Local Bounds for the Optimal Information Ratio of Secret Sharing Schemes

Oriol Farràs Jordi Ribes-González Sara Ricci

Department of Mathematics and Computer Science,
Universitat Rovira i Virgili,
Tarragona, Catalonia, Spain
{oriol.farras,jordi.ribes,sara.ricci}@urv.cat

May 22, 2018

Abstract

The information ratio of a secret sharing scheme Σ is the ratio between the length of the largest share and the length of the secret, and it is denoted by $\sigma(\Sigma)$. The optimal information ratio of an access structure Γ is the infimum of $\sigma(\Sigma)$ among all schemes Σ with access structure Γ, and it is denoted by $\sigma(\Gamma)$. The main result of this work is that for every two access structures Γ and Γ', $|\sigma(\Gamma) - \sigma(\Gamma')| \leq |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|$. We prove it constructively. Given any secret sharing scheme Σ for Γ, we present a method to construct a secret sharing scheme Σ' for Γ' that satisfies that $\sigma(\Sigma') \leq \sigma(\Sigma) + |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|$. As a consequence of this result, we see that *close* access structures admit secret sharing schemes with similar information ratio. We show that this property is also true for particular classes of secret sharing schemes and models of computation, like the family of linear secret sharing schemes, span programs, Boolean formulas and circuits.

In order to understand this property, we also study the limitations of the techniques for finding lower bounds on the information ratio and other complexity measures. We analyze the behavior of these bounds when we add or delete subsets from an access structure.

Key words. Cryptography, Secret sharing, Information ratio, Optimal information ratio, Monotone span program.

1 Introduction

Secret sharing is a cryptographic primitive that is used to protect a *secret value* by distributing it into *shares*. Secret sharing is used to prevent both the disclosure and the loss of secrets. In the typical scenario, each share is sent privately to a different *participant*. Then a subset of participants is *authorized* if their shares determine the

This work is supported by the European Union through H2020-ICT-2014-1-644024, by the Spanish Government through TIN2014-57364-C2-1-R, and by the Government of Catalonia through Grant 2014 SGR 537. Research was partially completed while the first author was visiting the Institute for Mathematical Sciences, National University of Singapore in 2016.

secret value, and *forbidden* if their shares do not contain any information on the secret value. The family of authorized subsets is monotone increasing, and it is called the *access structure* of the scheme. If every subset of participants is either authorized or forbidden, we say that the scheme is *perfect*. In this work we just consider perfect secret sharing schemes that are *information-theoretically secure*, that is, schemes whose security does not rely on any computational assumption.

Secret sharing schemes were introduced by Shamir [44] and Blakley [11] in 1979, and are used in many cryptographic applications such as secure multiparty computation, attribute-based encryption and distributed cryptography (see [3] for more details). These applications require the use of efficient secret sharing schemes. Namely, schemes with short shares, efficient generation of the shares and efficient reconstruction of the secret. The *information ratio* of a secret sharing scheme Σ is the ratio of the maximum length in bits of the shares to the length of the secret value, and we denote it by $\sigma(\Sigma)$. The information ratio is widely used as a measure of the efficiency of secret sharing schemes. *Linear* secret sharing schemes are of particular interest because they have homomorphic properties, and because the shares are generated by using linear mappings, simplifying the generation of shares and the reconstruction of the secret.

Ito, Saito and Nishizeki [29] presented a method to construct a secret sharing scheme for any monotone increasing family of subsets. Viewing access structures as monotone Boolean functions, Benaloh and Leichter [10] presented a method to construct a secret sharing scheme from any monotone Boolean formula. However, for almost all access structures, the information ratios of the schemes constructed using these and other general methods [10, 29, 32] are exponential on the number of participants. In order to understand the length of shares required to realize an access structure Γ, we define the *optimal information ratio* of Γ as the infimum of the information ratios of all the secret sharing schemes for Γ, and we denote it by $\sigma(\Gamma)$.

The computation of the optimal information ratio of access structures is difficult in general, and exact values are known only for certain families of access structures, like particular families of multipartite access structures (e.g. [12, 19, 20]), access structures with a small number of participants (e.g. [38, 23]), or access structures with small minimal sets (e.g. [16]). A common method to obtain bounds for this parameter is to define random variables associated to the shares and to the secret, and then apply the information inequalities of the Shannon entropy of these random variables. Csirmaz [15] used a connection between the Shannon entropy and polymatroids to develop a technique for finding lower bounds. Using this technique, it was possible to find access structures with n participants for which the optimal information ratio is $\Omega(n/\log(n))$. Currently, this is the best asymptotic lower bound on the information ratio.

Monotone span programs over a finite field $\mathbb{F}$ are equivalent to linear secret sharing schemes with secret in $\mathbb{F}$ [3, 32]. This connection was very useful to extend bounds on the complexity of monotone span programs to bounds on the information ratio of linear secret sharing schemes. Pitassi and Robere [39] showed that there are access structures that require linear secret sharing schemes with information ratio exponential in n. This result was obtained using the Razborov rank method [41].

For every perfect secret sharing scheme, the information ratio must be at least 1. The schemes that attain this bound are called *ideal*, and their access structures are also called *ideal*. Brickell and Davenport [13] showed that the access structure of ideal secret

sharing schemes determines a matroid. Conversely, entropic matroids determine ideal access structures, but little is known about the access structures associated to other families of matroids. The connection between ideal access structures and matroids is a powerful tool to characterize families of ideal access structures, e.g. [19], and it allows to transform secret sharing problems into combinatorial ones.

Beyond this connection, we lack of general criteria to determine if an access structure admits an efficient scheme. For instance, we lack of a criterion to determine if an access structure admits a secret sharing scheme with information ratio at most r, for some $r > 1$. Moreover, we do not know general properties of the family of access structures admitting efficient schemes. For other models of secret sharing, recent works provided interesting results on the characterization of the structures accepting efficient schemes [33, 45], but it is not clear how to extend them to the perfect model.

The main objective of this work is to find properties of the access structures that admit efficient secret sharing schemes. The specific question we consider is to know if access structures that are *close* admit secret sharing schemes with similar information ratios. Namely, the objective is to bound the difference between the optimal information ratios of access structures that differ on a small number of subsets. Answers to this question will help understand the limitations of secret sharing and the behavior of the optimal information ratio, seen as a function from the set of all the access structures with a certain number of participants to the real numbers.

Our main result is that $|\sigma(\Gamma)-\sigma(\Gamma')| \leq |\Gamma \cup \Gamma'|-|\Gamma \cap \Gamma'|$ for every two access structures Γ and Γ'. The proof of this result is constructive. From any secret sharing scheme Σ for Γ we can build a secret sharing scheme Σ' for Γ' that satisfies $\sigma(\Sigma') \leq \sigma(\Sigma)+|\Gamma \cup \Gamma'|-|\Gamma \cap \Gamma'|$. Moreover, if Σ is linear, then Σ' is linear too. The construction relies on a combinatorial result that allows the description of Γ' as a union and intersection of Γ with other access structures of a particular kind. Then, using an extension of the techniques of Benaloh and Leichter [10], we generate secret sharing schemes for the desired access structure.

An immediate consequence of this bound is that the access structures that are close to access structures with efficient secret sharing schemes also admit efficient schemes. Analogously, the access structures that are close to access structures requiring large shares also require large shares. This bound also has consequences on cryptographic schemes and protocols that use secret sharing. For instance, using the results in [17], we see that close Q_2 adversary structures admit secure multiparty computation protocols of similar complexity, in the passive adversary case. In the context of access control, we can build attribute-based encryption schemes [28] of similar complexity for similar policies.

Using the common terminology for functions between metric spaces, we can say that the optimal information ratio is a Lipschitz function with constant 1. Moreover, we prove that this constant is optimal, that is, σ is not Lipschitz for any constant smaller than 1.

By taking advantage of the combinatorial nature of our main result, we extend this bound to other models of computation. Therefore, we are able to bound the formula size, the circuit size, and the monotone span program size for monotone Boolean functions, obtaining analogous results. In order to understand the considered property, we also analyze the limitations of the techniques for finding lower bounds on the information ratio. In this setting, we study the nature of the bounds based on the

Shannon inequalities [15, 35], the Razborov rank method [40], the critical subfamilies method [4], and submodular formal complexity measures. We describe the behavior of each of these bounds when we add or delete subsets from an access structure.

The search for bounds on the information ratios of close access structures was motivated by a work by Beimel, Farràs and Mintz [5]. They presented a method that, given a secret sharing scheme Σ for an access structure Γ and an access structure Γ' with $\min\Gamma' \subseteq \min\Gamma$, provides a secret sharing scheme for Γ' (where $\min\Gamma$ stands for the family of minimal subsets of Γ). They showed that if Γ and Γ' are graph access structures and $\mathrm{dist}(\min\Gamma, \min\Gamma')$ is small, and Σ is efficient then the new scheme is also efficient. We also revise one of these techniques and we provide an alternative general combinatorial formulation of a result in [5] that can be further extended to other models of computation.

In Section 2 we define secret sharing, and in Section 3 we show preliminary results about secret sharing and access structures. Section 4 is dedicated to our main bound on the information ratio of secret sharing schemes. In Section 5 we analyze the asymptotic behavior of the optimal information ratio, and in Section 6 we present other secret sharing constructions used for bounding the optimal information ratio. In Sections 7 and 8 we analyze the existing techniques for finding lower bounds on the information ratio. In Section 9 we present results for formulas and circuits. Finally, we state some conclusions and open problems in Section 10.

2 Definition of Secret Sharing

This work is dedicated to unconditionally secure secret sharing schemes. In this section we define access structure, secret sharing scheme, and we present the complexity measures used in this work. The definition of secret sharing is taken from [3]. For an introduction to secret sharing, see [3, 37], for example.

Definition 2.1 (Access Structure)**.** Let P be a set. A collection $\Gamma \subseteq \mathcal{P}(P)$ is *monotone increasing* if $B \in \Gamma$ and $B \subseteq C \subseteq P$ implies $C \in \Gamma$. An *access structure* is a collection $\Gamma \subseteq \mathcal{P}(P)$ of non-empty subsets of P that is monotone increasing. The family of minimal subsets in Γ is denoted by $\min\Gamma$.

Definition 2.2 (Distribution Scheme)**.** Let $P = \{1, \ldots, n\}$ and let K be a finite set. A *distribution scheme* on P with domain of secrets K is a pair $\Sigma = (\Pi, \mu)$, where μ is a probability distribution on a finite set R, and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$. The set R is called *the set of random strings* and K_j is called the *domain of shares* of j.

For a distribution scheme (Π, μ) and for any $A \subseteq P$, we denote by $\Pi_A(s, r)$ the entries of $\Pi(s, r)$ indexed by elements in A. If $A = \{i\}$, we set $\Pi_i(s, r) = \Pi_A(s, r)$.

Definition 2.3 (Secret Sharing)**.** Let K be a finite set of secrets with $|K| \geq 2$. A distribution scheme (Π, μ) on P with domain of secrets K is a *secret-sharing scheme* realizing an access structure Γ if the following two requirements hold for every $A = \{i_1, \ldots, i_r\} \subseteq P$:

- If $A \in \Gamma$, then there exists a *reconstruction function* $\mathrm{Recon}_A : K_{i_1} \times \ldots \times K_{i_r} \to K$ such that for every $k \in K$,

$$\Pr[\, \mathrm{Recon}_A(\Pi_A(k, r)) = k \,] = 1. \tag{1}$$

- If $A \notin \Gamma$, then for every $a, b \in K$, and for every possible vector of shares $v = (s_j)_{j \in A}$,

$$\Pr[\,\Pi_A(a, r) = v] = \Pr[\,\Pi_A(b, r) = v]. \tag{2}$$

In a secret sharing scheme, we usually consider that there is an additional participant p_0 not in P called the *dealer*. The dealer distributes a secret $k \in K$ according to Σ by first sampling a random string $r \in R$ according to μ, computing a vector of *shares* $\Pi(k, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_j to party j. The subsets of participants in P satisfying condition (1) are called *authorized*, and the ones satisfying condition (2) are called *forbidden*. In this work we just consider *perfect* secret sharing schemes, that is, schemes in which every subset of participants is either authorized or forbidden.

Definition 2.4 (Linear Secret Sharing Scheme)**.** Let $\mathbb{F}$ be a finite field. A secret sharing scheme $\Sigma = (\Pi, \mu)$ is $(\mathbb{F}, \ell)$-*linear* if $K = \mathbb{F}^\ell$, the sets R, K_1, …, K_n are vector spaces over $\mathbb{F}$, μ is the uniform distribution on R, and Π is $\mathbb{F}$-linear.

For a secret sharing scheme Σ on P, the *information ratio* of Σ is defined as

$$\sigma(\Sigma) = \frac{\max_{1 \le j \le n} \log |K_j|}{\log |K|},$$

and the *total information ratio* of Σ is

$$\sigma^{\mathrm{T}}(\Sigma) = \frac{\sum_{1 \le j \le n} \log |K_j|}{\log |K|}.$$

We say that Σ is *ideal* if $\sigma(\Sigma) = 1$. In this case, we say that its access structure is *ideal* as well.

For an access structure Γ, we define the *optimal information ratio* $\sigma(\Gamma)$ as the infimum of the information ratio of secret sharing schemes for Γ. Also, we define the *optimal total information ratio* $\sigma^{\mathrm{T}}(\Gamma)$ as the infimum of the total information ratio of the secret sharing schemes for Γ. Analogously, for every power of a prime q we define $\lambda_{q,\ell}(\Gamma)$ and $\lambda^{\mathrm{T}}_{q,\ell}(\Gamma)$ as the infimum of the information ratios and total information ratios of the $(\mathbb{F}_q, \ell)$-linear secret sharing schemes for Γ, respectively. In cases in which the finite field and the domain of secrets are not relevant, we use $\lambda(\Gamma)$ and $\lambda^{\mathrm{T}}(\Gamma)$, the infimum of the information ratios and total information ratios of the linear secret sharing schemes for Γ.

If a participant $i \in P$ does not receive any share from the dealer in a secret sharing scheme, we set $K_i = \{\perp\}$. In this case, we say that i is *not relevant* in its access structure because i is not in any subset of $\min \Gamma$.

3 Preliminaries

First, we introduce some notation on access structures and we recall some of their properties. We use some definitions that are common in extremal combinatorics. See [27] for more details.

Let P be a set. We define the *distance* between $\mathcal{B}, \mathcal{B}' \subseteq \mathcal{P}(P)$ as

$$\operatorname{dist}(\mathcal{B}, \mathcal{B}') = |\mathcal{B} \cup \mathcal{B}'| - |\mathcal{B} \cap \mathcal{B}'|,$$

which is the size of the symmetric difference of the two sets. All through this paper, we measure the closeness between families of subsets by this distance. Observe that $\mathrm{dist}(\mathcal{B}, \mathcal{B}') = |\mathcal{B} \setminus \mathcal{B}'| + |\mathcal{B}' \setminus \mathcal{B}|$.

A family of subsets $\mathcal{B} \subseteq \mathcal{P}(P)$ is an *antichain* if $A \not\subseteq B$ for every $A, B \in \mathcal{B}$. For any $\mathcal{B} \subseteq \mathcal{P}(P)$ we define $\min \mathcal{B}$ and $\max \mathcal{B}$ as the families of minimal and maximal subsets in $\mathcal{B}$, respectively. Both $\min \mathcal{B}$ and $\max \mathcal{B}$ are antichains. We define the *complementary* of $\mathcal{B}$ as $\mathcal{B}^c = \mathcal{P}(P) \setminus \mathcal{B}$. The *degree* of $i \in P$ in $\mathcal{B}$, denoted by $\deg_i \mathcal{B}$, is defined as the number of subsets in $\mathcal{B}$ containing i. For every set $A \subseteq P$, we define the *closure* of a set A as $\mathrm{cl}(A) = \{B \subseteq P : A \subseteq B\}$. We also define the *closure* of $\mathcal{B}$ as $\mathrm{cl}(\mathcal{B}) = \bigcup_{A \in \mathcal{B}} \mathrm{cl}(A)$. The closure of any family of subsets is monotone increasing, and so it is an access structure. A family of subsets $\mathcal{B} \subseteq \mathcal{P}(P)$ is an access structure if and only if $\mathrm{cl}(\mathcal{B}) = \mathcal{B}$. If Γ is an access structure, then $\mathrm{cl}(\min \Gamma) = \Gamma$ and Γ^c is monotone decreasing.

3.1 Some Families of Ideal Access Structures

Now we define three parametrized families of access structures. As we show below, these access structures admit short formulas and ideal secret sharing schemes. For any nonempty set $A \subseteq P$, we define the access structures

$$F_A = \{B \subseteq P : B \not\subseteq A\}, \quad S_A = \{B \subseteq P : A \subsetneq B\}, \quad T_A = \mathrm{cl}(A).$$

The access structure T_A is the smallest access structure that contains A, and it is usually called the *trivial access structure* for A. The access structure S_A is T_A minus $\{A\}$, and $\min S_A = \{A \cup \{p\} : p \in P \setminus A\}$ is the *sunflower* of A [27]. The access structure F_A is the biggest access structure not containing A, and it has just one maximal forbidden subset, that is A. Its minimal access structure is $\min F_A = \{\{i\} : i \notin A\}$.

Now we present secret sharing schemes for the families of access structures F_A, S_A and T_A introduced above. These secret sharing schemes are ideal, and they are valid for any finite set of secrets K with $|K| \geq 2$. Moreover, if $K = \mathbb{F}^\ell$ for some finite field $\mathbb{F}$, then we show that these access structures also admit ideal (K, ℓ)-linear secret sharing schemes.

Let $K = \{a_0, \ldots, a_{m-1}\}$ be a set of size $m \geq 2$. For the constructions we present below, we assume that K is a group. In the case that K is not a group, our constructions will be defined over $\mathbb{Z}_m$ by using a bijection between K and $\mathbb{Z}_m$. Without loss of generality, let $P = \{1, \ldots, n\}$ and $A = \{1, \ldots, t\}$ for some $t \leq n$.

- F_A: Since $\min F_A = \{\{i\} : i \notin A\}$, the participants in A are not relevant, and so we just need to define the shares of the participants in $P \setminus A$. Let $K_j = \{\perp\}$ for $j \in A$ and $K_j = K$ for $j \in P \setminus A$. In this case there is no need for randomness. A secret sharing scheme for F_A is defined by the mapping Π with $\Pi_j(k) = k$ for $j \in P \setminus A$.

- S_A: For $A \subsetneq P$, consider $K_j = K$ for $j = 1, \ldots, n$, and μ the uniform distribution on $R = K^t$. A secret sharing scheme for S_A is defined by the mapping Π with $\Pi_j(k, r) = r_j$ for $1 \leq j \leq t$ and $\Pi_j(k, r) = k - \sum_{i=1}^{t} r_i$ for $t + 1 \leq j \leq n$. Observe that adapting this scheme we can construct an ideal secret sharing for any access structure Γ with $\min \Gamma \subseteq \min S_A$. For $A = P$, we have $S_P = F_P$.

- T_A: Since $\min T_A = \{A\}$, we just need to define the shares of the participants in A. Consider $K_j = K$ for $j \in A$, $K_j = \{\perp\}$ for $j \in P \setminus A$, and μ the uniform

distribution on $R = K^{t-1}$. A secret sharing scheme for T_A is defined by the mapping Π with $\Pi_j(k, r) = r_j$ for $1 \leq j < t$ and $\Pi_t(k, r) = k - \sum_{i=1}^{t-1} r_i$.

Given a secret sharing scheme Σ on P and $A \subseteq P$, we define $\Sigma|_A$ as the secret sharing scheme on P in which only the participants in A receive the shares from Σ. The access structure of $\Sigma|_A$ on P is $\Gamma|_A = \{B \subseteq P : B \cap A \in \Gamma\}$, and $\min(\Gamma|_A) = \min \Gamma \cap \mathcal{P}(A)$.

3.2 ANDs and ORs of Secret Sharing Schemes

For any access structure Γ on P, we can define the Boolean function $f : \mathcal{P}(P) \to \{0, 1\}$ satisfying $f(A) = 1$ if and only if $A \in \Gamma$. This function is monotone increasing because $f(A) \leq f(B)$ for every $A \subseteq B$.

Benaloh and Leichter [10] presented a recursive algorithm that, given a monotone Boolean formula computing the function f associated to Γ, creates a secret sharing scheme realizing Γ. The domain of secrets in this construction is $\mathbb{Z}_m$, and the scheme is obtained by translating the AND and OR logic operations into secret sharing operations [10]. Roughly speaking, the OR of two schemes Σ_1 and Σ_2 is a scheme in which the same secret is shared independently by using Σ_1 and Σ_2. In the case of the AND operation, the secret s is split into r and $s + r$, where r is a random value in $\mathbb{Z}_m$, and then the r is shared by means of Σ_1 and $r + s$ is shared independently by means of Σ_2.

Here we consider an extension of the secret sharing operations defined by Benaloh and Leichter [10] that is valid for arbitrary secret sharing schemes. We define AND and OR operations between any secret sharing schemes with the same domain of secrets. Since we did not find a precise description of these extended operations in the literature, we prefer to define them rigorously. Notice that the properties of these operations are crucial for our results in σ and λ. The proof of Lemma 3.1 has the same spirit as the one in [10], but we show it for the sake of completeness.

Let $\Sigma_1 = (\Pi^1, \mu^1)$ and $\Sigma_2 = (\Pi^2, \mu^2)$ be two secret sharing schemes on a set of participants P that have the same domain of secrets K, satisfying that μ^1 and μ^2 are independent probability distributions on some finite sets R^1 and R^2, and let $\Pi^i : K \times R^i \to K_1^i \times \ldots \times K_n^i$ for $i = 1, 2$.

We define the *OR* of Σ_1 and Σ_2 as the secret sharing scheme $\Sigma_1 \vee \Sigma_2 = (\Pi, \mu)$ where $\Pi : K \times R \to K_1 \times \ldots \times K_n$ is the mapping with $R = R^1 \times R^2$, $K_i = K_i^1 \times K_i^2$ for $i = 1, \ldots, n$, and

$$\Pi_i(k, r_1, r_2) = (\Pi_i^1(k, r_1), \Pi_i^2(k, r_2))$$

for $i = 1, \ldots, n$; and μ is the product of μ^1 and μ^2.

To define the *AND* of Σ_1 and Σ_2, we need to introduce an additional scheme. Let $\Sigma_3 = (\Pi^3, \mu^3)$ be the ideal secret sharing scheme on $P' = \{1, 2\}$ with access structure $\Gamma = T_{P'} = \{P'\}$ described above, with domain of secrets K, set of random strings $R^3 = K$, and uniform probability distribution μ^3 on K. The *AND* of Σ_1 and Σ_2 is the secret sharing scheme $\Sigma_1 \wedge \Sigma_2 = (\Pi, \mu)$ where $\Pi : K \times R \to K_1 \times \ldots \times K_n$ is the mapping with $R = R^1 \times R^2 \times R^3$, $K_i = K_i^1 \times K_i^2$ for $i = 1, \ldots, n$, and

$$\Pi_i(k, r_1, r_2, r_3) = (\Pi_i^1(\Pi_1^3(k, r_3), r_1), \Pi_i^2(\Pi_2^3(k, r_3), r_2))$$

for $i = 1, \ldots, n$; and μ is the product of μ^1, μ^2 and μ^3.

Lemma 3.1. *Let Σ_1 and Σ_2 be two secret sharing schemes on the same set of participants and with the same set of secrets. Let Γ_1 and Γ_2 be their access structures, respectively. Then the access structures of the schemes $\Sigma_1 \wedge \Sigma_2$ and $\Sigma_1 \vee \Sigma_2$ are $\Gamma_1 \cap \Gamma_2$ and $\Gamma_1 \cup \Gamma_2$, respectively.*

Proof. Let Recon_A^1, Recon_A^2 and Recon_A^3 be the reconstruction functions of the schemes Σ_1, Σ_2 and Σ_3, respectively. First we prove that the access structure of $\Sigma_1 \vee \Sigma_2$ is $\Gamma_1 \cup \Gamma_2$. For a subset $A \in \Gamma_1$, we define Recon_A as Recon_A^1 over the elements from Σ_1. If $A \notin \Gamma_1$ but $A \in \Gamma_2$, we define Recon_A as Recon_A^2 over the elements from Σ_2. Then subsets in $\Gamma_1 \cup \Gamma_2$ can recover the secret. If $A \notin \Gamma_1$ and $A \notin \Gamma_2$, then A is forbidden in $\Sigma_1 \vee \Sigma_2$, because for every $a, b \in K$ and for every possible vector of shares $(s_j)_{j\in A} = (s_j^1, s_j^2)_{j\in A}$,

$$\begin{aligned}\Pr[\,\Pi_A(a, r_1, r_2) = (s_j)_{j\in A}\,] &= \Pr[\,\Pi_A^1(a, r_1) = (s_j^1)_{j\in A}\,] \cdot \Pr[\,\Pi_A^2(a, r_2) = (s_j^2)_{j\in A}\,] \\ &= \Pr[\,\Pi_A^1(b, r_1) = (s_j^1)_{j\in A}\,] \cdot \Pr[\,\Pi_A^2(b, r_2) = (s_j^2)_{j\in A}\,] \\ &= \Pr[\,\Pi_A(b, r) = (s_j)_{j\in A}\,].\end{aligned}$$

Now we prove that the access structure of $\Sigma_1 \wedge \Sigma_2$ is $\Gamma_1 \cap \Gamma_2$. For a subset $A \in \Gamma_1 \cap \Gamma_2$, we can reconstruct the secret by applying Recon_A^3 to the outputs of Recon_A^1 and Recon_A^2, and so A is authorized. If A is neither in Γ_1 nor Γ_2, then A is forbidden in $\Sigma_1 \wedge \Sigma_2$. Now suppose that A is in Γ_1 but not in Γ_2. For every $a, b \in K$ and for every possible vector of shares $(s_j)_{j\in A} = (s_j^1, s_j^2)_{j\in A}$,

$$\begin{aligned}&\Pr[\,\Pi_A(a, r_1, r_2, r_3) = (s_j^1, s_j^2)_{j\in A}\,] = \\ &= \Pr[\Pi_A^1(\Pi_1^3(a, r_3), r_1) = (s_j^1)_{j\in A}\,] \cdot \Pr[\,\Pi_A^2(\Pi_2^3(a, r_3), r_2) = (s_j^2)_{j\in A}\,] \\ &= \Pr[\Pi_A^1(r_3, r_1) = (s_j^1)_{j\in A}\,] \cdot \Pr[\,\Pi_A^2(a - r_3, r_2) = (s_j^2)_{j\in A}\,] \\ &= \Pr[\Pi_A^1(\Pi_1^3(b, r_3), r_1) = (s_j^1)_{j\in A}\,] \cdot \Pr[\,\Pi_A^2(\Pi_2^3(b, r_3), r_2) = (s_j^2)_{j\in A}\,] \\ &= \Pr[\,\Pi_A(b, r_1, r_2, r_3) = (s_j^1, s_j^2)_{j\in A}\,],\end{aligned}$$

and so A is forbidden. For $A \in \Gamma_2 \setminus \Gamma_1$ the proof is analogous, and for $A \notin \Gamma_2 \cap \Gamma_1$ the proof is immediate. □

In both cases, each participant receives a share from Σ_1 and a share from Σ_2, so $\sigma(\Sigma_1 \wedge \Sigma_2) = \sigma(\Sigma_1 \vee \Sigma_2) \leq \sigma(\Sigma_1) + \sigma(\Sigma_2)$, and $\sigma^{\mathrm{T}}(\Sigma_1 \wedge \Sigma_2) = \sigma^{\mathrm{T}}(\Sigma_1 \vee \Sigma_2) = \sigma^{\mathrm{T}}(\Sigma_1) + \sigma^{\mathrm{T}}(\Sigma_2)$. Therefore, for every two access structures Γ_1 and Γ_2, $\sigma(\Gamma_1 \cup \Gamma_2)$ and $\sigma(\Gamma_1 \cap \Gamma_2)$ are smaller than or equal to $\sigma(\Gamma_1) + \sigma(\Gamma_2)$. Both operations preserve linearity. That is, if Σ_1 and Σ_2 are $(\mathbb{F}, \ell)$-linear secret sharing scheme for a finite field $\mathbb{F}$ and $\ell > 0$, then $\Sigma_1 \vee \Sigma_2$ and $\Sigma_1 \wedge \Sigma_2$ are also $(\mathbb{F}, \ell)$-linear.

Now we present two well-known constructions for every access structure Γ [29]. Since $\Gamma = \bigcup_{A\in \min \Gamma} T_A$ and each T_A admits an ideal secret sharing scheme on A, using the OR operation we can construct a scheme Σ for Γ with $\sigma(\Sigma) = \deg(\min \Gamma) \leq |\min \Gamma|$. Since $\Gamma = \bigcap_{A\in \max \Gamma^c} F_A$ and each F_A admits an ideal secret sharing scheme on $P \setminus A$, we can construct a secret sharing scheme Σ with $\sigma(\Sigma) \leq |\max \Gamma^c|$.

Remark 3.2. All the results in this section can be adapted to other kinds of secret sharing schemes: perfect secret sharing schemes defined by discrete random variables (see [3]), statistical secret sharing schemes (see [3]), or computational secret sharing schemes (see [9]). The AND and OR operations can also be defined in these models, but in some cases they require additional restrictions.

4 The Main Result

We dedicate this section to the proof and the analysis of the following theorem, which is the main result of this work.

Theorem 4.1. *Let Γ, Γ' be two access structures on a set P. Then*

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq \operatorname{dist}(\Gamma, \Gamma').$$

The approach we follow to give an upper bound for $|\sigma(\Gamma) - \sigma(\Gamma')|$ for any two access structures Γ and Γ' is the following. Given a secret sharing scheme Σ for Γ, we show a way to construct a secret sharing scheme Σ' for Γ' with $\sigma(\Sigma') \leq \sigma(\Sigma) + \operatorname{dist}(\Gamma, \Gamma')$. In order to do so, we find a description of Γ' in terms of Γ and some ideal access structures, which is presented in Lemma 4.2. Then, according to this description, we can construct Σ' reusing Σ in a special form, according to the description of Γ'. This theorem is a direct consequence of Proposition 4.3.

The motivation for reusing Σ in the construction of Σ' is that, if Γ and Γ' are close, Σ already satisfies most of the reconstruction and privacy requirements we need for Σ'. Our construction is an elegant method to delete subsets from Γ, that is, to find a solution for the case $\Gamma' \subseteq \Gamma$. In this situation, we have to revoke the right of some subsets in Γ to know the secret in Σ.

Lemma 4.2. *Let Γ, Γ' be two access structures on P. Then*

$$\Gamma' = \Big(\Gamma \cap \bigcap_{A \in I} F_A\Big) \cup \bigcup_{A \in J} T_A,$$

where $I = \max(\Gamma \setminus \Gamma')$ and $J = \min(\Gamma' \setminus \Gamma)$.

Proof. Recall that $\Gamma' = \cup_{A \in \Gamma'} T_A = \cap_{A \notin \Gamma'} F_A$. First, consider the following two cases:

1. If $\Gamma \subseteq \Gamma'$, then
$$\Gamma' = \bigcup_{A \in \Gamma} T_A \cup \bigcup_{A \in \Gamma' \setminus \Gamma} T_A = \Gamma \cup \bigcup_{A \in J} T_A.$$
2. If $\Gamma' \subseteq \Gamma$, then
$$\Gamma' = \bigcap_{A \notin \Gamma} F_A \cap \bigcap_{A \in \Gamma \setminus \Gamma'} F_A = \Gamma \cap \bigcap_{A \in I} F_A.$$

Suppose that Γ is not contained in Γ' and vice versa. Then consider their intersection and observe that $\Gamma \cap \Gamma' \subseteq \Gamma$. Following the arguments used above in case 2 we obtain that

$$\Gamma \cap \Gamma' = \Gamma \cap \bigcap_{A \in I'} F_A,$$

where $I' = \max(\Gamma \setminus (\Gamma \cap \Gamma')) = \max(\Gamma \setminus \Gamma') = I$. Since $\Gamma \cap \Gamma' \subseteq \Gamma'$, following the arguments used above in case 1 we obtain that

$$\Gamma' = (\Gamma \cap \Gamma') \cup \bigcup_{A \in J'} T_A,$$

where $J' = \min(\Gamma' \setminus (\Gamma \cap \Gamma')) = \min(\Gamma' \setminus \Gamma) = J$. This concludes the proof. □

Proposition 4.3. *Let Γ, Γ' be two access structures on P. Then*

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq |\max(\Gamma \setminus \Gamma')| + |\min(\Gamma' \setminus \Gamma)|.$$

Proof. Let Σ be a secret sharing scheme for Γ. By Lemma 4.2, the access structure Γ' is realized by the secret sharing scheme

$$\Sigma' = \Big(\Sigma \wedge \bigwedge_{A \in I} \Sigma_{F_A}\Big) \vee \bigvee_{A \in J} \Sigma_{T_A},$$

where $I = \max(\Gamma \setminus \Gamma')$, $J = \min(\Gamma' \setminus \Gamma)$, and Σ_{F_A} and Σ_{T_A} are ideal secret sharing schemes for F_A and T_A, respectively. Then $\sigma(\Sigma') \leq \sigma(\Sigma) + |I| + |J|$. □

In the proof of the last theorem we construct a secret sharing scheme for Γ' in terms of ANDs and ORs of a scheme for Γ and schemes for access structures of the form T_A and F_A. These access structures admit ideal schemes for any set of secrets. Therefore, this result is also valid if we restrict ourselves to secret sharing schemes for a particular secret size, for example to secret sharing schemes sharing one bit. In addition, these access structures also admit ideal $(\mathbb{F}, \ell)$-linear secret sharing schemes for any finite field $\mathbb{F}$, for any nonempty $A \subseteq P$ and for any $\ell > 0$. Hence, if we have a $(\mathbb{F}, \ell)$-linear secret sharing scheme realizing Γ, we obtain a $(\mathbb{F}, \ell)$-linear secret sharing scheme for Γ'.

Corollary 4.4. *Let Γ, Γ' be two access structures on P, and let $\mathbb{F}_q$ be a finite field. For every $\ell \geq 1$,*

$$|\lambda_{q,\ell}(\Gamma) - \lambda_{q,\ell}(\Gamma')| \leq \operatorname{dist}(\Gamma, \Gamma').$$

As a consequence of the previous results, the access structures that are close to access structures with efficient secret sharing schemes also admit efficient schemes, and the access structures that are close to access structures requiring large shares also require large shares.

Some applications of secret sharing schemes do not require a complete definition of the access structure. They require subsets in a family $\mathcal{A} \subseteq \mathcal{P}(P)$ to be forbidden, and subsets in a family $\mathcal{B} \subseteq \mathcal{P}(P)$ to be authorized. We say that an access structure Γ is *compatible* with $\mathcal{A}$ and $\mathcal{B}$ if $\mathcal{A} \subseteq \Gamma^c$ and $\mathcal{B} \subseteq \Gamma$. If $\mathcal{A} \cup \mathcal{B} \neq \mathcal{P}(P)$, then there is a certain degree of freedom when choosing the access structure. The number of subsets that are not required to be authorized or forbidden is $r = 2^n - (|\mathcal{A}| + |\mathcal{B}|)$. If we know $\sigma(\Gamma)$ for an access structure Γ that is compatible with $\mathcal{A}$ and $\mathcal{B}$, then we know that the smallest optimal information ratio of the access structures compatible with $\mathcal{A}$ and $\mathcal{B}$ is at least $\sigma(\Gamma) - r$.

4.1 The Lipschitz constant of the optimal information ratio

Next, we present an example that shows that, for distance equal to one, it is not possible to improve the general bound in Theorem 4.1 and in Corollary 4.4. Namely, we describe access structures Γ_n, Γ'_n and Γ''_n with $n \geq 3$ such that $\operatorname{dist}(\Gamma''_n, \Gamma_n) = \operatorname{dist}(\Gamma''_n, \Gamma'_n) = 1$ and $|\sigma(\Gamma''_n) - \sigma(\Gamma_n)| = |\sigma(\Gamma''_n) - \sigma(\Gamma'_n)| = 1 - 1/(n-2)$. For distance greater than one, we do not know whether the bounds in Theorem 4.1 and in Corollary 4.4 are tight.

Example 4.5. Consider the access structures Γ_n and Γ'_n on $P = \{1, \ldots, n\}$ with $\min \Gamma_n = \{\{1, i\} : 2 \leq i \leq n\}$ and $\min \Gamma'_n = \{\{1\}, \{2, \ldots, n\}\}$. These access structures

admit ideal secret sharing schemes for every set of secrets, and ideal linear secret sharing schemes for any finite field $\mathbb{F}$. Now consider the access structures Γ''_n with $\min \Gamma''_n = \{\{1, i\} : 2 \leq i \leq n\} \cup \{\{2, \ldots, n\}\}$. Observe that $\Gamma''_n = \Gamma_n \cup \{\{2, \ldots, n\}\} = \Gamma'_n \setminus \{\{1\}\}$, and so $\operatorname{dist}(\Gamma''_n, \Gamma_n) = \operatorname{dist}(\Gamma''_n, \Gamma'_n) = 1$. By Theorem 4.1 and Corollary 4.4, $\sigma(\Gamma''_n) \leq 2$ and $\lambda(\Gamma''_n) \leq 2$. It was proved in [20] that $\lambda(\Gamma''_n) = \sigma(\Gamma''_n) = 2 - 1/(n-2)$ for $n \geq 3$.

Now we use the notion of Lipschitz continuity to describe the properties of the optimal information ratio. Let $f : X \to Y$ be a function mapping a metric space (X, d_X) to a metric space (Y, d_Y), where d_X and d_Y denote the distance functions in the domain X and in the range Y, respectively. We say that f has *Lipschitz constant* k if $d_Y(f(x), f(y)) \leq k \cdot d_X(x, y)$ for every $x, y \in X$. In this case we also say that f is k-Lipschitz.

In the context of this work, we view the information ratio σ as a function whose domain is M_n, the collection of access structures on $\{1, \ldots, n\}$, and whose range is $\mathbb{R}_{\geq 1}$. Observe that $(M_n, \operatorname{dist})$ and $\mathbb{R}_{\geq 1}$ with the Euclidian distance are metric spaces. Then, we can state the following result, which is in fact equivalent to Theorem 4.1.

Corollary 4.6. *The optimal information ratio is* 1*-Lipschitz.*

By the Example 4.5, it is not possible to give a better general Lipschitz constant for σ. The notion of Lipschitz is often used in continuous domains. However, it has also been used in discrete domains, for example in the study of differential privacy (e.g. [30]). The Lipschitz property provides valuable information about the sensitivity of the function when we vary the input. In this case, it illustrates that close access structures have similar optimal information ratio. Therefore, in M_n we have regions in which the access structures admit secret sharing schemes with *low* information ratio, for instance around ideal access structures. The distribution of these regions and their density in M_n is an open problem. Moreover, the characterization of the values of $\mathbb{R}_{\geq 1}$ that have a preimage by σ is also an open problem.

5 Asymptotic Behavior of the Bound

Our work is focused on the local behavior of the optimal information ratio, and our results are motivated by the study of the optimal information ratio of access structures that are close. In this section we analyze the asymptotic behavior of the optimal information ratio, and the convenience of bounding the difference between the optimal information ratio of two access structures by the distance between them.

In Section 4.1, we presented pairs of access structures at distance one which satisfy that the difference between their optimal information ratios tends to one. We did not find an equivalent result for distance greater than one, but we can show some examples that suggest that our bounds are still useful for large distances, in general.

First, we analyze the bound in Proposition 4.3. Let $f : \mathbb{N} \to \mathbb{R}$ be a function satisfying that $|\sigma(\Gamma) - \sigma(\Gamma')| \leq f(r)$ for every two access structures Γ and Γ', where $r = |\max(\Gamma \setminus \Gamma')| + |\min(\Gamma' \setminus \Gamma)|$. Now we consider a well-known family of access structures defined by Csirmaz in [15], which we denote by $\mathcal{F}$. For every Γ in $\mathcal{F}$, $\sigma(\Gamma) = \Omega(n/\log n)$, where n is the number of participants, $n = N + \log N$, and N is the number of minimal authorized subsets. Observe that, since $x/\log x$ is an increasing function for $x > e$ we have that $n/\log n \geq N/\log N$ for $N \geq 3$, and so $\sigma(\Gamma) = \Omega(N/\log N)$.

If we take Γ to be the empty access structure and Γ' to be in $\mathcal{F}$, then we see that $|\sigma(\Gamma) - \sigma(\Gamma')| = \Omega(N/\log N)$ and $|\max(\Gamma \setminus \Gamma')| + |\min(\Gamma' \setminus \Gamma)| = N$. Hence, we obtain the restriction that $f(r) = \Omega(r/\log r)$. Therefore, if it were possible to improve the bound in Proposition 4.3, it could be improved at most by a logarithmic factor.

Now we analyze the bound in Corollary 4.4. We consider two different families of access structures, and we analyze the bound using particular results for these families. Let $\mathbb{F}_q$ be a finite field, ℓ a positive integer, and let $g : \mathbb{N} \to \mathbb{R}$ be a function that satisfies $|\lambda_{q,\ell}(\Gamma) - \lambda_{q,\ell}(\Gamma')| \leq g(d)$ for every two access structures Γ and Γ', where $d = \mathrm{dist}(\Gamma, \Gamma')$.

Let $\mathcal{H}$ be the family of access structures on a set of n participants, n even, in which all subsets of size strictly greater than $n/2$ are authorized, and the ones of size strictly smaller than $n/2$ are forbidden. There are $2^{\binom{n}{n/2}}$ access structures in $\mathcal{H}$, including the n/2-threshold access structure. Observe that for every access structure in $\mathcal{H}$, half of the access structures in $\mathcal{H}$ are at a distance greater than or equal to $\binom{n}{n/2}/2$.

Linear secret sharing schemes can be represented by matrices (see [3, 37], for example). In a $(\mathbb{F}_q, \ell)$-linear secret sharing scheme with information ratio at most s, the dealer is associated to ℓ rows, which can be considered to be fixed to any set of linearly independent vectors in $\mathbb{F}_q^\ell$. Each participant is associated to at most ℓs rows, and so we have at most $s\ell n + \ell$ rows. By linear algebra, since P is an authorized subset, we can always find an equivalent $(\mathbb{F}_q, \ell)$-linear secret sharing scheme in which the number of columns is smaller or equal than the number of rows minus ℓ. Hence, the number of matrices of this kind is at most $q^{s^2\ell^2n^2}$. Then the number of access structures Γ with $\lambda_{q,\ell}(\Gamma) \leq s$ is smaller than $q^{s^2\ell^2n^2}$. Now we take

$$s = \frac{2^{n/2-1}}{\ell^2 n^{5/4}\sqrt{\log q}}.$$

Using the property that $\binom{n}{n/2} \sim \frac{2^n}{\sqrt{\pi n/2}}$, if we compare $q^{s^2\ell^2n^2}$ with $2^{\binom{n}{n/2}}$, we see that almost all access structures Γ in $\mathcal{H}$ satisfy $\lambda_{q,\ell}(\Gamma) \geq s$. This counting argument is similar to the one in [2].

We take Γ to be the $n/2$-threshold access structure. Then there exists Γ' in $\mathcal{H}$ with $\lambda_{q,\ell}(\Gamma') \geq s$ at a distance $d = \mathrm{dist}(\Gamma, \Gamma')$, where $\binom{n}{n/2}/2 \leq d \leq \binom{n}{n/2}$. These access structures satisfy

$$|\lambda_{q,\ell}(\Gamma) - \lambda_{q,\ell}(\Gamma')| \geq 1 + s = \Omega\left(\frac{\sqrt{d}}{\ell \log(d)\sqrt{\log q}}\right).$$

Hence, we obtain the restriction that $g(d) = \Omega(\sqrt{d}/\log d)$.

Now we consider the family of forbidden graph access structures. Given a graph $G = (V, E)$, the *forbidden graph* access structure determined by G is the access structure on V containing all the pairs in E and all subsets of size at least 3. In this case, the distance between the access structures determined by $G = (V, E)$ and $G' = (V, E')$ is $|E \cup E'| - |E \cap E'|$. As a consequence of the results in [6], for any two forbidden graph access structures Γ and Γ' and for every large enough finite field $\mathbb{F}_q$ we have $|\lambda_{q,1}(\Gamma) - \lambda_{q,1}(\Gamma')| = \tilde{O}(d^{1/4})$, where $d = \mathrm{dist}(\Gamma, \Gamma')$. The results in [34] show that every forbidden graph access structure admits a non-linear secret sharing scheme of information ratio $n^{O(\sqrt{\log\log n/\log n})} = n^{o(1)}$. This suggests that there may exist a better bound for $|\sigma(\Gamma) - \sigma(\Gamma')|$ for forbidden graph access structures.

6 Other Constructions for Close Access Structures

In the previous section, we presented a way to describe an access structure Γ' in terms of another access structure Γ. This combinatorial result was used to construct, given a secret sharing scheme for Γ, a secret sharing scheme for Γ'.

In this section we present a method to construct secret sharing schemes that follows the same strategy, which uses different combinatorial results. As in the previous section, we are able to provide bounds on the optimal information ratio of access structures. These bounds are useful for access structures whose minimal access structures are in a special disposition. We use combinatorial results that are different from the ones presented in the previous section. In particular, the results are based on a new combinatorial notion of $(\mathcal{B}_1, \mathcal{B}_2)$-*covering*, which will be used to construct secret sharing schemes. The interest in using $(\mathcal{B}_1, \mathcal{B}_2)$-*coverings* is that we can transform the problem of finding an efficient scheme into the search of small coverings, and so translate a secret sharing problem into a combinatorial one.

6.1 $(\mathcal{B}_1, \mathcal{B}_2)$-coverings

We introduce here a notion of covering that will be used to find useful descriptions of minimal access structures that are close.

Definition 6.1. Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}(P)$ be two families of subsets satisfying $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$. A family of subsets $\mathcal{C} \subseteq \mathcal{P}(P)$ is a $(\mathcal{B}_1, \mathcal{B}_2)$-*covering* if it satisfies the following properties:

1. for every $A \in \mathcal{B}_1$ and for every $B \in \mathcal{C}$, $A \nsubseteq B$, and
2. for every $A \in \mathcal{B}_2$ there exists $B \in \mathcal{C}$ such that $A \subseteq B$.

Example 6.2. Let $\mathcal{B} \subseteq \mathcal{P}(P)$ be an antichain and let $A \in \mathcal{B}$. Then $\mathcal{C} = \{P \setminus \{i\} : i \in A\}$ is an $(\{A\}, \mathcal{B} \setminus \{A\}) - covering$.

Next, we present in Lemma 6.3 a necessary and sufficient condition for the existence of coverings, and we present in Lemma 6.4 a technical result that is used in the proof of Theorem 6.5.

Lemma 6.3. *Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}(P)$. There exists a $(\mathcal{B}_1, \mathcal{B}_2)$-covering if and only if*

$$A \nsubseteq B \text{ for every } A \in \mathcal{B}_1 \text{ and } B \in \mathcal{B}_2. \tag{3}$$

Proof. Let $\mathcal{C}$ be a $(\mathcal{B}_1, \mathcal{B}_2)$-covering. For every $A \in \mathcal{B}_1$ and $B \in \mathcal{B}_2$, $\mathrm{cl}(A) \cap \mathcal{C} = \emptyset$ and $\mathrm{cl}(B) \cap \mathcal{C} \neq \emptyset$, so $A \nsubseteq B$. Conversely, if $A \nsubseteq B$ for every $A \in \mathcal{B}_1$ and $B \in \mathcal{B}_2$, then $\mathcal{B}_2$ is a $(\mathcal{B}_1, \mathcal{B}_2)$-covering. □

Lemma 6.4. *Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}(P)$. A $(\mathcal{B}_1, \mathcal{B}_2)$-covering is also a $(\mathcal{B}_1, \mathcal{B}_3)$-covering for every $\mathcal{B}_3 \subseteq \mathcal{B}_2$.*

Beimel, Farràs and Mintz constructed efficient secret sharing schemes for very dense graphs [5]. Some of these constructions have been recently improved in [7]. The next theorem abstracts some of the techniques used in [5, Lemma 5.2] and [5, Lemma 5.4]. The proof of the theorem uses colorings of hypergraphs. A *coloring* of $\mathcal{B} \subseteq \mathcal{P}(P)$ with c colors is a mapping $\mu : P \to \{1, \ldots, c\}$ such that for every $A \in \mathcal{B}$ there exists $u, v \in A$ with $\mu(u) \neq \mu(v)$.

Theorem 6.5. *Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \binom{P}{k}$ be two families of subsets with $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ for some $k > 1$. If $\mathcal{B}_1$ has degree d, then there is a $(\mathcal{B}_1, \mathcal{B}_2)$-covering of degree at most $2^k k^k d^{k-1} \ln n$.*

Proof. Due to Lemma 6.3, if $\mathcal{B}_1 \subseteq \binom{P}{k}$, the biggest family of subsets $\mathcal{B}_2' \subseteq \binom{P}{k}$ admitting a $(\mathcal{B}_1, \mathcal{B}_2')$-covering is $\mathcal{B}_2' = \binom{P}{k} \setminus \mathcal{B}_1$. By Lemma 6.4, it is enough to restrict our proof to the case $\mathcal{B}_2 = \binom{P}{k} \setminus \mathcal{B}_1$.

In order to construct a $(\mathcal{B}_1, \mathcal{B}_2)$-covering, we use colorings of $\mathcal{B}_1$. Given a coloring μ of $\mathcal{B}_1$, we consider the family of subsets of elements in P of the same color. Observe that if all the elements in a subset $A \subseteq P$ have the same color by μ, then it implies that $B \nsubseteq A$ for every $B \in \mathcal{B}_1$.

The existence of the covering is proved by using the probabilistic method (see [1], for example). We choose $r = 2^k k^k d^{k-1} \ln n$ random colorings $\mu_1, \ldots, \mu_r$ of $\mathcal{B}_1$ with $2kd$ colors. For every coloring μ_i, we define $\mathcal{C}_i = \{\mu_i^{-1}(c) : \text{c is a color of } \mu_i\}$, that is, $\mathcal{C}_i$ is the collection of maximal monochromatic subsets in μ_i. Now we show that $\mathcal{C} = \cup_{i=1}^r \mathcal{C}_i$ is a $(\mathcal{B}_1, \mathcal{B}_2)$-covering with probability at least $1 - 1/(k!)$.

Let $A = \{v_1, \ldots, v_k\} \in \mathcal{B}_2$. We fix i and compute the probability that $A \subseteq B$ for some $B \in \mathcal{C}_i$, which is equivalent to say that A is monochromatic in μ_i. Fix an arbitrary coloring of $\mathcal{B}_1 \cap \mathcal{P}(P \setminus A)$ with domain $P \setminus A$. We prove that conditioned on this coloring, the probability that A is monochromatic in an extended coloring of $\mathcal{B}_1$ is at least $\frac{1}{2(2kd)^{k-1}}$. Let $B \in \mathcal{B}_1$ with $v_1 \in B$. If $B \setminus \{v_1\}$ is monochromatic, then the color of v_1 must be different from the color of $B \setminus \{v_1\}$. Thus, there are at most d colors that v_1 cannot take. Extending this argument, there are at most kd colors that do not allow A to be monochromatic. Thus the probability that v_1 is colored by one of the remaining $2kd - kd$ colors is at least one half, and the probability that in this case $v_2, \ldots, v_k$ are colored in the same color as v_1 is at least $1/(2kd)^{k-1}$. Then $A \subseteq B$ for some $B \in \mathcal{C}_i$ with probability at least $1/(2(2kd)^{k-1})$.

The probability that $A \nsubseteq B$ for every $B \in \mathcal{C}$ is

$$\left(1 - \frac{1}{2(2kd)^{k-1}}\right)^r \leq e^{-\frac{r}{2(2kd)^{k-1}}} = \frac{1}{n^k}.$$

Thus, the probability that $\mathcal{C}$ is not a $(\mathcal{B}_1, \mathcal{B}_2)$-covering is less than $\binom{n}{k}/n^k \leq 1/k!$. In particular, such covering exists. □

This result has also consequences in graph theory, which corresponds to the case $k = 2$. It implies that every graph $G = (V, E)$ with $E \subseteq \binom{V}{2}$ admits an equivalence cover of degree $16d \ln n$, where d is the degree of the complementary graph $(V, \binom{V}{2} \setminus E)$ (see [5] for more details).

The next proposition allows us to construct formulas, circuits and secret sharing schemes for access structures.

Proposition 6.6. *Let Γ, Γ' be two access structures with $\min \Gamma' \subseteq \min \Gamma$. If $\mathcal{C}$ is a $(\min \Gamma \setminus \min \Gamma', \min \Gamma')$-covering, then*

$$\min \Gamma' = \{A \in \min \Gamma \,:\, A \subseteq B \text{ for some } B \in \mathcal{C}\}.$$

Proof. For every subset $A \in \min \Gamma'$, there exists $B \in \mathcal{C}$ with $A \subseteq B$. For every $A \in \min \Gamma \setminus \min \Gamma'$, $A \nsubseteq B$ for every $B \in \mathcal{C}$, and so the equality holds. □

6.2 Secret Sharing Constructions Using Coverings

The main result of this subsection is Theorem 6.9. The quality of the bounds in this theorem depends on the degree of a covering. In Theorem 6.5, we provide a bound on the degree of coverings. In Example 6.10, we show an access structure for which this technique provides optimal secret sharing schemes.

Lemma 6.7. *Let Γ, Γ' be two access structures with $\min\Gamma' \subseteq \min\Gamma$. Let Σ be a secret sharing scheme for Γ. If there exists a $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering of degree d, then there exists a secret sharing scheme Σ' for Γ' with*

$$\sigma(\Sigma') \leq d\sigma(\Sigma) \quad \text{and} \quad \sigma^T(\Sigma') \leq d\sigma^T(\Sigma).$$

Proof. Let $\mathcal{C}$ be a $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering of degree d. We define a secret sharing scheme Σ' as the OR of all the secret sharing schemes $\Sigma|_A$ for $A \in \mathcal{C}$. By Proposition 6.6, Σ' realizes Γ'. In this scheme, each $i \in P$ receives $\deg_i(\mathcal{C})$ shares. Since $\deg_i(\mathcal{C}) \leq d$, $\sigma(\Sigma') \leq d\sigma(\Sigma)$, and $\sigma^{\mathrm{T}}(\Sigma') = \sum_{A\in\mathcal{C}} \sigma^{\mathrm{T}}(\Sigma|_A) \leq d\sigma^{\mathrm{T}}(\Sigma)$. □

Example 6.8. Let Γ, Γ' be two access structures with $\mathrm{dist}(\min\Gamma, \min\Gamma') = 1$ and $\min\Gamma' \subseteq \min\Gamma$. Observe that in this case $\mathrm{dist}(\Gamma, \Gamma')$ can be much bigger than 1. As we saw in Example 6.2, there exists a $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering $\mathcal{C}$ of degree at most $n-1$. Hence, given a secret sharing scheme Σ for Γ we can construct a secret sharing scheme for Γ' whose information ratio is less than $(n-1)\sigma(\Sigma)$.

Theorem 6.9. *Let Γ, Γ' be two access structures on P. If there exists a $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering of degree d, then*

$$\sigma(\Gamma') \leq d\sigma(\Gamma) + t \quad \text{and} \quad \sigma^T(\Gamma') \leq d\sigma^T(\Gamma) + nt,$$

where $t = \deg(\min\Gamma' \setminus \min\Gamma)$.

Proof. Let Γ'' be the access structure defined by $\min\Gamma'' = \min\Gamma' \cap \min\Gamma$. Observe that $\min\Gamma \setminus \min\Gamma' = \min\Gamma \setminus \min\Gamma''$, and that every $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering is also a $(\min\Gamma \setminus \min\Gamma'', \min\Gamma'')$-covering by Lemma 6.4. Given a secret sharing scheme Σ for Γ, there is a secret sharing scheme Σ'' for Γ'' with $\sigma(\Sigma'') \leq d\sigma(\Sigma)$ and $\sigma^{\mathrm{T}}(\Sigma'') \leq d\sigma^{\mathrm{T}}(\Sigma)$ by Lemma 6.7. Then, using the construction in the proof of Proposition 4.3, we can construct a secret sharing scheme Σ' with access structure Γ' as $\Sigma' = \Sigma'' \vee \Sigma'''$, where $\Sigma''' = \bigvee_{A\in I} \Sigma_{T_A}$ and $I = \min(\Gamma' \setminus \Gamma'') = \min\Gamma' \setminus \min\Gamma$. □

In Example 6.8, we studied the case of two access structures Γ and Γ' with $\mathrm{dist}(\min\Gamma, \min\Gamma') = 1$, and the technique we described can be extended to distances greater than 1. By Theorems 6.5 and 6.9, if $\min\Gamma' \subseteq \min\Gamma$, $|A| \leq k$ for every $A \in \min\Gamma$, and the degree of $\min\Gamma \setminus \min\Gamma'$ is d, then $\sigma(\Gamma') \leq (2^k k^k d^{k-1} \ln n)\sigma(\Gamma)$. This result was proved in [5], and it was improved for the case $k = 2$ [5, Theorem 6.1].

In the following example, we use a technique involving coverings to construct an optimal secret sharing scheme.

Example 6.10. Let P be a set of $n = 2\ell + 1$ participants for some $\ell > 0$. We consider a partition $P = \{a\} \cup P_1 \cup P_2$, where $|P_1| = |P_2| = \ell$. Let Γ be the 2-threshold access structure on P and let Σ be an ideal secret sharing scheme for Γ. Let Γ' be the access structure on P with $\min\Gamma' = \binom{P}{2} \setminus \{\{a, b\} : b \in P_2\}$. By [5, Theorem 7.1], we know that $\sigma^{\mathrm{T}}(\Gamma') \geq n + \ell = 3\ell + 1$. Now we prove that this bound is tight.

Let $\mathcal{C} = \{C_1, C_2\}$ be the $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering with $C_1 = \{a\} \cup P_1$ and $C_2 = P_1 \cup P_2$. Using the construction described in Lemma 6.7, we obtain that $\Sigma' = \Sigma|_{C_1} \vee \Sigma|_{C_2}$ is a secret sharing scheme for Γ'. It satisfies $\sigma^{\mathrm{T}}(\Sigma') = \sigma^{\mathrm{T}}(\Sigma|_{C_1}) + \sigma^{\mathrm{T}}(\Sigma|_{C_2}) = \ell + 1 + 2\ell = 3\ell + 1$. Therefore we can conclude that $\sigma^{\mathrm{T}}(\Gamma') = n + \ell$.

6.3 A Construction Using Sunflowers

In Proposition 6.12, we present another secret sharing construction that follows a procedure analogous to the one in Theorem 4.1, which uses a different description of the access structures.

Lemma 6.11. *Let Γ, Γ' be two access structures on P. Let $\tilde{\Gamma}$ be the access structure with $\min\tilde{\Gamma} = (\min\Gamma) \cap \Gamma'$. Then*

$$\Gamma' = \tilde{\Gamma} \cup \bigcup_{A \in \Gamma \setminus \Gamma'} G_A \cup \bigcup_{A \in J} T_A,$$

where $G_A = \mathrm{cl}((\min S_A) \cap \Gamma')$ and $J = \min(\Gamma' \setminus \Gamma)$.

Proof. Let $\Gamma'' = \Gamma \cap \Gamma'$. According to Lemma 4.2, we can describe Γ' as $\Gamma' = \Gamma'' \cup \bigcup_{A \in J} T_A$. We dedicate the rest of the proof to show that $\Gamma'' = \tilde{\Gamma} \cup \bigcup_{A \in \Gamma \setminus \Gamma'} G_A$. Since $\Gamma = \min\Gamma \cup \bigcup_{A \in \Gamma} \min S_A$, we have that

$$\begin{aligned}\Gamma'' = \mathrm{cl}(\Gamma'') = \mathrm{cl}(\Gamma \cap \Gamma') = \mathrm{cl}((\min\Gamma \cup (\Gamma \setminus \min\Gamma)) \cap \Gamma') \\ = \mathrm{cl}((\min\Gamma) \cap \Gamma') \cup \bigcup_{A \in \Gamma} G_A = \tilde{\Gamma} \cup \bigcup_{A \in \Gamma} G_A.\end{aligned}$$

Let $\mathcal{B}_1 = \Gamma \setminus \Gamma'$, $\mathcal{B}_2 = \min(\Gamma \cap \Gamma')$, and $\mathcal{B}_3 = (\Gamma \cap \Gamma') \setminus \min(\Gamma \cap \Gamma')$. Let $\mathcal{A}_i = \bigcup_{A \in \mathcal{B}_i} G_A$ for $i = 1, 2, 3$. Observe that $\mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3 = \Gamma$, that $\Gamma'' = \tilde{\Gamma} \cup \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$ and that $\mathcal{A}_3 \subseteq \mathcal{A}_2$.

We claim that $\mathcal{A}_2 \subseteq \tilde{\Gamma} \cup \mathcal{A}_1$. Let $A \in \mathcal{B}_2$. If $A \in \min\Gamma$, then $A \in \tilde{\Gamma}$ because $\mathcal{B}_2 \subseteq \Gamma'$, and so $\min S_A \subseteq \tilde{\Gamma}$. Suppose that $A \notin \min\Gamma$. Then there exists $B \in \Gamma$ satisfying $A \in \min S_B$, and in particular $A \in (\min S_B) \cap \Gamma'$. Since $A \in \min(\Gamma \cap \Gamma')$, we have that $B \in \Gamma \setminus (\Gamma \cap \Gamma') = \Gamma \setminus \Gamma' = \mathcal{B}_1$. Then $\mathrm{cl}(\min S_A) \subseteq \mathrm{cl}(A) \subseteq G_B$. Therefore $\mathcal{A}_2 \subseteq \tilde{\Gamma} \cup \mathcal{A}_1$ and so $\Gamma'' = \tilde{\Gamma} \cup \mathcal{A}_1$, which concludes the proof. □

Proposition 6.12. *Let Γ, Γ' be two access structures. Let $\tilde{\Gamma}$ be the access structure with $\min\tilde{\Gamma} = (\min\Gamma) \cap \Gamma'$. Then*

$$\sigma(\Gamma') \leq \sigma(\tilde{\Gamma}) + \mathrm{dist}(\Gamma', \Gamma).$$

Proof. Let Σ and $\tilde{\Sigma}$ be secret sharing schemes for Γ and $\tilde{\Gamma}$, respectively. We use Lemma 6.11 to construct a secret sharing scheme for Γ'. Observe that for every $A \in \Gamma$, $(\min S_A) \cap \Gamma' \subseteq \min S_A$. Hence, using the scheme described for S_A in Section 3 we can construct an ideal secret sharing scheme for G_A, which we call Σ''_A. Then the access structure Γ' is realized by the secret sharing scheme

$$\Sigma' = \Big(\tilde{\Sigma} \vee \bigvee_{A \in \Gamma \setminus \Gamma'} \Sigma''_A\Big) \vee \bigvee_{A \in \Gamma' \setminus \Gamma} \Sigma_{T_A},$$

where Σ_{T_A} is an ideal secret sharing scheme for T_A. It satisfies $\sigma(\Sigma') \leq \sigma(\tilde{\Sigma}) + |\Gamma \setminus \Gamma'| + |\Gamma' \setminus \Gamma| = \sigma(\tilde{\Sigma}) + \mathrm{dist}(\Gamma, \Gamma')$. □

Theorem 4.1 and Proposition 6.12 are based on constructions of the same spirit, but they cannot be compared, in general.

7 Lower Bounds on the Information Ratio

In this section and in the following one, we study techniques for finding lower bounds on the information ratio. For these bounds, we analyze the effect of adding and deleting subsets in the access structure

If we view the secret and the shares of a scheme as random variables, we can compute the entropy of the secret and of the shares. Then, we can obtain bounds on the information ratio using the Shannon information inequalities and other information inequalities (see [3, 35, 23], for example). We study the lower bound on $\sigma(\Gamma)$ introduced by Martí-Farré and Padró [35], which is denoted by $\kappa(\Gamma)$. The bound κ exploits the connection between secret sharing schemes and polymatroids, which is presented below. The value of κ for an access structure can also be obtained by requiring the Shannon inequalities on the entropies of the shares and the secret (see [15, 37] for more details).

The main result in this section is Theorem 7.3, which shows a property of κ that is analogous to the one in Theorem 4.1. We dedicate Section 7.1 to the proof of this theorem.

Definition 7.1. A *polymatroid* is a pair $\mathcal{S} = (Q, f)$ formed by a finite set Q, the *ground set*, and a *rank function* $f\colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

- $f(\emptyset) = 0$.
- f is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $f(X) \leq f(Y)$.
- f is *submodular*: $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y)$ for every $X, Y \subseteq Q$.

Additionally, if $f(X) \leq |X|$ for every $X \subseteq Q$ and f is integer-valued, then we say that $\mathcal{S}$ is a *matroid*.

Definition 7.2. Let Γ be an access structure on P and let $\mathcal{S} = (Q, f)$ be a polymatroid with $Q = P \cup \{p_0\}$. Then $\mathcal{S}$ is a Γ-*polymatroid* if $f(\{p_0\}) = 1$ and it satisfies the following properties for every $A \subseteq P$:

- If $A \in \Gamma$ then $f(A \cup \{p_0\}) = f(A)$.
- If $A \notin \Gamma$ then $f(A \cup \{p_0\}) = f(A) + 1$.

For every access structure Γ on P, we define $\kappa(\Gamma)$ as the infimum of $\max_{p \in P} f(p)$ over all Γ-polymatroids $\mathcal{S} = (Q, f)$. It satisfies $\sigma(\Gamma) \geq \kappa(\Gamma)$ [35]. Most of the known lower bounds on the optimal information ratio have been obtained by computing the exact value of κ, or by computing lower bounds on κ. The exact value of κ can be obtained by solving a Linear Programming problem. More details about this technique can be found in [23], for example. Next, we present the main result of this section.

Theorem 7.3. *Let Γ, Γ' be two access structures on P. Then*

$$|\kappa(\Gamma) - \kappa(\Gamma')| \leq \operatorname{dist}(\Gamma, \Gamma').$$

The proof of this theorem is constructive, and has the spirit as the proof of Theorem 4.1. In this case, we show that given a Γ-polymatroid, we can construct a Γ'-polymatroid in which the rank of the singletons increases at most by $\operatorname{dist}(\Gamma, \Gamma')$. The proof requires new technical lemmas and constructions on polymatroids and so we defer it to Section 7.1.

The access structures presented in Example 4.5 have the property that σ and κ coincide, and so we have the same asymptotic behaviour for κ. That is, κ is 1-Lipschitz and it is not possible to give a better general Lipschitz constant for κ.

An access structure Γ is a *matroid port* if there exists a Γ-polymatroid $\mathcal{S}$ that is a matroid. If Γ is a matroid port, then $\kappa(\Gamma) = 1$ [13, 35]. As a consequence of Theorem 7.3, the value of κ of access structures that are close to matroid ports is small. Martí-Farré and Padró [35] showed that if an access structure Γ is not a matroid port, then $\kappa(\Gamma) \geq 3/2$. In this case, if Γ is at distance 1 of a matroid port, now we can say that then $3/2 \leq \kappa(\Gamma) \leq 2$.

Csirmaz [15] proved that $\kappa(\Gamma) \leq n$ for every access structure Γ. Therefore, the previous theorem only provides useful bounds for access structures that are very close. However, it illustrates the nature of the optimization problems with restrictions derived from Shannon inequalities and the access structure, which may be interesting for other results of information theory.

Recently, this method has been extended to non-Shannon inequalities, for instance in [8, 23, 36]. For an access structure Γ on P and for a family of information inequalities or rank inequalities I, we can define $\kappa_I(\Gamma)$ as the infimum of $\max_{x\in P} f(p)$ over all Γ-polymatroids satisfying the restrictions of I. An interesting open problem is to study for which restrictions I Theorem 7.3 can be extended to κ_I.

7.1 Proof of Theorem 7.3

This subsection is dedicated to the proof of Theorem 7.3. Here we use notation introduced in [18, 36] to describe polymatroids and some technical results in [18] For a function $F : \mathcal{P}(Q) \to \mathbb{R}$ and subsets $X, Y, Z \subseteq Q$, we denote

$$\Delta_F(Y{:}Z|X) = F(X \cup Y) + F(X \cup Z) - F(X \cup Y \cup Z) - F(X) \tag{4}$$

and $\Delta_F(Y{:}Z) = \Delta_F(Y{:}Z|\emptyset)$. Observe that $\Delta_F(Y{:}Z|X) = \Delta_F(Y{:}X \cup Z) - \Delta_F(Y{:}X)$. In order to simplify the notation, we write $F(x)$ instead of $F(\{x\})$ for any $x \in Q$.

Proposition 7.4 ([18])**.** *A map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if $f(\emptyset) = 0$ and $\Delta_f(y{:}z|X) \geq 0$ for every $X \subseteq Q$ and $y, z \in Q \setminus X$.*

If $\mathcal{S} = (Q, f)$ is a Γ-polymatroid, then $\Delta_f(p_0{:}A) = 1$ if $A \in \Gamma$ and $\Delta_f(p_0{:}A) = 0$ if $A \notin \Gamma$. In this case, $f(A \cup \{p_0\}) = f(A) + 1 - \Delta_f(p_0{:}A)$ for every $A \subseteq P$. Next, we enumerate some properties of Γ-polymatroids that will be used in the proof of Proposition 7.6.

Lemma 7.5. *Let Γ be an access structure an let $\mathcal{S} = (Q, f)$ be a Γ-polymatroid. Then for every $A \subseteq Q$ and $p, q \in Q \setminus A$ we have*

p1) $\Delta_f(p{:}p|A) = f(p \cup A) - f(A) \geq 0$.

p2) $\Delta_f(p{:}A \cup \{q\}) \geq \Delta_f(p{:}A)$

p3) $\Delta_f(p{:}q|A \cup \{p_0\}) - \Delta_f(p{:}q|A) =$
$= \Delta_f(p_0{:}A \cup \{p, q\}) + \Delta_f(p_0{:}A) - \Delta_f(p_0{:}A \cup \{p\}) - \Delta_f(p_0{:}A \cup \{q\})$.

Below we define the AND and OR operations on Γ-polymatroids. We show in Proposition 7.6 that these operations are well defined and that the resulting polymatroids are associated to the intersection and union of access structures, respectively.

Proposition 7.6. *Let Γ_1 and Γ_2 be two access structures on P. Let $\mathcal{S}_1 = (Q, f_1)$ be a Γ_1-polymatroid and $\mathcal{S}_2 = (Q, f_2)$ a Γ_2-polymatroid. Let $f_1 \vee f_2$ and $f_1 \wedge f_2$ be the real functions on Q satisfying that for every $A \subseteq P$*

- $(f_1 \vee f_2)(A) = f_1(A) + f_2(A) - \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}$
- $(f_1 \vee f_2)(A \cup \{p_0\}) = f_1(A \cup \{p_0\}) + f_2(A \cup \{p_0\}) - 1$
- $(f_1 \wedge f_2)(A) = f_1(A) + f_2(A)$
- $(f_1 \wedge f_2)(A \cup \{p_0\}) = f_1(A \cup \{p_0\}) + f_2(A \cup \{p_0\}) + \max\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\} - 1$

Then the pair $(Q, f_1 \vee f_2)$ is a $\Gamma_1 \cup \Gamma_2$-polymatroid, and $(Q, f_1 \wedge f_2)$ is a $\Gamma_1 \cap \Gamma_2$-polymatroid. These polymatroids are denoted by $\mathcal{S}_1 \vee \mathcal{S}_2$ and $\mathcal{S}_1 \wedge \mathcal{S}_2$, respectively.

Proof. First we prove that $\mathcal{S}_1 \vee \mathcal{S}_2$ and $\mathcal{S}_1 \wedge \mathcal{S}_2$ are polymatroids using Proposition 7.4. We show that $\Delta_{f_1 \vee f_2}(p{:}q|A) \geq 0$ and $\Delta_{f_1 \vee f_2}(p{:}q|A \cup \{p_0\}) \geq 0$ for every $p, q \in Q$ and $A \subseteq P$; and then we show the same property for $f_1 \wedge f_2$. By p1) in Lemma 7.5, it is enough to check it for $p \neq q$, and so we can split the proof into the following 6 different cases.

Let $A \subseteq P$ and let $p, q \in P$. In order to simplify the notation, we define the set $Ap = A \cup \{p\}$ and, analogously, Ap_0, Aq and Apq.

1. $\Delta_{f_1 \vee f_2}(p{:}q|A) = \Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) + a - b$, where

   $$a = \min\{\Delta_{f_1}(p_0{:}Apq), \Delta_{f_2}(p_0{:}Apq)\} + \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}, \text{ and}$$
   $$b = \min\{\Delta_{f_1}(p_0{:}Ap), \Delta_{f_2}(p_0{:}Ap)\} + \min\{\Delta_{f_1}(p_0{:}Aq), \Delta_{f_2}(p_0{:}Aq)\}.$$

   Suppose that $a < b$. If $a = 0$ then $\Delta_{f_1}(p_0{:}Apq) = 0$ or $\Delta_{f_2}(p_0{:}Apq) = 0$. By p2) of Lemma 7.5, it implies that $b = 0$. Hence, we can restrict ourselves to the case $a = 1$ and $b = 2$. In this case, there exists some $i \in \{1, 2\}$ for which $\Delta_{f_i}(p_0{:}Apq) = \Delta_{f_i}(p_0{:}Ap) = \Delta_{f_i}(p_0{:}Aq) = 1$ and $\Delta_{f_i}(p_0{:}A) = 0$. Using p3) of Lemma 7.5, we have that

   $$\begin{aligned} a - b =& \Delta_{f_i}(p_0{:}Apq) + \Delta_{f_i}(p_0{:}A) - \Delta_{f_i}(p_0{:}Ap) - \Delta_{f_i}(p_0{:}Aq) \\ =& \Delta_{f_i}(p{:}q|Ap_0) - \Delta_{f_i}(p{:}q|A) \end{aligned}$$

   Therefore $\Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) + a - b \geq 0$.

2. $\Delta_{f_1 \vee f_2}(p{:}p_0|A) = \Delta_{f_1 \vee f_2}(p_0{:}Ap) - \Delta_{f_1 \vee f_2}(p_0{:}A)$

   $$= \max\{\Delta_{f_1}(p_0{:}Ap), \Delta_{f_2}(p_0{:}Ap)\} - \max\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}.$$

   It is nonnegative by property p2) of Lemma 7.5.

3. $\Delta_{f_1 \vee f_2}(p{:}q|Ap_0) = \Delta_{f_1}(p{:}q|Ap_0) + \Delta_{f_2}(p{:}q|Ap_0) \geq 0$.

4. $\Delta_{f_1 \wedge f_2}(p{:}q|A) = \Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) \geq 0$.

5. $\Delta_{f_1 \wedge f_2}(p{:}p_0|A) = \Delta_{f_1 \wedge f_2}(p_0{:}Ap) - \Delta_{f_1 \wedge f_2}(p_0{:}A)$

$$= \min\{\Delta_{f_1}(p_0{:}Ap), \Delta_{f_2}(p_0{:}Ap)\} - \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}.$$

   It is nonnegative by property p2) of Lemma 7.5.

6. $\Delta_{f_1 \wedge f_2}(p{:}q|A \cup \{p_0\}) = \Delta_{f_1 \vee f_2}(p{:}q|A)$ because $f_1 \wedge f_2(Ap_0) = f_1 \vee f_2(A) + 1$. Hence, it is also nonnegative.

Therefore, $\mathcal{S}_1 \vee \mathcal{S}_2$ and $\mathcal{S}_1 \wedge \mathcal{S}_2$ are polymatroids. Observe that $f_1 \vee f_2(p_0) = f_1 \wedge f_2(p_0) = 1$. Since $\Delta_{f_1 \vee f_2}(p_0{:}A) = \max\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}$, we have that $\Delta_{f_1 \vee f_2}(p_0{:}A) = 1$ if and only if $A \in \Gamma_1$ or $A \in \Gamma_2$, and so $\mathcal{S}_1 \vee \mathcal{S}_2$ is a $\Gamma_1 \cup \Gamma_2$-polymatroid. Since $\Delta_{f_1 \wedge f_2}(p_0{:}A) = \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}$, we have that $\Delta_{f_1 \wedge f_2}(p_0{:}A) = 1$ if and only if $A \in \Gamma_1$ and $A \in \Gamma_2$, and so $\mathcal{S}_1 \wedge \mathcal{S}_2$ is a $\Gamma_1 \cap \Gamma_2$-polymatroid. □

Proof of Theorem 7.3. The proof of this theorem is analogous to the proof of Theorem 4.1. Let $A \subseteq P$. We define the T_A-polymatroid $\mathcal{S}_{T_A} = (Q, h)$ as the one with $h(B) = |B \cap A|$ for every $B \subseteq P$, and $\Delta_h(p_0 : B) = 1$ if and only if $A \subseteq B$. We define the F_A-polymatroid $\mathcal{S}_{F_A} = (Q, h)$ as the one with $h(B) = 1$ if $|B \cap (P \setminus A)| \neq 0$ and $h(B) = 0$ otherwise, and $\Delta_h(p_0 : B) = 1$ if and only if $|B \cap (P \setminus A)| > 0$.

Let $\mathcal{S}$ be a Γ-polymatroid. By Lemma 4.2, the following construction is a Γ'-polymatroid:

$$\mathcal{S}' = \Big(\mathcal{S} \wedge \bigwedge_{A \in I} \mathcal{S}_{F_A}\Big) \vee \bigvee_{A \in J} \mathcal{S}_{T_A},$$

where $I = \max(\Gamma \setminus \Gamma')$ and $J = \min(\Gamma' \setminus \Gamma)$. Then $\kappa(\Gamma') \leq \kappa(\Gamma) + |\Gamma \setminus \Gamma'| + |\Gamma' \setminus \Gamma| = \kappa(\Gamma) + \mathrm{dist}(\Gamma, \Gamma')$. □

8 Bounds for Linear Secret Sharing Schemes

For any finite field $\mathbb{F}$, every $(\mathbb{F}, 1)$-linear secret sharing scheme Σ is equivalent to a monotone span program of size $\sigma^{\mathrm{T}}(\Sigma)$ (see [3] for more details). Since the bounds studied in this section are bounds on the total information ratio of $(\mathbb{F}, 1)$-linear secret sharing schemes, we have the same results for the size of monotone span programs. Next, we present a formulation of the Razborov rank measure [40] that is adapted to the context of secret sharing and access structures.

8.1 Razborov's Rank Measure

Let Γ be an access structure on P, and let $U \subseteq \Gamma$ and $V \subseteq \Gamma^c$ be two families of subsets. For any $U_0 \subseteq U$ and $V_0 \subseteq V$, we say that the Cartesian product $U_0 \times V_0$ is a (U, V)-*rectangle*. For each $i \in P$, define the (U, V)-rectangle $R_i = (U \times V) \cap (T_{\{i\}} \times F_{\{i\}})$. Denote the set of all such rectangles by $\mathcal{R}_\Gamma(U, V) = \{R_1, \ldots, R_n\}$.

Let $\mathbb{F}$ be a field and let A be any $|U| \times |V|$ matrix over $\mathbb{F}$ with rows indexed by elements of U and columns indexed by elements of V. The *restriction* of A to the rectangle $R = U_0 \times V_0$ is the submatrix $A \restriction_R$ obtained by setting to 0 all entries not indexed by R.

Definition 8.1 ([40])**.** Let $\Gamma \subseteq \mathcal{P}(P)$ be an access structure, $U \subseteq \Gamma$, $V \subseteq \Gamma^c$. Let $\mathbb{F}$ be a field and let A be a $|U| \times |V|$ matrix over $\mathbb{F}$. If $\text{rank}(A) > 0$, the *rank measure of* Γ *with respect to* A is given by

$$\mu_A(\Gamma) = \frac{\text{rank}(A)}{\max_{R \in \mathcal{R}_\Gamma(U,V)} \text{rank}(A \restriction_R)}.$$

If $\text{rank}(A) = 0$, we set $\mu_A(\Gamma) = 0$. We accordingly define the *rank measure of* Γ as

$$\mu(\Gamma) = \max_A \mu_A(\Gamma),$$

where the maximum is taken over all families of subsets $U \subseteq \Gamma$, $V \subseteq \Gamma^c$ and all matrices A of the form stated above.

Razborov [40] showed that the rank measure of a monotone Boolean function is a lower bound on the size of the shortest formula for this function (see Section 9). Later, Gál [26] proved that the rank measure is also a lower bound on the size of monotone span programs. Taking into account the connection between monotone span programs and linear secret sharing schemes mentioned above, we obtain that the rank function is a lower bound on the optimal information ratio for linear secret sharing schemes. Namely, we have the following result.

Theorem 8.2. *Let $\Gamma \subseteq \mathcal{P}(P)$ an access structure, $U \subseteq \Gamma$, $V \subseteq \Gamma^c$. Let $\mathbb{F}_q$ be a field and let A be a $|U| \times |V|$ matrix over $\mathbb{F}_q$. Then,*

$$\mu_A(\Gamma) \leq \lambda^T_{q,1}(\Gamma).$$

In the following theorem, we study the behavior of the rank measure when we add or delete subsets from an access structure.

Proposition 8.3. *Let $\Gamma, \Gamma' \subseteq \mathcal{P}(P)$ be access structures, $U \subseteq \Gamma$, $V \subseteq \Gamma^c$. Fix a field $\mathbb{F}$ and let A be a $|U| \times |V|$ matrix over $\mathbb{F}$. Then, there exist $U' \subseteq \Gamma'$, $V' \subseteq \Gamma'^c$ and a $|U'| \times |V'|$ matrix A' such that*

$$\mu_A(\Gamma) \leq \mu_{A'}(\Gamma') + \text{dist}(\Gamma, \Gamma').$$

Proof. Set $U' = U \cap \Gamma'$ and $V' = V \cap \Gamma'^c$, and let A' be the restriction of A to $U' \times V'$. Then, observe that $|U \backslash U'| \leq |\Gamma \backslash \Gamma'|$, since $U \backslash U' = U \backslash \Gamma'$ and $U \subseteq \Gamma$. Similarly, we see that $|V \backslash V'| \leq |\Gamma' \backslash \Gamma|$ by using $\Gamma^c \backslash \Gamma'^c = \Gamma' \backslash \Gamma$. Since A' is the submatrix obtained by setting to 0 all rows in A indexed by $U \backslash U'$ and all columns indexed by $V \backslash V'$, we have

$$\text{rank}(A) \leq \text{rank}(A') + |U \backslash U'| + |V \backslash V'| \leq \text{rank}(A') + \text{dist}(\Gamma, \Gamma').$$

Let $\mathcal{R}_\Gamma(U,V) = \{R_1, \ldots, R_n\}$ and $\mathcal{R}_{\Gamma'}(U',V') = \{R'_1, \ldots, R'_n\}$. Since $R'_i = R_i \cap (U' \times V')$, we have that $A' \restriction_{R'_i}$ is a submatrix of $A \restriction_{R_i}$, and thus $\text{rank}(A \restriction_{R_i}) \geq \text{rank}(A' \restriction_{R'_i})$. Hence,

$$\max_{R \in \mathcal{R}_\Gamma(U,V)} \text{rank}(A \restriction_R) \geq \max_{R' \in \mathcal{R}_{\Gamma'}(U',V')} \text{rank}(A' \restriction_{R'}).$$

Given a rectangle $R \in \mathcal{R}_\Gamma(U,V)$, let $R' = R \cap (U' \times V')$. Note that $A' \restriction_{R'}$ is a submatrix of $A \restriction_R$, and thus $\text{rank}(A \restriction_R) \geq \text{rank}(A' \restriction_{R'})$. Since the map $\mathcal{R}_\Gamma(U,V) \to \mathcal{R}_{\Gamma'}(U',V')$ given by $R \mapsto R \cap (U' \times V')$ is exhaustive, we get the inequality

$$\max_{R \in \mathcal{R}_\Gamma(U,V)} \text{rank}(A \restriction_R) \geq \max_{R' \in \mathcal{R}_{\Gamma'}(U',V')} \text{rank}(A' \restriction_{R'}).$$

By using the previous inequalities, we see that

$$\mu_A(\Gamma) = \frac{\operatorname{rank}(A)}{\max_{R\in\mathcal{R}_\Gamma(U,V)} \operatorname{rank}(A\restriction_R)} \leq \frac{\operatorname{rank}(A') + \operatorname{dist}(\Gamma,\Gamma')}{\max_{R'\in\mathcal{R}'_{\Gamma'}(U',V')} \operatorname{rank}(A'\restriction_{R'})}$$
$$\leq \mu_{A'}(\Gamma') + \operatorname{dist}(\Gamma,\Gamma').$$

□

Theorem 8.4. *Let $\Gamma, \Gamma' \subseteq \mathcal{P}(P)$ be access structures. Then*

$$|\mu(\Gamma) - \mu(\Gamma')| \leq \operatorname{dist}(\Gamma,\Gamma').$$

Proof. Let A be the $|U| \times |V|$ matrix such that $\mu(\Gamma) = \mu_A(\Gamma)$, and let A' be the restriction of A to $U' \times V'$, where $U' = U \cap \Gamma'$ and $V' = V \cap \Gamma'^c$. By Proposition 8.3 we have $\mu(\Gamma) \leq \mu_{A'}(\Gamma') + \operatorname{dist}(\Gamma,\Gamma')$. Now, by definition $\mu_{A'}(\Gamma') \leq \mu(\Gamma')$, so $\mu(\Gamma) \leq \mu(\Gamma') + \operatorname{dist}(\Gamma,\Gamma')$. □

Note that the behavior of the rank function bound is different from that of $\lambda^{\mathrm{T}}_{q,1}$. If we extend the bound on Corollary 4.4 to λ^{T} we have that $|\lambda^{\mathrm{T}}_{q,\ell}(\Gamma) - \lambda^{\mathrm{T}}_{q,\ell}(\Gamma')| \leq n \cdot \operatorname{dist}(\Gamma,\Gamma')$ for every two access structures Γ and Γ'.

Recently, in [39], the rank function bound has been used to prove that for every prime p there exist access structures Γ^p for which $\lambda^{\mathrm{T}}_{q,1}(\Gamma^p) = 2^{\Omega(n)}$ for every finite field $\mathbb{F}_q$ of characteristic different from p. Let $P = P_2 \cup P_3$, where $P_2 = \{1,\ldots,n\}$ and $P_3 = \{n+1,\ldots,2n\}$. Let Γ be the access structure P with $\Gamma|_{P_2} = \Gamma^2$ and $\Gamma|_{P_3} = \Gamma^3$ satisfying that for every $A \in \min\Gamma$ either $A \subseteq P_2$ or $A \subseteq P_3$. This access structure satisfies $\lambda^{\mathrm{T}}_{q,1}(\Gamma) = 2^{\Omega(n)}$ for every finite field $\mathbb{F}_q$.

8.2 Critical subfamilies

The next technique provides lower bounds on the size of the shares for linear secret sharing schemes. It was first introduced in [4].

Definition 8.5. Let Γ be an access structure and let $\mathcal{H} \subseteq \min\Gamma$. We say that $\mathcal{H}$ is a *critical subfamily* for Γ, if every $H \in \mathcal{H}$ contains a set $T_H \subseteq H$, $|T_H| \geq 2$, such that the following two conditions are satisfied

1. The set T_H uniquely determines H in the subfamily $\mathcal{H}$: No other set in $\mathcal{H}$ contains T_H.
2. For any subset $Y \subseteq T_H$, the set $S_Y = \cup_{A\in\mathcal{H},\, A\cap Y\neq\emptyset} A \setminus Y$ does not contain any member of $\min\Gamma$.

Theorem 8.6. *Let $\mathbb{F}_q$ be a finite field. Let Γ be an access structure and let $\mathcal{H}$ be a critical subfamily for Γ. Then $\lambda^{T}_{q,1}(\Gamma) \geq |\mathcal{H}|$.*

Given a critical subfamily for an access structure Γ, it is easy to construct a critical subfamily for an access structure Γ' obtained by deleting some subsets from Γ or from $\min\Gamma$. However, it is not easy to find a critical subfamily for access structures that are obtained by adding subsets to Γ or to $\min\Gamma$.

Lemma 8.7. *Let $\mathcal{H}$ be the critical subfamily for an access structure Γ. Let Γ' be an access structure with $\min\Gamma' \subseteq \min\Gamma$ and $|\min\Gamma \setminus \min\Gamma'| = \ell$, and let Γ'' be an access structure with $\Gamma'' \subseteq \Gamma$ and $|\Gamma \setminus \Gamma''| = \ell$. Then there exist two critical subfamilies $\mathcal{H}'$ and $\mathcal{H}''$ for Γ' and Γ'', respectively, with $|\mathcal{H}'| \geq |\mathcal{H}| - \ell$ and $|\mathcal{H}''| \geq |\mathcal{H}| - \ell$.*

Proof. The families of subsets $\mathcal{H}' = \mathcal{H} \cap \min\Gamma'$ and $\mathcal{H}'' = \mathcal{H} \cap \Gamma''$ are critical subfamilies for Γ' and Γ'', respectively. □

9 Formulas for Monotone Boolean Functions

In this section, we apply the approach of Section 4 to study the behavior of the complexity measures associated to monotone Boolean functions. Informally, our results show that similar monotone Boolean functions have close complexity measures. In particular, we aim to give similar bounds as those in Theorems 4.1 and 6.9 and to Proposition 6.12 for the leafsize and the size of monotone Boolean functions. For an introduction to Boolean functions, see [31, 46], for example.

9.1 Definitions

A *Boolean function* is a function of the form $f : \{0,1\}^n \to \{0,1\}$ for some $n \geq 1$. We also see the domain of a Boolean function as the power set of $P = \{1, \ldots, n\}$ via the bijection $\{0,1\}^n \to \mathcal{P}(P)$ given by $(x_i)_{i \in P} \mapsto \{i \in P : x_i = 1\}$. Then we denote by Γ_f the collection of elements $A \in \mathcal{P}(P)$ such that $f(A) = 1$. A Boolean function f is called *monotone* if Γ_f is an access structure. In this case, we denote $\min f = \min\Gamma_f$. If the domain of a Boolean function f is $\{0,1\}^n$, we say f is *fanin-n*. For two monotone fanin-n Boolean functions f, f', we define the *distance* between f and f' as $\operatorname{dist}(f, f') = \operatorname{dist}(\Gamma_f, \Gamma'_f)$.

Given a Boolean function $f : \mathcal{P}(P) \to \{0,1\}$ and a set $B \subseteq P$, we define the *restriction of f to B* as the Boolean function $f|_B : \mathcal{P}(P) \to \{0,1\}$ given by $f|_B(A) = f(A \cap B)$. We have that $\Gamma_{f|_B} = \Gamma_f|_B$.

If $\Phi, g_1, \ldots, g_m$ are Boolean functions and Φ is fanin-m, we can define a Boolean function $\Phi(g_1, \ldots, g_m)$ by applying all the outputs of $g_1, \ldots, g_m$ to Φ in an orderly manner. For $i \in P$, we denote the *i-th input variable* by x_i. Note that x_i can be seen as the monotone Boolean function satisfying $\Gamma_{x_i} = T_{\{i\}}$.

We now define formulas and some related concepts.

Definition 9.1. Let Ω be a set of Boolean functions. A *formula S over Ω* is a sequence $(g_1, \ldots, g_m)$ of Boolean functions such that

- the first k Boolean functions $g_1, \ldots, g_k$ are input variables,
- for every g_j that is not an input variable, there exists $\Phi \in \Omega$ and $\ell_1, \ldots, \ell_{d_j} < j$ such that $g_j = \Phi(g_{\ell_1}, \ldots, g_{\ell_{d_j}})$, and
- for every g_j other than g_m, there exists a single function in S that is computed using g_j (i.e., g_j is *fanout*-1).

We say a formula $S = (g_1, \ldots, g_m)$ *computes* a Boolean function f if $f = g_m$. We say that a formula over Ω is *monotone* if $\Omega = \{\wedge, \vee\}$. Similarly, we say it is *deMorgan* if $\Omega = \{\wedge, \vee, \neg\}$ and the gate $\neg$ can only be applied to input variables.

Let F_f and F_g be formulas computing monotone Boolean functions f and g, respectively. Then, $F_f \wedge F_g$ denotes the formula computing the Boolean function $h = f \wedge g = \max\{f, g\}$ built by appending the AND of the outputs of F_f and F_g. We then have $\Gamma_h = \Gamma_f \cap \Gamma_g$. Similarly, $F_f \vee F_g$ denotes the formula computing the Boolean function $h' = f \vee g = \min\{f, g\}$ built by appending the OR of the outputs of F_f and F_g, and we have $\Gamma_{h'} = \Gamma_f \cup \Gamma_g$. For every formula F and $B \subseteq P$, we define $F|_B$ as the formula that is obtained by replacing x_i by 0 for every $i \notin B$. If F computes a function f, then $F|_B$ computes $f|_B$.

9.2 Bounds on the Size of Formulas and Circuits

We now analyze the minimal leafsize L, which is a complexity measure attached to monotone Boolean functions. The *leafsize* of a formula is defined as the number of input variables in it. We define the *deMorgan* (resp. *monotone*) *minimal leafsize* $L(f)$ (resp. $L_+(f)$) of a Boolean function f as the smallest leafsize over all deMorgan (resp. monotone) formulas computing f. We state our results here in terms of L, but they all hold verbatim for L_+. Moreover, our results can be adapted to other complexity measures, such as the size of circuits.

Before stating our results, we give formulas and complexity measures for particular families of Boolean functions. We start with the Boolean functions associated to the access structures T_A, R_A, S_A defined in Section 3, and we proceed with the restriction $f|_B$ of a Boolean function f to $B \subseteq P$.

The functions f_{T_A} and f_{F_A} admit the formulas $\bigwedge_{i \in A} x_i$ and $\bigvee_{i \in P \setminus A} x_i$ of leafsizes $|A|$ and $n - |A|$, respectively. Since $S_A = T_A \cap F_A$, we have that $\left(\bigwedge_{i \in A} x_i\right) \wedge \left(\bigvee_{i \in P \setminus A} x_i\right)$ is a formula for f_{S_A} of leafsize n.

We now consider the restriction $f|_B : \{0,1\}^n \to \{0,1\}$ of a Boolean function f. By applying the restriction $x_i = 0$ for all $i \notin B$ to a minimal monotone or deMorgan formula for f, and removing redundant input variables and Boolean functions, we get a formula for $f|_B$. Therefore $L(f|_B) \leq L(f)$.

Next, we present analogous results to Theorems 4.1 and 6.9 and Proposition 6.12 for the minimal leafsize of monotone Boolean functions. The following proposition shows that close monotone Boolean functions have similar minimal leafsizes.

Proposition 9.2. *For every two monotone Boolean functions f and f',*

$$|L(f) - L(f')| \leq n \cdot \operatorname{dist}(f, f').$$

Proof. Let F be a formula computing f. Let $I = \max(\Gamma \setminus \Gamma')$ and let $J = \min(\Gamma' \setminus \Gamma)$. Using Lemma 4.2 with $\Gamma = \Gamma_f$ and $\Gamma' = \Gamma_{f'}$ we see that

$$F' = (F \wedge \bigwedge_{A \in I} G_A) \vee \bigvee_{A \in J} H_A$$

is a formula computing f', where G_A and H_A are the formulas for F_A and T_A described above, respectively. Hence,

$$L(f') \leq L(f) + \sum_{A \in I} |P \setminus A| + \sum_{A \in J} |A| \leq L(f) + n \cdot \operatorname{dist}(\Gamma, \Gamma').$$

□

The proofs of the next results are omitted because they are analogous to the proofs of Theorem 6.9 and Proposition 6.12.

Proposition 9.3. *Let $f, f' : \{0,1\}^n \to \{0,1\}$ be two monotone Boolean functions. If there exists a $(\min f \setminus \min f', \min f' \cap \min f')$-covering of degree d, then*

$$L(f') \leq dL(f) + nt,$$

where $t = \deg(\min f' \setminus \min f)$.

Proposition 9.4. *Let f, f' be two monotone Boolean functions, and let $\tilde{f}$ be the monotone Boolean function with $\min \tilde{f} = \min f \cap \Gamma_{f'}$. Then*

$$L(f') \leq L(\tilde{f}) + n \cdot \mathrm{dist}(f, f').$$

9.3 Submodular Formal Complexity Measures

A nonnegative real-valued function μ defined on the set of monotone Boolean functions in n variables is a *submodular formal complexity measure* if

- $\mu(x_i) \leq 1$ for $i = 1, \ldots, n$,
- $\mu(f \wedge g) + \mu(f \vee g) \leq \mu(f) + \mu(g)$ for all monotone Boolean functions f, g.

For every submodular formal complexity measure μ and for every monotone Boolean function f, $\mu(f) \leq L(f)$ [41]. See [31, 41] for more details about submodular formal complexity measures.

Proposition 9.5. *Let μ be a submodular formal complexity measure. Then for every two monotone Boolean functions f and f',*

$$|\mu(f) - \mu(f')| \leq n \cdot \mathrm{dist}(f, f')$$

Proof. Let $\Gamma = \Gamma_f$ and $\Gamma' = \Gamma_{f'}$. Let $I = \max(\Gamma \setminus \Gamma')$, let $J = \min(\Gamma' \setminus \Gamma)$, and let g and h be the monotone Boolean functions associated to the access structures $\cap_{A \in I} F_A$ and $\cup_{A \in J} T_A$, respectively. Since $f' = (f \wedge g) \vee h$ and μ is submodular,

$$\begin{aligned}
\mu(f') &= \mu((f \wedge g) \vee h) \\
&\leq \mu(f \wedge g) + \mu(h) - \mu((f \wedge g) \wedge h) \\
&\leq \mu(f) + \mu(g) - \mu(f \vee g) + \mu(h) - \mu((f \wedge g) \wedge h) \\
&\leq \mu(f) + \mu(g) + \mu(h).
\end{aligned}$$

Since μ is submodular, the size of the monotone formulas described above for T_A and F_A are upper bounds on $\mu(f_{T_A})$ and $\mu(f_{F_A})$ (see [41]). Then

$$\begin{aligned}
\mu(g) + \mu(h) = \mu(\bigcap_{A \in I} F_A) + \mu(\bigcup_{A \in J} T_A) &\leq \sum_{A \in I} (n - |A|) + \sum_{A \in J} |A| \\
&\leq n \cdot |I| + n \cdot |J| \leq n \cdot \mathrm{dist}(f, f').
\end{aligned}$$

□

The Razborov rank measure we introduced in Section 8.1 was originally defined over Boolean functions, and it is submodular (see [41]). Note that the bound we obtained for the Razborov rank measure in Theorem 8.4 is much better than the one in the previous proposition.

The behavior of μ_A and L for close monotone Boolean functions is different. Let f and f' be two monotone Boolean functions at a distance ℓ. Let A and A' be matrices over a finite field $\mathbb{F}$ that maximize $\mu_A(f)$ and $\mu_{A'}(f')$, respectively. By Theorem 8.4, the difference $\mu_A(f) - \mu_{A'}(f')$ is at most ℓ, but the difference $L(f) - L(f')$ can be much bigger than ℓ.

The following examples show that the functions κ, σ, σ^{T}, λ, and λ^{T} are neither submodular nor supermodular. Let Γ and Γ' be the access structures on $P = \{1,2,3,4\}$ with $\min\Gamma = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}$ and $\min\Gamma' = \{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\}$. Both Γ and Γ' admit ideal linear secret sharing schemes, but $\kappa(\Gamma \cap \Gamma') = 3/2$. Hence none of the functions is submodular. Now let Γ and Γ' be the access structures on P with $\min\Gamma = \{\{1,2\},\{2,3\},\{3,4\}\}$ and $\min\Gamma' = \{\{1,2\},\{1,4\},\{3,4\}\}$. Both $\Gamma \cap \Gamma'$ and $\Gamma \cup \Gamma'$ admit ideal linear secret sharing schemes, but $\kappa(\Gamma) = \kappa(\Gamma') = 3/2$. Hence none of the parameters is supermodular.

10 Conclusions and open problems

The main objective of this work was to discover properties of the access structures that admit efficient secret sharing schemes. We showed that access structures that are close admit secret sharing schemes with similar information ratio. We bounded the difference between information ratios by the distance between the access structures. Our results are constructive: we presented a method which, given a secret sharing scheme for a particular access structure, allows to create secret sharing schemes for nearby access structures. This method is simple, but it apparently provides good bounds for both short and large distances (Sections 4.1 and 5).

Since access structures that are close admit secret sharing schemes with similar information ratio, in the domain of access structures we have regions in which the access structures admit secret sharing schemes with low information ratio, for instance around ideal access structures. An interesting line of research is to study these regions, analyze their distribution and their density in the domain of access structures.

We also provide a combinatorial result that leads to general bounds for the optimal information ratio of access structures whose minimal access structures are close. We translate the search of efficient secret sharing scheme to a combinatorial problem. For graph access structures, better constructions are known [5, 7], but for general access structures our approach is still valid.

Our techniques are general, and we extended them to other models of computation, bounding the formula size, the circuit size, and the monotone span program size for monotone Boolean functions. Moreover, we believe that our approach can also be useful in information theory and coding theory, in particular in network coding and index coding. Our problem can be seen as an information-theoretic problem as follows. Suppose that we have a family of random variables, satisfying certain dependence conditions. Then, we modify these conditions and we aim at constructing new random variables with low entropy satisfying the new conditions.

We extended these results in order to analyze the techniques for finding lower

bounds on the optimal information ratio, and we studied the behavior of these bounds when we add or delete subsets from an access structure. We studied bounds based on the Shannon inequalities, the Razborov rank measure, critical subfamilies, and submodular formal complexity measures. These bounds are used for other models of computation and information theoretic schemes, and so the results are useful in other areas.

In the information theoretic setting, another interesting problem is to know the effect of small changes in the dependence conditions. For instance, given an access structure, to study the change in the optimal information ratio if we allow some forbidden subsets to have a certain amount of information about the secret. In this case, we are dealing with non-perfect secret sharing schemes. Using access functions [18], we can quantify the knowledge about the secret with real numbers, and extend the optimal information ratio to a continuous domain [18]. Then, a natural open question is to know if the optimal information ratio is a continuous function.

References

[1] N. Alon and J. H. Spencer. *The Probabilistic Method*. John Wiley & Sons, 3rd edition, 2008.

[2] L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica* **19(3)** (1999) pp. 301–319.

[3] A. Beimel. Secret-Sharing Schemes: A Survey. *Coding and Cryptology, Third International Workshop, IWCC 2011, Lecture Notes in Comput. Sci.* **6639** (2011) 11–46.

[4] A. Beimel, A. Gál, M. Paterson. Lower Bounds for Monotone Span Programs. *36th Annual Symposium on Foundations of Computer Science - STOC*, pp. 674–681, 1995.

[5] A. Beimel, O. Farràs, Y. Mintz. Secret Sharing Schemes for Very Dense Graphs. *J. of Cryptology*, **29(2)** (2016) pp. 336–362.

[6] A. Beimel, O. Farràs, Y. Mintz, N. Peter. *Theory of Cryptography. TCC 2017. Lecture Notes in Comput. Sci.* **10678** (2017) pp. 394–423.

[7] A. Beimel, O. Farràs, N. Peter. Secret Sharing Schemes for Dense Forbidden Graphs. *Security and Cryptography for Networks, SCN 2016, Lecture Notes in Comput. Sci.* **9841** (2016) pp. 509–528.

[8] A. Beimel, I. Orlov. Secret Sharing and Non-Shannon Information Inequalities. *IEEE Trans. Inform. Theory* **57** (2011) pp. 5634–5649.

[9] M. Bellare, P. Rogaway. Robust computational secret sharing and a unified account of classical secret-sharing goals. *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007*, pp. 172–184, 2007.

[10] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology, CRYPTO 1988, Lecture Notes in Comput. Sci.*, **403** (1990) pp. 27–35.

[11] G. R. Blakley. Safeguarding cryptographic keys. In *1979 AFIPS National Computer Conference*, pp. 313–317, 1979.

[12] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.* **6** (1989) pp. 105–113.

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

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

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

[16] L. Csirmaz. Secret sharing on the d–dimensional cube. *Des. Codes Cryptogr.*, **74(3)** (2015) pp. 719–729.

[17] R. Cramer, I. Damgård, U. Maurer. General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme. *Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Comput. Sci.* **1807** (2000) pp. 316–334.

[18] O. Farràs, T. Hansen, T. Kaced, C. Padró. On the Information Ratio of Non-Perfect Secret Sharing Schemes. *Algorithmica* **79** (2017) pp. 987–1013.

[19] O. Farràs, J. Martí-Farré, and C. Padró. Ideal multipartite secret sharing schemes. *J. of Cryptology*, **25(1)** (2012) pp. 434–463.

[20] O. Farràs, J. R. Metcalf-Burton, C. Padró, L. Vázquez. On the Optimization of Bipartite Secret Sharing Schemes. *Des. Codes Cryptogr.* **63(2)** (2012) pp. 255–271.

[21] O. Farràs, J. Ribes-González, S. Ricci. Local Bounds for the Optimal Information Ratio of Secret Sharing Schemes. IACR Cryptology ePrint Archive 2016: 726 (2016)

[22] O. Farràs, J. Ribes-González, S. Ricci. Privacy-preserving Data Splitting: A Combinatorial Approach. arXiv:1801.05974 (2018)

[23] O. Farràs, T. Kaced, S. Martín, C. Padró. Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing. To appear in EUROCRYPT 2018.

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

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

[26] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Computational Complexity*, **10(4)** (2001) pp. 277–296.

[27] P. Frankl. Extremal Set Systems. *Handbook of Combinatorics, volume II,* Elsevier, Amsterdam, 1995, pp. 1293–1329.

[28] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pp. 89–98, 2006.

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

[30] M. Jha, S. Raskhodnikova. Testing and Reconstruction of Lipschitz Functions with Applications to Data Privacy *SIAM J. Comput.*, **42(2)** (2013) pp. 700–731.

[31] S. Jukna. *Boolean Function Complexity. Advances and Frontiers* Springer-Verlag, Berlin, 2012.

[32] M. Karchmer and A. Wigderson. On span programs. In *8th Structure in Complexity Theory*, pp. 102–111, 1993.

[33] I. Komargodski, M. Naor, E. Yogev. Secret-Sharing for NP. *Advances in Cryptology – ASIACRYPT 2014. Lecture Notes in Comput. Sci.* **8874** (2014) pp. 254–273.

[34] T. Liu, V. Vaikuntanathan, H. Wee. Conditional disclosure of secrets via non-linear reconstruction. *Advances in Cryptology – CRYPTO 2017. Lecture Notes in Comput. Sci.* **10401**, (2017) pp. 758–790.

[35] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) pp. 95–120.

[36] S. Martín, C. Padró, A. Yang. Secret Sharing, Rank Inequalities, and Information Inequalities. *IEEE Trans. Inform. Theory* **62** (2016) pp. 599–609.

[37] C. Padró. Lecture Notes in Secret Sharing. *Cryptology ePrint Archive* 2012/674.

[38] C. Padró, L. Vázquez, A. Yang. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Discrete Appl. Math.* **161** (2013) pp. 1072–1084.

[39] T. Pitassi, R. Robere. Lifting Nullstellensatz to Monotone Span Programs over any Field. *Electronic Colloquium on Computational Complexity (ECCC)* 165 (2017).

[40] A. A. Razborov. Applications of Matrix Methods to the Theory of Lower Bounds in Computational Complexity. *Combinatorica* **10 (1)** (1990) pp. 81–93.

[41] A. A. Razborov. On submodular complexity measures. In *Proceedings of the London Mathematical Society Symposium on Boolean Function Complexity*, pp. 76–83, 1992.

[42] R. Robere, T. Pitassi, B. Rossman, S. A. Cook, Exponential Lower bounds for Monotone Span Programs. *FOCS*, pp. 406–415, 2016.

[43] A. Schrijver. *Combinatorial Optimization. Polyhedra and Efficiency.* Springer-Verlag, Berlin, 2003.

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

[45] V. Vaikuntanathan, P. N. Vasudevan. Secret Sharing and Statistical Zero Knowledge *Advances in Cryptology – ASIACRYPT 2015. Lecture Notes in Comput. Sci.* **9452** (2015) pp. 656–680.

[46] I. Wegener. *The Complexity of Boolean Functions.* Wiley-Teubner, 1987.