Oriol Farràs

Secret sharing schemes for ports of matroids of rank 3

Kybernetika, Vol. 56 (2020), No. 5, 903–915

Persistent URL: http://dml.cz/dmlcz/148490

KYBERNETIKA — VOLUME *56* (2020), NUMBER 5, PAGES 903–915

SECRET SHARING SCHEMES FOR PORTS OF MATROIDS OF RANK 3

Oriol Farràs

A secret sharing scheme is ideal if the size of each share is equal to the size of the secret. Brickell and Davenport showed that the access structure of an ideal secret sharing scheme is determined by a matroid. Namely, the minimal authorized subsets of an ideal secret sharing scheme are in correspondence with the circuits of a matroid containing a fixed point. In this case, we say that the access structure is a matroid port. It is known that, for an access structure, being a matroid port is not a sufficient condition to admit an ideal secret sharing scheme.

In this work we present a linear secret sharing scheme construction for ports of matroids of rank 3 in which the size of each share is at most n times the size of the secret. Using the previously known secret sharing constructions, the size of each share was $O(n^2/\log n)$ the size of the secret.

Our construction is extended to ports of matroids of any rank $k \geq 2$, obtaining secret sharing schemes in which the size of each share is at most n^{k-2} times the size of the secret. This work is complemented by presenting lower bounds: There exist matroid ports that require $(\mathbb{F}_q, \ell)$-linear secret schemes with total information ratio $\Omega(2^{n/2}/\ell n^{3/4}\sqrt{\log q})$.

Keywords: secret sharing schemes, matroids, matroid ports

Classification: 94A60,94A62,05B35

1. INTRODUCTION

Secret sharing schemes are cryptographic mechanisms that are designed to protect a *secret value* by distributing it into *shares*. They were introduced by Blakley [11] and Shamir [36], and are used to prevent the disclosure or the loss of the secret value in many cryptographic applications. In this work we consider schemes that are *information-theoretically secure*, i. e. their security does not rely on any computational assumption. It is common to assume that the secret is held by a *dealer*, and each share is sent privately to a different *participant*. Then a subset of participants is *authorized* if their shares determine the secret value, and *forbidden* if their shares do not contain any information on the secret value. The *access structure* of a secret sharing scheme is the family of authorized subsets. In this work we just consider schemes that are *perfect*, which means that every subset of participants is either authorized or forbidden.

DOI: 10.14736/kyb-2020-5-0903

The efficiency of the schemes depends on the size of the shares that are generated. If the size of each share is equal to the size of the secret, then the scheme is *ideal*, and its access structure is called *ideal* as well. This is the optimal situation for perfect schemes. In order to study the efficiency of non-ideal schemes, we consider the *information ratio* of a scheme, which is a parameter that approximates the size of the largest share divided by the size of the secret. In general, for a given access structure, it is not known what the scheme with smallest information ratio is. By means of general constructions, we know that every access structure on a set of n participants admits a scheme with information ratio $O(2^{cn})$ for some $c < 1$ [1, 25]. On the other hand, Csirmaz proved that there exists a family of access structures that require schemes with information ratio $O(n/\log n)$ [14]. Currently, these are the best upper and lower bounds on the information ratio.

For some particular families of access structures, there exist specific techniques that allow a deeper insight to the efficiency problem. The study of these particular cases is also an interesting approach to infer more general results and to understand the nature of the secret sharing problem. This is the case of ideal access structures. Brickell and Davenport [13] proved that ideal access structures are determined by matroids. Namely, the minimal authorized subsets of ideal secret sharing schemes are in correspondence with the circuits of a matroid containing a fixed point. In this case, we say that the access structure is a *port* of that matroid, or that it is a *matroid port*. Conversely, ports of linearly representable matroids admit ideal linear secret sharing schemes. Despite the characterization of ideal access structures is still an open problem, these results were used in many works in order to construct ideal linear secret sharing schemes and, among particular families of access structures, to characterize the ideal ones (e. g. [6, 18, 26, 27]). Later, Martí-Farré and Padró showed that the information ratio of secret sharing schemes realizing access structures that are not matroid ports is at least $3/2$ [28].

The connection between ideal access structures and matroids was studied in several subsequent works. Matúš showed that matroids whose ports admit ideal secret sharing schemes are multiples of *entropic* polymatroids and admit *representations by partitions* [29, 30]. He studied the adhesivity of polymatroids, and showed that entropic polymatroids are *selfadhesive* [31], providing new tools for the characterization of ideal access structures. Simonis and Ashikhmin [37] constructed ideal linear schemes from matroids that do not admit linear representations but admit multilinear representations, and Beimel et al. [8] studied the power of these constructions. Matroids that admit linear or multilinear representations are representable by partitions [30], but there exist algebraic matroids that are not [9]. Also, there exist ports of matroids that are not representable by partitions that admit schemes in which the information ratio can be arbitrarily close to 1 [7].

Little is known about the efficiency of secret sharing schemes for matroids that are not representable by partitions. For the Vámos matroid and other matroids on a small number of points, it is possible to obtain bounds on the size of the shares by means of non-Shannon information inequalities [8, 17, 19, 30]. However, it is hard to obtain valuable bounds for matroids on a large number of points. There is a port of the Vámos matroid in which the information ratio is at least $561/491$ [19]. This is the current best lower bound on the information ratio for matroid ports, while there are no specific upper bounds.

The objective of this work was to find general results on the information ratio of ports of matroids. In particular, find secret sharing constructions that exploit the combinatorial properties of matroids. Matroids of rank 2 are linearly representable, and so ports of matroids of rank 2 admit ideal linear schemes. However, for $k > 2$, there exist matroids of rank k that do not admit ideal schemes [30]. Moreover, it is conjectured [32] that asymptotically almost every matroid has a minor that is the Vámos matroid, and so it is conjectured that almost every matroid port needs schemes with information ratio larger than 1.

In this work, we present a linear secret sharing construction for matroid ports that improves the general constructions when the rank of the matroid is small. First, we present a secret sharing scheme for ports of matroids of rank 3 that has information ratio at most n. It improves by a factor of $O(n/\log n)$ the information ratio of the previous best scheme for this family of access structures.

The construction for ports of matroids of rank 3 is extended recursively to ports of matroids of rank k for any $k > 2$. The resulting scheme has information ratio at most n^{k-2}. For $k \ll \ln n/\ln\ln n$, it improves the previously known constructions. It is the first general construction for matroid ports that takes benefit of its combinatorial properties.

We found that these results also have applications on the complexity of Boolean functions defined by ports of matroids. We show that ports of matroids of rank k admit monotone formulas of size $O(n^{k-1}\log n)$.

Since the secret sharing construction for matroids of rank $k > 2$ only uses the advantage gained on matroids of rank 2, it is very likely that the construction can be refined. Also, it is possible that the construction for matroids of rank 3 can be improved by taking into account that simple matroids of rank 3 can be embedded in projective planes, or by using non-linear schemes. However, the potential improvement of the linear constructions is limited. We show that there exist matroid ports that require $(\mathbb{F}_q, \ell)$-linear secret schemes with total information ratio $\Omega(2^{n/2}/\ell n^{3/4}\sqrt{\log q})$. The bound is obtained by counting the number of matroid ports and using a counting argument from [2].

Section 2 is dedicated to preliminaries on secret sharing schemes, and Section 3 is dedicated to matroid ports. Our constructions are presented in Section 4, and the lower bounds are presented in Section 5.

2. SECRET SHARING SCHEMES

In this section, we define secret sharing schemes and we present some results on homogeneous access structures. For an introduction to secret sharing, see [4, 34]. Given a discrete random vector $S = (S_i)_{i\in Q}$ and a set $X \subseteq Q$, the Shannon entropy of the random variable $S_X = (S_i)_{i\in X}$ is denoted by $H(S_X)$.

Definition 2.1. An *access structure* on a set P is a monotone increasing family of subsets $\Gamma \subseteq \mathcal{P}(P)$. The family of its minimal subsets is denoted by $\min\Gamma$.

Definition 2.2. Let P be a set and $Q = P \cup \{p_o\}$. A *secret sharing scheme* Σ on P is a collection $(S_i)_{i\in Q}$ of discrete random variables where $H(S_{p_0}) > 0$ and $H(S_{p_0} \mid S_P) = 0$.

The random variable S_{p_0} corresponds to the *secret value* that is distributed into *shares* among the participants in P according to the random variables $(S_i)_{i\in P}$.

Definition 2.3. Let $\Sigma = (S_i)_{i\in Q}$ be a secret sharing scheme. A set $X \subseteq P$ is *forbidden* for Σ if $H(S_{p_0} \mid S_X) = H(S_{p_0})$, while it is *authorized* for Σ if $H(S_{p_0} \mid S_X) = 0$. The *access structure* of Σ is the family of authorized subsets of Σ. A secret sharing scheme is *perfect* if every set of players is either forbidden or authorized.

Definition 2.4. Let $\mathbb{F}$ be a finite field and let ℓ be a positive integer. A secret sharing scheme $\Sigma = (S_i)_{i\in Q}$ is $(\mathbb{F}, \ell)$-*linear* if the random variables $(S_i)_{i\in Q}$ are given by surjective $\mathbb{F}$-linear maps $S_i : V \to E_i$, where V and E_i are $\mathbb{F}$-vector spaces, the probability distribution taken on V is the uniform one, and $E_0 = \mathbb{F}^\ell$. We say that Σ is ℓ-linear if it is $(\mathbb{F}, \ell)$-linear for some finite field $\mathbb{F}$.

The *information ratio* $\sigma(\Sigma)$ and the *total information ratio* $\sigma_{\mathrm{T}}(\Sigma)$ of a secret sharing $\Sigma = (S_i)_{i\in Q}$ are defined as

$$\sigma(\Sigma) = \frac{\max_{i\in P} H(S_i)}{H(S_{p_0})} \qquad \text{and} \qquad \sigma_{\mathrm{T}}(\Sigma) = \frac{\sum_{i\in P} H(S_i)}{H(S_{p_0})}.$$

This work is restricted to the study of secret sharing schemes whose access structure is *connected*. That is, that every participant is in at least one minimal authorized subset.

Definition 2.5. We say that a secret sharing scheme Σ is *ideal* if the information ratio of Σ is 1. In this case, we say that its access structure is *ideal* as well.

Next, we introduce some set operations that will be used in this work. For any $\Lambda \subseteq 2^P$, we define the *closure* of Λ as $\mathrm{cl}(\Lambda) = \{A \cup B : A \in \Lambda, B \subseteq P \setminus A\}$. Since access structures are monotone increasing, $\Gamma = \mathrm{cl}(\Gamma) = \mathrm{cl}(\min \Gamma)$ for every access structure Γ.

For every access structure Γ on P and $B \subseteq P$, we define the access structures $\Gamma\backslash B$ and Γ/B on the set $P \setminus B$ by

$$\Gamma\backslash B = \{A \subseteq P \setminus B : A \in \Gamma\} \quad \text{and} \quad \Gamma/B = \{A \subseteq P \setminus B : A \cup B \in \Gamma\}.$$

The operations $\setminus$ and $/$ are called *deletion* and *contraction*, respectively. Any access structure obtained by a sequence of deletions and contractions of subsets of P is a *minor* of Γ. Minors of access structures correspond to a natural scenario. Namely, if several participants of a secret sharing scheme leave the scheme or reveal their shares, then the new access structure is a minor of the original one. The *dual* of an access structure Γ on a set P is the access structure Γ^* on the same set defined by $\Gamma^* = \{A \subseteq P : P \setminus A \notin \Gamma\}$. The next result is an extension of a result in [22].

Theorem 2.6. (Padró [34]) If Σ is linear secret sharing scheme with access structure Γ, then Γ^* admits a linear secret sharing scheme of the same information ratio.

Every access structure Γ on $P = [n]$ defines a monotone Boolean formula $f : \{0,1\}^P \to \{0,1\}$ where $f(x) = 1$ if and only if the support of x is in Γ. Benaloh and Leichter [10]

presented a general method to construct secret sharing schemes in which, given a monotone formula of length L computing f, it creates a secret sharing scheme with total information ratio L. In particular, if Γ is an access structure whose minimal subsets are of size at most $k \leq n/2$, the DNF formula for Γ gives a secret sharing scheme with information ratio at most $\binom{n-1}{k-1}$. As a consequence of the results in [15], these access structures also admit schemes with information ratio at most $\frac{n^{k-1}}{\log n}(\frac{1}{k!} + o(1))$. If k is close $n/2$, then the schemes in [1, 25] have smaller information ratio. In this work, we denote the logarithmic function with base 2 and base e by log and ln, respectively.

3. MATROID PORTS

In this section we introduce the family of matroid ports and we present properties of matroids that are used later in this work.

A *matroid* is a pair $\mathcal{M} = (Q, r)$, where Q is a non-empty finite set and r is a mapping $r : 2^Q \to \mathbb{Z}$ satisfying the following properties for all $X, Y \subseteq Q$:

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

The set Q and the mapping r are called, respectively, the *ground set* and the *rank function* of the matroid $\mathcal{M}$. If a nonempty subset $A \subseteq Q$ satisfies that $r(A) > r(A \setminus \{p\})$ for all $p \in A$, then A is *independent*. If not, it is *dependent*. The maximal independent subsets are called *basis*, and the minimal dependent subsets are called *circuits*. A matroid $\mathcal{M} = (Q, r)$ is *connected* if for every $x, y \in Q$ there exists a circuit containing both x and y. A matroid is *paving* if its circuits are of size $r(\mathcal{M})$ or $r(\mathcal{M}) + 1$.

Given a matroid $\mathcal{M} = (Q, r)$ and a set $Z \subseteq Q$, we define the matroids $\mathcal{M}\backslash Z = (Q \setminus Z, r_{\backslash Z})$ and $\mathcal{M}/Z = (Q \setminus Z, r_{/Z})$ with $r_{\backslash Z}(A) = r(A)$ and $r_{/Z}(A) = r(A \cup Z) - r(Z)$. Every matroid that can be obtained from $\mathcal{M}$ by repeatedly applying these operations is called a *minor* of $\mathcal{M}$. For every minor $\mathcal{M}'$ of $\mathcal{M}$, there exist $Z_1, Z_2 \subseteq Q$ for which $\mathcal{M}' = (\mathcal{M}\backslash Z_1)/Z_2$. The dual of $\mathcal{M}$ is the matroid $\mathcal{M}^* = (Q, r^*)$ whose rank function $r^* : 2^Q \to \mathbb{Z}$ is defined by $r^*(X) = |X| - r(Q) + r(Q \setminus X)$.

Definition 3.1. Let Γ be an access structure on P and let $\mathcal{M} = (Q, r)$ be a matroid on $Q = P \cup \{p_0\}$. We say that $\min \Gamma$ is a *port* of $\mathcal{M}$ at p_0 if

$$\min \Gamma = \{A \subseteq P \,:\, A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\}.$$

If $\min \Gamma$ is a port of a matroid, then $\Gamma = \{A \subseteq P \,:\, r(A \cup \{p_0\}) = r(A)\}$. By an abuse of notation, in this case we also say that Γ *is a port of* $\mathcal{M}$, and that Γ is a *matroid port*. If Γ is a port of the matroid $\mathcal{M}$, and $B \subseteq P$, then $\Gamma\backslash B$ is a port of the matroid $\mathcal{M}\backslash B$ and Γ/B a port of the matroid $\mathcal{M}/B$.

The interest in matroid ports for secret sharing is due to the following result of Brickell and Davenport [13].

Theorem 3.2. (Brickell and Davenport [13]) Every ideal access structure is a matroid port.

If Γ is a connected access structure on P that is a matroid port, then there exists a unique connected matroid $\mathcal{M}$ on $Q = P \cup \{p_0\}$ with $\Gamma = \Gamma_{p_0}(\mathcal{M})$. This is a consequence of the following two facts. First, by [33, Proposition 4.1.2], a matroid $\mathcal{M}$ is connected if and only if one of its ports is connected, and in this case all the ports of $\mathcal{M}$ are connected. Second, a connected matroid is completely determined by the circuits that contain some given point [33, Theorem 4.3.3]. Therefore, there is a bijection between the family of connected access structures on P that are ports of matroids, and the family of connected matroids on Q. This bijection is used in the proof of Proposition 5.1.

The following lemma shows a connection between the ports of a matroid and the ports of its dual.

Lemma 3.3. If Γ is the p_0-port of a matroid $\mathcal{M}$, then Γ^* is the p_0-port of $\mathcal{M}^*$.

Matroid ports were characterized by Seymour [35]. The forbidden minors of the matroid ports are the access structures $\Phi, \widehat{\Phi}, \widehat{\Phi}^*$, and Ψ_s described below.

The access structures $\Phi, \widehat{\Phi}, \widehat{\Phi}^*$ are defined on $P = \{p_1, p_2, p_3, p_4\}$. The minimal subsets of Φ are $\{p_1, p_2\}$, $\{p_2, p_3\}$, $\{p_2, p_4\}$ and $\{p_3, p_4\}$, the minimal subsets of $\widehat{\Phi}$ are $\{p_1, p_2\}$, $\{p_2, p_3\}$ and $\{p_3, p_4\}$, and the minimal subsets of $\widehat{\Phi}^*$ are $\{p_1, p_3, p_4\}$, $\{p_2, p_3\}$ and $\{p_2, p_4\}$. For $s \geq 3$, Ψ_s is the access structure on $P = \{p_1, \ldots, p_s, p_{s+1}\}$ whose minimal subsets are $\{p_1, \ldots, p_s\}$ and $\{p_i, p_{s+1}\}$ for every $i = 1, \ldots, s$.

Theorem 3.4. (Seymour [35]) 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 for some $s \geq 3$.

Martí-Farré and Padró used the previous characterization of matroid ports to obtain a bound on the information ratio of secret sharing schemes realizing access structures that are not matroid ports [28].

Theorem 3.5. (Martí-Farré and Padró [28]) — The information ratio of secret sharing schemes realizing access structures that are not matroid ports is at least $3/2$.

The rest of this section is dedicated to some results on the information ratio of matroid ports. If Γ is a 2-homogeneous access structure that defines a connected graph, and this graph is not a complete multipartite graph, then the information ratio of the schemes realizing Γ is at least $3/2$ [12]. Namely, it was shown in [12] that if a connected graph is not a complete multipartite graph, then it has a minor isomorphic to Φ or $\widehat{\Phi}$. Therefore, they showed that if G is a connected graph that is not complete multipartite graph, then it is not a matroid port. On the other hand, we know that complete multipartite graphs admit ideal linear secret sharing schemes [13]. Therefore, we obtain the following result.

Corollary 3.6. Let Γ be an access structure whose minimal subsets are of size at most 2. Then it is a matroid port if and only if $\min \Gamma$ is the union of disjoint complete multipartite graphs and singletons. In this case, Γ admits an ideal $(\mathbb{F}, 1)$-linear secret sharing scheme for any finite field $\mathbb{F}$ with $|\mathbb{F}| \geq n$.

The characterization of the ideal access structures whose minimal authorized subsets are of size at most 3 is an open problem. Matúš [30], and Martí-Farré and Padró [27]

studied this family of access structures, and showed that there are matroid ports that do not admit ideal secret sharing schemes. The characterization of the ideal 3-homogeneous access structures is also an open problem, but for the case of sparse access structures it was solved in [26]. In both cases, for matroid ports that do not admit ideal schemes, there are no specific bounds on the information ratio.

4. SCHEMES FOR MATROID PORTS

This section is dedicated to the construction of secret sharing schemes for matroid ports. First, in Theorem 4.1, we present a construction for ports of matroids of rank 3, and then, in Theorem 4.3, we extend it to arbitrary matroids.

4.1. Ports of matroids of rank 3

Theorem 4.1. Let Γ be port of a matroid of rank 3. Then it admits a 1-linear secret sharing scheme whose information ratio is at most n.

In order to prove this theorem, we need to define some specific notation and a technical result. Let Γ be an access structure on P. For any $p \in P$, we define the access structure Γ_p on $P \setminus \{p\}$ as the one with

$$\min \Gamma_p = \{A \subseteq P \setminus \{p\} \,:\, A \cup \{p\} \in \min \Gamma\},$$

and the access structure $\tilde{\Gamma}_p = \Gamma \setminus \{p\}$. Observe that

$$\Gamma = \mathrm{cl}(\{A \cup \{p\} \,:\, A \in \min \Gamma_p \text{ for some } p \in P\}) \tag{1}$$

$$= \mathrm{cl}(\{A \cup \{p\} \,:\, A \in \min \Gamma_p \cup \min \tilde{\Gamma}_p \text{ for some } p \in P\}). \tag{2}$$

Lemma 4.2. Let $Q = P \cup \{p_0\}$, let $p \in P$, let $\mathcal{M} = (Q, r)$ be a matroid of rank $k > 1$, and let Γ be the p_0-port of $\mathcal{M}$. If Γ is connected and $\{p\} \notin \Gamma$, then there exists an access structure Γ' that is a port of a matroid of rank $k-1$ satisfying

$$\min \Gamma_p \subseteq \min \Gamma' \subseteq \min \Gamma_p \cup \min \tilde{\Gamma}_p.$$

P r o o f . Let $\mathcal{M}' = (Q \setminus \{p\}, r')$ be the matroid defined by $\mathcal{M}' = \mathcal{M}/\{p\}$, and let Γ' be the p_0-port of $\mathcal{M}'$. Since Γ is connected, then $r'(A) = r(A \cup \{p\}) - r(\{p\}) = r(A \cup \{p\}) - 1$ for every $A \subseteq Q \setminus \{p\}$. Hence,

$$r'(A) \leq r(A) \leq r'(A) + 1 \quad \text{for every } A \subseteq Q \setminus \{p\}. \tag{3}$$

First we prove that $\min \Gamma' \subseteq \min \Gamma_p \cup \min \tilde{\Gamma}_p$. Let $A \cup \{p_0\}$ be a circuit of $\mathcal{M}'$. By (3), $|A| \leq r(A \cup \{p_0\}) \leq |A| + 1$. If $r(A \cup \{p_0\}) = |A|$, then $A \cup \{p_0\}$ is dependent in $\mathcal{M}$. In this case, $A \cup \{p_0\}$ is a circuit of $\mathcal{M}$, because $r(A \cup \{p_0\} \setminus \{q\}) \geq r'(A \cup \{p_0\} \setminus \{q\}) = |A|$ for every $q \in A \cup \{p_0\}$. Therefore, $A \in \min \Gamma$, and $A \in \min \tilde{\Gamma}_p$ because $p \notin A$.

If $r(A \cup \{p_0\}) = |A| + 1$, then $A \cup \{p_0\}$ is independent in $\mathcal{M}$. The subset $A \cup \{p, p_0\}$ is dependent in $\mathcal{M}$ because $r(A \cup \{p, p_0\}) = r'(A \cup \{p_0\}) + 1 = |A| + 1$. Moreover, it is a circuit, because $r(A \cup \{p, p_0\} \setminus \{q\}) = r'(A \cup \{p_0\} \setminus \{q\}) + 1 = |A| + 1$ for every $q \in A \cup \{p_0\}$, and $r(A \cup \{p_0\}) = |A| + 1$. Hence, $A \cup \{p\} \in \min \Gamma$ and $A \in \min \Gamma_p$.

Finally, we prove that $\min\Gamma_p \subseteq \min\Gamma'$. Suppose that there exists $A \in \min\Gamma_p \setminus \min\Gamma'$. In this case, $A \cup \{p, p_0\}$ is a circuit of $\mathcal{M}$ and $A \cup \{p_0\}$ is not a circuit of $\mathcal{M}'$. Since $r'(A \cup \{p_0\}) = r(A \cup \{p, p_0\}) - 1 = |A|$, $A \cup \{p_0\}$ is a dependent set of $\mathcal{M}'$ that is not a circuit. Hence, there exists $q \in A \cup \{p_0\}$ for which $r'(A \cup \{p_0\} \setminus \{q\}) = |A| - 1$. But then $r(A \cup \{p, p_0\} \setminus \{q\}) = r'(A \cup \{p_0\} \setminus \{q\}) + 1 = |A|$, which implies that $A \cup \{p, p_0\} \setminus \{q\}$ is a dependent set of $\mathcal{M}$, a contradiction. □

Proof. [Proof of Theorem 4.1] Let $\mathcal{M}$ be the matroid associated to Γ. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \geq n$. Let $s \in \mathbb{F}$ be the secret to be shared. For each $p \in P$, we construct a secret sharing scheme Σ_p to share s. The resulting secret sharing scheme Σ consists on sharing independently s by means of every Σ_p.

If $\{p\} \in \Gamma$, just send s to p. In this case $\Gamma_p = \Gamma'_p = \tilde{\Gamma}_p = \{\emptyset\}$. If $\{p\} \notin \Gamma$, consider an access structure Γ'_p satisfying that it is a port of a matroid of rank 2, and

$$\min\Gamma_p \subseteq \min\Gamma'_p \subseteq \min\Gamma_p \cup \min\tilde{\Gamma}_p. \tag{4}$$

It exists by Lemma 4.2. By Corollary 3.6, Γ'_p admits an ideal linear secret sharing scheme Σ_p on $P \setminus \{p\}$. Send a random element $r \in \mathbb{F}$ to p and share $r + s$ with the scheme Σ_p among $P \setminus \{p\}$.

The resulting scheme Σ has information ratio at most n and has access structure

$$\mathrm{cl}(\{A \cup \{p\} \,:\, A \in \min\Gamma'_p \text{ for some } p \in P\}).$$

By (1), (2), and (4), the access structure of Σ is Γ. □

4.2. Ports of matroids of higher rank

In this section we extend the result on ports of matroids of rank 3 to ports of matroids of arbitrary rank. We also see that this result can be extended to the construction of monotone formulas for monotone Boolean functions.

Theorem 4.3. Let Γ be port of a matroid of rank k. Then it admits a 1-linear secret sharing scheme of information ratio n^{k-2}.

Proof. The result is proved by induction. For $k = 2$ it is satisfied by Corollary 3.6. Suppose that it is true for ports of matroid of rank less or equal than $k - 1$.

Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \geq n$. Let $s \in \mathbb{F}$ be the secret to be shared. For every $p \in P$, consider an access structure Γ'_p satisfying that it is a port of a matroid of rank $k-1$, and $\min\Gamma_p \subseteq \min\Gamma'_p \subseteq \min\Gamma_p \cup \min\tilde{\Gamma}_p$. It exists by Lemma 4.2. By the induction hypothesis, Γ'_p admits a linear secret sharing scheme Σ_p on $P \setminus \{p\}$ with information ratio n^{k-3}. Using the construction provided in the proof of Theorem 4.1, we construct a secret sharing scheme for Γ whose information ratio is at most $n \cdot n^{k-3} = n^{k-2}$. □

The scheme in Theorem 4.3 is only useful when k is small. The DNF construction from [10] has information ratio at most $\binom{n-1}{k-1}$. Observe that if $k = \frac{\ln n}{\ln\ln n}$, then

$$\binom{n}{k} < \frac{n^k e^k}{k^k} = \frac{n^k e^{\frac{\ln n}{\ln\ln n}}}{e^{\frac{\ln n}{\ln\ln n}\ln(\frac{\ln n}{\ln\ln n})}} = \frac{n^k n^{\frac{1}{\ln\ln n}}}{n^{1-\frac{\ln\ln\ln n}{\ln\ln n}}} = n^{k-1+o(1)},$$

and so $\binom{n-1}{k-1} = n^{k-2+o(1)}$. Therefore, our construction is useful if k is constant or $k \ll \frac{\ln n}{\ln \ln n}$.

Corollary 4.4. Let Γ be a port of a matroid of rank $n-k$ for some $k > 1$. Then it admits a 1-linear secret sharing of information ratio at most n^{k-1}.

P r o o f. Assume that Γ is the p_0-port of a matroid $\mathcal{M} = (Q, r)$. Since $\mathcal{M}$ has rank $n-k$, $\mathcal{M}^*$ has rank $n+1-(n-k) = k+1$. By Theorem 4.1, the p_0-port of $\mathcal{M}^*$ admits a linear secret sharing scheme with information ratio n^{k-1}. The result holds by Theorem 2.6 and Lemma 3.3. □

The recursive construction for secret sharing schemes can be also applied to monotone formulas for monotone Boolean functions in a straightforward manner. See [38] for an introduction to this area.

Definition 4.5. Let $\mathcal{M} = (Q, r)$ be a matroid. A monotone Boolean function $f : \{0,1\}^P \to \{0,1\}$ is a *p_0-port* of $\mathcal{M}$ if for every $A \subseteq P$,

$$A \text{ is a minterm of f if and only if } A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}.$$

Corollary 4.6. Let f be a monotone Boolean function that is a port of a matroid of rank k. Then there is a AND-OR formula for f of size $O(n^{k-1} \log n)$.

P r o o f. By Corollary 3.6, the minterms of monotone Boolean functions determined by matroids of rank 2 define mulipartite graphs. A multipartite graph on a set of n points can be described by an AND-OR formula of size $O(n \log n)$. The result holds by using the recursive argument in Theorem 4.3. □

5. LOWER BOUNDS FOR LINEAR SECRET SHARING SCHEMES

In this section we show a lower bound on the size of linear secret sharing schemes for matroid ports.

5.1. Number of matroid ports

First, we approximate the number of matroid ports in Proposition 5.1. This number is approximated by using the latest results on the number of matroids [3] and on the number or connected matroids [32].

For every $n > 1$, let $\mathrm{m}(n)$ be the number of matroids on a ground set on n elements, and let $\mathrm{mp}(n)$ be the number of matroid ports on a set of n participants.

Proposition 5.1.

$$\log \mathrm{mp}(n) = \Theta(2^n / n^{3/2}).$$

In order to prove this result we need some results on matroid theory that are presented below. As discussed in Section 3, the number of connected access structures on P that are matroid ports is equal to the number of labeled p_0-ports of connected matroids on Q. It is conjectured that almost every matroid is connected [32]. The best result in this direction is the following theorem.

Theorem 5.2. (Mayhew et al. [32]) The proportion of n-element matroids that are connected is asymptotically at least $1/2$.

In the following theorem, we present bounds on $\mathrm{m}(n)$. Both bounds were presented by Bansal et al. [3], and the lower bound combines the results of Knuth [24] and Graham and Sloane [20].

Theorem 5.3. (Bansal et al. [3])

$$\frac{1}{n}\binom{n}{\lfloor n/2\rfloor} \leq \log \mathrm{m}(n) \leq \frac{2}{n}\binom{n}{\lfloor n/2\rfloor}(1+o(1)).$$

Proof. [Proof of Proposition 5.1] Every matroid defines a matroid port, and so $\mathrm{mp}(n) \leq \mathrm{m}(n+1)$. Moreover, by Theorem 5.2, for a large enough n we have $\mathrm{mp}(n) > \frac{1}{2}\mathrm{m}(n+1)$. Now we use Theorem 5.3 to bound $\log \mathrm{mp}(n)$. The proof is completed by considering the approximation of the binomial coefficients $\binom{n}{\lfloor n/2\rfloor} = \Theta(2^n/\sqrt{n})$. □

Using the approximation of the number of matroid ports presented above, we have some information about the proportion of matroid ports among the family of access structures, and the total information ratio of linear schemes for matroid ports.

Let $a(n)$ be the number of access structures on a set of n elements for every $n > 1$. It is known that $a(n)$ is equal to the nth Dedekind number, and it satisfies $a(n) \sim \binom{n}{\lfloor n/2\rfloor}$ (see [23], for example). Hence,

$$\frac{\log a(n)}{\log \mathrm{mp}(n)} = \Theta(n).$$

5.2. A lower bound

Next, we provide an asymptotic lower bound on the total information ratio of linear secret sharing schemes for matroid ports. The proof of this bound follows the techniques used by Babai, Gál and Wigderson [2] for proving lower bounds on the size of span programs for general access structures.

Theorem 5.4. For every finite field $\mathbb{F}_q$ and integer $\ell > 0$ and for every large enough n, there exists a matroid port that requires $(\mathbb{F}_q, \ell)$-linear secret sharing schemes of total information ratio

$$\Omega\left(\frac{2^{n/2}}{n^{3/4}\ell\sqrt{\log q}}\right).$$

Proof. For any $t \geq n$, we define $L(n,t,q,\ell)$ as the family of access structures on $[n]$ that admit $(\mathbb{F}_q,\ell)$-linear secret sharing schemes with total information ratio at most t. We also define $A(\ell,t,q)$ as the family of $\ell(t+1) \times \ell t$ matrices over $\mathbb{F}_q$ in which the first ℓ rows are the first ℓ rows of the identity matrix.

We can assume that a $(\mathbb{F}_q,\ell)$-linear secret sharing scheme with total information ratio t' determines a $(t'+1)\ell \times k$ matrix M over $\mathbb{F}_q$, for some $k \leq t'\ell$, in which the first ℓ

rows are the first ℓ rows of the identity matrix (see [4] for more details). By adding zero rows and columns to M, we can assume that M is in $A(\ell, t, q)$ for any $t \geq t'$. Hence, $|L(n, t, q, \ell)| \leq |A(\ell, t, q)| = q^{\ell^2 t^2}$.

By Proposition 5.1, $\log \mathrm{mp}(n) = \Omega(2^n/n^{3/2})$. Hence, there exists some $c \in \mathbb{R}_+$ for which the parameter $t = c2^{n/2}/(n^{3/4}\ell\sqrt{\log q})$ satisfies $|L(n, t, q, \ell)| < \mathrm{mp}(n)$ for a large enough n. It implies that there exist matroid ports that require $(\mathbb{F}_q, \ell)$-linear secret sharing schemes with total information ratio greater than t. □

ACKNOWLEDGEMENT

I would like to thank Michael Bamiloshin, Amos Beimel, Aner Ben-Efraim and Carles Padró for helpful discussions regarding this work.
This work is supported by the Spanish Government through RTI2018-095094-B-C21 and by the Government of Catalonia through Grant 2017 SGR 705.

(Received April 6, 2019)

REFERENCES

[1] B. Applebaum, A. Beimel, O. Farràs, O. Nir, and N. Peter: Secret-Sharing Schemes for General and Uniform Access Structures. In: Advances in Cryptology – EUROCRYPT 2019, Lect. Notes Comput. Sci. *11478* (2019), Springer, pp. 441-471. DOI:10.1007/978-3-030-17659-4_15

[2] L. Babai, A. Gál, and A. Wigderson: Superpolynomial lower bounds for monotone span programs. Combinatorica *19* (1999), 301–319. DOI:10.1007/s004930050058

[3] N. Bansal, R. A. Pendavingh, and J. G. van der Pol: On the number of matroids. Combinatorica *49* (2013), 675–694. DOI:10.1007/s00493-014-3029-z

[4] A. Beimel: Secret-sharing schemes: A survey. In: IWCC 2011, Lect. Notes Comput. Sci. *6639* (2019), Springer, pp. 11–46. DOI:10.1007/978-3-642-20901-7_2

[5] A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin: Multi-linear secret-sharing schemes. In: TCC, Lect. Notes Comput. Sci. *8349* (2019), Springer, pp. 394–418. DOI:10.1007/978-3-642-20901-7_2

[6] A. Beimel and B. Chor: Universally ideal secret sharing schemes. IEEE Trans. Inform. Theory *40* (1994), 3, 786–794. DOI:10.1109/18.335890

[7] A. Beimel and N. Livne: On matroids and nonideal secret sharing. IEEE Trans. Inform. Theory *54* (2008), 6, 2626–2643. DOI:10.1109/tit.2008.921708

[8] A. Beimel, N. Livne, and C. Padró: Matroids can be far from ideal secret sharing. In: TCC 2008, Lect. Notes Comput. Sci. *4948* (2008), Springer, pp. 194–212. DOI:10.1007/978-3-540-78524-8_12

[9] A. Ben-Efraim: Secret-sharing matroids need not be algebraic. Discrete Math. *339* (2016), 8, 2136–2145. DOI:10.1016/j.disc.2016.02.012

[10] J. C. Benaloh and J. Leichter: Generalized secret sharing and monotone functions. In: CRYPTO'88, Lect. Notes Comput. Sci. *403* (1988), Springer, pp. 27–35. DOI:10.1007/0-387-34799-2_3

[11] G. R. Blakley: Safeguarding cryptographic keys. In: AFIPS Conference Proc. *48* (1979), pp. 313–317. DOI:10.1109/mark.1979.8817296

[12] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro: Graph decomposition and secret sharing schemes. J. of Cryptology *8* (1995), 1, 39–64. DOI:10.1007/bf00204801

[13] E. F. Brickell and D. M. Davenport: On the classification of ideal secret sharing schemes. J. of Cryptology *4* (1991), 73, 123–134. DOI:10.1007/bf00196772

[14] L. Csirmaz: The size of a share must be large. J. Cryptology *1* (1997), 4, 223–231. DOI:10.1007/s001459900029

[15] L. Csirmaz, P. Ligeti, and G. Tardos: Erdös–Pyber theorem for hypergraphs and secret sharing. Graphs Combinator. *31* (2015), 5, 1335–1346. DOI:10.1007/s00373-014-1448-7

[16] P. Erdös and L. Pyber: Covering a graph by complete bipartite graphs. Discrete Math. *170* (1997), 1–3, 249–251. DOI:10.1016/s0012-365x(96)00124-0

[17] O. Farràs, T. Kaced, S. Martín, and C. Padró: Improving the linear programming technique in the search for lower bounds in secret sharing. In: Advances in Cryptology — Eurocrypt 2018, volume 10820 Lecture Notes in Comput. Sci. *10820* (2018), Springer, pp. 597–621. DOI:10.1007/978-3-319-78381-9_22

[18] O. Farràs, J. Martí-Farré, and C. Padró: Ideal multipartite secret sharing schemes. J. Cryptology *25* (2012), 434–463. DOI:10.1007/s00145-011-9101-6

[19] E. Gürpinar and A. Romashchenko: How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma. In: 2019 IEEE International Symposium on Information Theory (ISIT), pp. 1377–1381.

[20] R. L. Graham and N. J. A. Sloane: Lower bounds for constant weight codes. IEEE Trans. Inform. Theory *26* (1980), 1, 37–43. DOI:10.1109/tit.1980.1056141

[21] A. W. Ingleton: Representation of matroids. In: Combinatorial Mathematics and its Applications, (D. J. A. Welsh, ed.), Academic Press, London 1971, pp. 149–167.

[22] W.-A. Jackson and K. M. Martin: Geometric secret sharing schemes and their duals. Codes Cryptography *4* (1994), 1, 83–95. DOI:10.1007/bf01388562

[23] A. D. Korshunov: Monotone Boolean functions. Russ. Math. Surv. *58* (2003), 5, 929–1001. DOI:10.1070/rm2003v058n05abeh000667

[24] D. E. Knuth: The asymptotic number of geometries. J. Combinator. Theory, Ser. A *16* (1974), 3, 398–400. DOI:10.1016/0097-3165(74)90063-6

[25] T. Liu and V. Vaikuntanathan: Breaking the circuit-size barrier in secret sharing. In: 50th STOC 2018, pp. 699–708.

[26] J. Martí-Farré and C. Padró: Secret sharing schemes on sparse homogeneous access structures with rank three. Electr. J. Comb. *11* (2004), 1. DOI:10.37236/1825

[27] J. Martí-Farré and C. Padró: Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. Des. Codes Cryptography *52* (2009), 1, 1–14. DOI:10.1007/s10623-008-9264-9

[28] J. Martí-Farré and C. Padró: On secret sharing schemes, matroids and polymatroids. J. Math. Cryptology *4* (2010), 2, 95–120. DOI:10.1007/s10623-008-9264-9

[29] F. Matúš: Probabilistic conditional independence structures and matroid theory: Background. Int. J. Gen. Syst. *22* (1994), 185–196. DOI:10.1080/03081079308935205

[30] F. Matúš: Matroid representations by partitions. Discrete Math. *203* (1999), 169–194. DOI:10.1016/s0012-365x(99)00004-7

[31] F. Matúš: Adhesivity of polymatroids. Discrete Math. *307* (2007), 2464–2477. DOI:10.1016/j.disc.2006.11.013

[32] D. Mayhew, M. Newman, D. Welsh, and G. Whittle: On the asymptotic proportion of connected matroids. Eur. J. Comb. *32* (2011), 6, 882–890. DOI:10.1016/j.ejc.2011.01.016

[33] J. G. Oxley: Matroid Theory. Second Edition. Oxford Graduate Texts in Mathematics *21*, The Clarendon Press, Oxford 2011.

[34] C. Padró: Lecture notes in secret sharing. Cryptology ePrint Archive, Report 2012/674 (2912).

[35] P. D. Seymour: A forbidden minor characterization of matroid ports. Quart. J. Math. Oxford Ser. *27* (1976), 407–413. DOI:10.1093/qmath/27.4.407

[36] A. Shamir: How to share a secret. Comm. ACM *22* (1979), 612–613. DOI:10.1145/359168.359176

[37] J. Simonis and A. Ashikhmin: Almost affine codes. Designs Codes Cryptogr. *14* (1998), 2, 179–197. DOI:10.1023/a:1008244215660

[38] I. Wegener: The Complexity of Boolean Functions. Wiley-Teubner, 1987.

Oriol Farràs, Universitat Rovira i Virgili, Tarragona, Catalonia. Spain.
e-mail: oriol.farras@urv.cat