 < \sigma(\Gamma) < 3/2$ has been proved recently [3].

5 On Non-Ideal Matroid Ports

Since there exist matroids that are not ss-representable, there are matroid ports that are not ideal. Very little is known about the optimal complexity of these access structures. We cannot find lower bounds by the techniques in Section 3 because $\kappa(\Gamma) = 1$ if Γ is a matroid port. We present here some upper bounds on the optimal complexity of the ports of the Vamos matroid and the non-Desargues matroid. They are obtained by using the decomposition technique introduced by Stinson in [45]. Specifically, we use the following proposition, which is a corollary of [45, Theorem 2.1].

Proposition 5.1. *Let Γ be an access structure on a set P of participants, and let $(\Gamma_1, \ldots, \Gamma_m)$ be a collection of substructures of Γ (that is, $\Gamma_i \subseteq \Gamma$) such that $\Gamma = \bigcup_{i=1}^{m} \Gamma_i$. For every $i = 1, \ldots, m$, consider the set $P_i \subseteq P$ of participants that appear in some minimal qualified subset of the substructure Γ_i, and, for every $x \in P$, consider $w(x) = |\{i : x \in P_i\}|$ and*

take $w = \max_{x \in P} w(x)$. *For every minimal qualified subset* $A \in \min \Gamma$, *consider* $\gamma(A) = |\{i : A \in \Gamma_i\}|$ *and take* $\gamma = \min_{A \in \min \Gamma} \gamma(A)$. *Assume that there exists a finite field* $\mathbb{K}$ *such that all substructures* Γ_i *are* $\mathbb{K}$*-vector space access structures. Then, there exists for the access structure* Γ *a* $\mathbb{K}$*-linear secret sharing scheme with set of secrets* $E_0 = \mathbb{K}^\gamma$ *whose complexity is equal to* w/γ.

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 [40], and hence, its ports are not ideal.

The *non-Desargues matroid* $\mathcal{N}$ is the matroid with rank 3 on a set with 10 points determined by a non-Desargues configuration on a projective plane. That is, take three different lines L_1, L_2, L_3 that meet in a point p and, on the line L_i, two different points $q_i, r_i \neq p_0$. Finally, consider the points s_1, s_2, and s_3, where s_k is the intersection of the lines $q_i q_j$ and $r_i r_j$ if $\{i, j, k\} = \{1, 2, 3\}$. If such a configuration has been taken on a projective plane over a field, the points s_1, s_2 and s_3 must be collinear by the Desargues' Theorem. The non-Desargues matroid is defined by this configuration but considering that the three points s_i are not collinear. That is, the ground set of $\mathcal{N}$ is $Q_2 = \{p, q_1, q_2, q_3, r_1, r_2, r_3, s_1, s_2, s_3\}$, 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 over any field [36]. Moreover, Matúš [33] proved that it is not ss-representable.

Let $\mathcal{B}$ be the family of bases of the Vamos matroid $\mathcal{V}$. On the same ground set $Q_1 = \{v_1, \ldots, v_8\}$ as the Vamos matroid, consider, for $i = 1, \ldots, 4$, the matroid $\mathcal{M}_i$ with family of bases $\mathcal{B}_i$, where

- $\mathcal{B}_1 = \mathcal{B} \cup \{\{v_1, v_2, v_3, v_4\}\}$,
- $\mathcal{B}_2 = \mathcal{B} \cup \{\{v_3, v_4, v_5, v_6\}\}$,
- $\mathcal{B}_3 = \mathcal{B} \cup \{\{v_3, v_4, v_7, v_8\}\}$, and
- $\mathcal{B}_4 = \mathcal{B} - \{\{v_1, v_2, v_7, v_8\}\}$.

Lemma 5.2. *Each one of the matroids* $\mathcal{M}_1, \ldots, \mathcal{M}_4$ *is representable over every large enough finite field.*

Proof. We prove first that, for every large enough finite field $\mathbb{K}$, there exists a matrix of the form

$$M_1 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & x_5 & x_6 & 0 & 0 \\ x_1 & x_2 & 0 & 0 & 0 & 0 & x_7 & x_8 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

that is $\mathbb{K}$-representation of $\mathcal{M}_1$. It is easy to check that, for each one of the four circuits of $\mathcal{M}_1$ with four points, the corresponding columns of M_1 are linearly dependent. In addition, for every basis $B \subseteq Q$ of $\mathcal{M}_1$, the determinant $\det(M_B)$ of the corresponding submatrix of M_1 is a nonzero polynomial over $\mathbb{K}$ on the variables $x_1, \ldots, x_8$. Therefore, if $\mathbb{K}$ is large enough, there exist a point in $\mathbb{K}^8$ that is not a zero of the polynomial

$$\prod_{B \in \mathcal{B}_1} \det(M_B).$$

By substituting the variables $x_1, \ldots, x_8$ by the coordinates of this point, we obtain a matrix M_1 that represents $\mathcal{M}_1$ over $\mathbb{K}$. A similar argument applies for the matroids $\mathcal{M}_2$ and $\mathcal{M}_4$ by considering, respectively, the matrices

$$M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & x_5 & x_6 & x_7 & x_8 \\ x_1 & x_2 & 0 & 0 & 1-x_5 & 1-x_6 & 0 & 0 \\ 1-x_1 & 1-x_2 & x_3 & x_4 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and

$$M_4 = \begin{pmatrix} x_1 & x_2 & 0 & 0 & 0 & 0 & x_7 & x_8 \\ 0 & 0 & x_3 & x_4 & 0 & 0 & x_7 & x_8 \\ 0 & 0 & 0 & 0 & x_5 & x_6 & x_7 & x_8 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Finally, observe that $\mathcal{M}_3$ is isomorphic to $\mathcal{M}_1$. □

Lemma 5.3. *For every $x \in Q_2$, the matroid $\mathcal{N} \setminus \{x\}$ is representable over every large enough finite field.*

Proof. If the finite field $\mathbb{K}$ has enough elements, it is possible to find 9 points in the projective plane over $\mathbb{K}$ that are in the configuration corresponding to the matroid $\mathcal{N} \setminus \{x\}$. □

Theorem 5.4. *If an access structure Γ is a port of the Vamos matroid or the non-Desargues matroid, then $\lambda(\Gamma) \leq 4/3$.*

Proof. Consider the access structures $\Gamma = \Gamma_{v_3}(\mathcal{V})$ and $\Gamma_i = \Gamma_{v_3}(\mathcal{M}_i)$, where $i = 1, \ldots, 4$. Then

- $\min \Gamma_1 = \min \Gamma - \{\{v_1, v_2, v_4\}\}$,
- $\min \Gamma_2 = \min \Gamma - \{\{v_4, v_5, v_6\}\}$,
- $\min \Gamma_3 = \min \Gamma - \{\{v_4, v_7, v_8\}\}$, and
- $\min \Gamma_4 = \min \Gamma - \{\{v_1, v_2, v_7, v_8\}\}$.

Since by Lemma 5.2 the matroids $\mathcal{M}_i$ are representable over every large enough finite field, there exists a finite field $\mathbb{K}$ such that all access structures Γ_i are $\mathbb{K}$-vector space access structures. By applying Proposition 5.1 to the collection $(\Gamma_1, \ldots, \Gamma_4)$, we obtain a $\mathbb{K}$-linear secret sharing scheme for Γ with complexity $w/\gamma = 4/3$. Every port $\Gamma_{v_i}(\mathcal{V})$ of the Vamos matroid is isomorphic to $\Gamma_{v_3}(\mathcal{V})$ or to $\Gamma_{v_1}(\mathcal{V})$. In addition, $\Gamma_{v_1}(\mathcal{V})$ is isomorphic to $(\Gamma_{v_3}(\mathcal{V}))^*$. Therefore, for every $v_i \in Q_1$, there exists a linear secret sharing scheme with access structure $\Gamma_{v_i}(\mathcal{V})$ and complexity equal to $4/3$.

Let $p_0 \in Q_2$ be an arbitrary point in the ground set of the non-Desargues matroid $\mathcal{N}$ and consider the access structure $\Gamma = \Gamma_{p_0}(\mathcal{N})$ on the set $P_2 = Q_2 - \{p_0\}$ of participants. By Lemma 5.3, there exists a finite field $\mathbb{K}$ such that the matroid $\mathcal{N} \setminus \{x\}$ is $\mathbb{K}$-representable for every $x \in P_2$, and hence $\Gamma \setminus \{x\}$ is a $\mathbb{K}$-vector space access structure. Therefore, we can apply Proposition 5.1 to the collection formed by the nine access structures $(\Gamma \setminus \{x\})_{x \in P_2}$. Clearly $w = 8$ and, since every minimal qualified subset of Γ has at most three participants, $\gamma = 6$. Therefore, a linear secret sharing scheme for Γ with complexity equal to $w/\gamma = 8/6 = 4/3$ is obtained. □

6 New Techniques Are Needed

The open problem that is studied in this paper is very far from being solved. There is a huge gap between the best known general lower and upper bounds on the optimal complexity $\sigma(\Gamma)$, and almost nothing is known about the asymptotic behavior, in relation to the number of participants, of this parameter. The main methods that have been using until now to derive those bounds have been discussed in this paper. Recall that they can be described in terms of the parameters κ and λ from the fact that the inequalities

$$\kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$$

hold for every access structure Γ. Lower bounds on $\kappa(\Gamma)$ can be obtained from combinatorial properties of Γ, while constructions of linear secret sharing schemes provide upper bounds for $\lambda(\Gamma)$.

Of course, better bounds on those parameters can be found, but it is clear that new techniques are needed in order to significatively advance in our knowledge about the open problem considered here. For instance, Beimel and Weinreb [6] presented and infinite family (Γ_n) of access structures for which $\sigma(\Gamma_n)$ is polynomial on the number of participants while $\lambda(\Gamma_n)$ is superpolynomial. Therefore, this separation result between the parameters σ and λ implies that new methods to construct efficient nonlinear schemes are needed.

On the other hand, Theorem 3.3 seems to indicate the limitations of the combinatorial method to obtain lower bounds on the optimal complexity. Nevertheless, no strong separation results between the parameters κ and σ are known. The first examples of access structures for which $\kappa(\Gamma) < \sigma(\Gamma)$ have been presented recently in [3], a paper that appeared during the preparation of this work. A slight improvement on the results in [3] is given in [35]. The results in those recent works, combined with the upper bounds in Section 5, can be summarized as follows. For the access structures $\Gamma_1 = \Gamma_{v_1}(\mathcal{V})$ and $\Gamma_3 = \Gamma_{v_3}(\mathcal{V})$, the two non-isomorphic ports of the Vamos matroid, the following inequalities are satisfied.

- $\kappa(\Gamma_1) = 1 < 21/19 \leq \sigma(\Gamma_1) \leq \lambda(\Gamma_1) \leq 4/3$.
- $\kappa(\Gamma_3) = 1 < 19/17 \leq \sigma(\Gamma_3) \leq \lambda(\Gamma_3) \leq 4/3$.
- $6/5 \leq \lambda(\Gamma_1) = \lambda(\Gamma_3) \leq 4/3$.

In addition to providing the first example of a separation between the parameters κ and σ, the ports of the Vamos matroid are as well the first known examples of access structures with $1 < \sigma(\Gamma) < 3/2$. Of course, the above lower bounds on $\sigma(\Gamma_i)$ have not been derived from lower bounds on $\kappa(\Gamma)$, which are obtained by using only the basic *Shannon inequalities* on the entropy. Nevertheless, there exist several inequalities for the entropies of a set of random variables that cannot be deduced from the basic ones. These are the so-called *non-Shannon information inequalities*. The first examples of such inequalities were given by Zhang and Yeung [47], and other examples have been presented subsequently in [19, 30, 34] and other works. The results in [3] are obtained by combining a non-Shannon inequality in [47] with results from [2]. By using other non-Shannon inequalities from [19], the bounds in [3] have been improved in [35]. Even though non-Shannon inequalities can provide better lower bounds on $\sigma(\Gamma)$, their limitations have been discussed very recently by Beimel and Orlov [4]. They proved that, from all known non-Shannon inequalities, only lower bounds on $\sigma(\Gamma)$ that are linear in the number of participants can be obtained. Therefore, these inequalities cannot improve our knowledge on the asymptotic behavior of $\sigma(\Gamma)$.

Acknowledgments

The authors thank Amos Beimel, Ronald Cramer, Bert Gerards, Robbert de Haan, František Matúš, Jessica Metcalf-Burton, 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 [39], and to Bert Gerards, who independently found the construction proving Theorem 3.3.

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. *Third Theory of Cryptography Conference, TCC 2006. Lecture Notes in Comput. Sci.* **3876** (2006) 482–501.

[3] A. Beimel, N. Livne, C. Padró. Matroids Can Be Far From Ideal Secret Sharing. *Fifth Theory of Cryptography Conference, TCC 2008, Lecture Notes in Comput. Sci.* **4948** (2008) 194–212.

[4] A. Beimel, I. Orlov. Secret Sharing and Non-Shannon Information Inequalities. *Sixth Theory of Cryptography Conference, TCC 2009. Lecture Notes in Comput. Sci.* **5444** (2009) 539–557.

[5] 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.

[6] A. Beimel, E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.* **34** (2005) 1196–1215.

[7] J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88. Lecture Notes in Comput. Sci.* **403** (1990) 27–35.

[8] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*. **48** (1979) 313–317.

[9] 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.

[10] 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** (1993) 148–167.

[11] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.

[12] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.

[13] E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.

[14] E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology* **5** (1992) 153–166.

[15] 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.

[16] T.M. Cover, J.A. Thomas. *Elements of Information Theory*, 2nd ed. Wiley, New York, 2006.

[17] L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.

[18] M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls. Improved constructions of secret sharing schemes by applying (λ, ω)-decompositions. *Inf. Process. Lett.* **99** (2006) 154–157.

[19] R. Dougherty, C. Freiling, K. Zeger. Six new non-Shannon information inequalities. In *IEEE International Symposium on Information Theory (ISIT)* (2006) 233–236.

[20] S. Fehr. Efficient Construction of the Dual Span Program. Manuscript.

[21] S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18.

[22] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* **39** (1978) 55–72.

[23] 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.

[24] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87* (1987) 99–102.

[25] W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95.

[26] W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286.

[27] E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.

[28] A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725.

[29] A. Lehman. Matroids and Ports. *Notices Amer. Math. Soc.* **12** (1965) 356–360.

[30] K. Makarychev, Y. Makarychev, A. Romashchenko, N. Vereshchagin. A new class of non-Shannon type inequalities for entropies. *Communications in Information and Systems* **2** (2002) 147–166.

[31] J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes Cryptogr.* **34** (2005) 17–34.

[32] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics* **154** (2006) 552–563.

[33] F. Matúš. Matroid representations by partitions. *Discrete Math.* **203** (1999) 169–194.

[34] F. Matúš. Infinitely many information inequalities. *IEEE International Symposium on Information Theory 2007*, pp. 41–44, 2007.

[35] J.R. Metcalf-Burton. Improved Upper Bounds for the Information Rates of the Secret Sharing Schemes Induced by the Vamos Matroid. Preprint, available at http://arxiv.org/abs/0809.3010 (2008).

[36] J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[37] C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604.

[38] 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.

[39] P.D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.

[40] P.D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B* **56** (1992) 69–73.

[41] A. Shamir. How to share a secret. *Commun. of the ACM* **22** (1979) 612–613.

[42] J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) 179–197.

[43] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.

[44] 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.

[45] D.R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory* **40** (1994) 118–125.

[46] D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.

[47] Z. Zhang, R.W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory* **44** (1998) 1440–1452.