Bounds on the Information Ratios of Secret Sharing Schemes for Close Access Structures

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

July 23, 2016

Abstract

The information ratio of a secret sharing scheme Σ measures the size of the largest share of the scheme, and is denoted by $\sigma(\Sigma)$. The optimal information ratio of an access structure Γ is the infimum of $\sigma(\Sigma)$ among all schemes Σ for Γ, and is denoted by $\sigma(\Gamma)$. The main result of this work is that for every two access structures Γ and Γ', $|\sigma(\Gamma) - \sigma(\Gamma')| \leq |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|$. 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 families 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, Monotone span program, Monotone Boolean formula.

1 Introduction

Secret sharing is 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 *qualified* if their shares determine the secret value, and *forbidden* if their shares do not contain any information on the secret value. The family of qualified subsets is monotone increasing, and it is called the *access structure* of the scheme. If every subset of participants is either qualified 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 [40] and Blakley [9] in 1979, and are used in many cryptographic applications such as secure multiparty computation, attribute-based

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. Oriol Farràs is supported through a Juan de la Cierva grant

encryption and distributed cryptography (see [2] 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 [27] 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 [8] 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 [8, 27, 31] 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 concrete values are known only for certain families of access structures, like particular families of multipartite access structures (e.g. [11, 20, 21]), access structures with a small number of participants (e.g. [36]), or access structures with small minimal sets (e.g. [16]). A common method to obtain bounds on 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 an access structure with n participants for which the optimal information ratio is $\Omega(n/\log(n))$. Currently, it is the best lower bound on the information ratio for an access structure.

Linear secret sharing schemes are equivalent to monotone span programs [2, 31]. This connection was very useful to extend bounds on the complexity of monotone span programs to bounds on the information ratio of the linear secret sharing schemes. Cook et al. [14] showed that there is an access structure that requires linear schemes of information ratio $2^{\Omega(n^{1/14}\log(n))}$. Previously, other superpolynomial lower bounds were presented, like [3].

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 [12] showed that the access structure of ideal secret sharing schemes determines a matroid. Conversely, linear matroids determine ideal access structures, but a little is known about 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. [20]. However, we lack of general criteria to determine if an access structure admits an efficient scheme. That, we lack of general criteria to determine if an access structure admits secret sharing scheme with information ratio at most r, for certain $r > 1$. Recent works provided interesting results on the characterization of access structures with efficient schemes for other models of secret sharing [32, 41].

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 whether 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 to understand the

limitations of secret sharing and the behavior of the optimal information ratio, as a function from the set of access structures to the set of 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. Given any secret sharing scheme Σ for Γ, we can construct a secret sharing scheme Σ' for Γ' that satisfies that $\sigma(\Sigma') \leq \sigma(\Sigma) + |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|$. Moreover, if Σ is linear, then Σ' is linear too. The construction relies on a combinatorial result that allows a description of Γ' as the union and the intersection of Γ and other access structures of a particular kind. Then, using an extension of the techniques of Benaloh and Leichter [8], 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, and the access structures that are close to access structures requiring large shares, also require large shares. This bound also has consequences on cryptographic applications 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, for similar policies, we can build attribute-based encryption schemes of similar complexity [26].

By taking advantage of the combinatorial nature of this result, we extend this bound to other models of computation like formulas, circuits, and span programs. We are able to bound the formula size, the circuit size, and the span program size for monotone Boolean formulas, obtaining analogous results. In order to understand this property, we also study the limitations of the techniques for finding lower bounds on the information ratio. We study the nature of the bounds based on the Shannon inequalities [15, 33], the Razborov's rank method [37], the subcritical families method [3], and submodular formal complexity measures. We study the behavior 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 [4]. They presented a method that, given a secret sharing scheme Σ for an access structure Γ and an access structure Γ' with $\Gamma' \subseteq \Gamma$ and $\min \Gamma' \subseteq \min \Gamma$, it provides a secret sharing scheme for 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. The results were improved in [5].

In this work, we also revise the techniques in [4] and we provide a general combinatorial formulation of a result in [4] that can be extended to other models of computation.

In Section 2 we define secret sharing, and in Section 3 we present the combinatorial results that are the basis of the main results in this work. Section 4 is dedicated to the main bound on the information ratio of secret sharing schemes. Sections 5 and 6 are dedicated to the study of the lower bounds on the information ratio. Finally, we present in Section 7 the results for formulas and circuits.

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 from [2]. For an introduction to secret sharing, see [2, 35], for example.

Definition 2.1 (Access Structure)**.** Let P be a set. A collection $\Gamma \subseteq \mathcal{P}(P)$ is *monotone* if $B \in \Gamma$ and $B \subseteq C \subseteq P$ implies $C \in \Gamma$. An *access structure* is a monotone collection $\Gamma \subseteq \mathcal{P}(P)$ of non-empty subsets of P. 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 $\Pi(s, r)_A$ the projection of $\Pi(s, r)$ to its A-entries.

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 $A \subseteq P$:

- 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 $k \in K$,

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

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

$$\Pr[\, \Pi(a, r)_A = (s_j)_{j \in A} \,] = \Pr[\, \Pi(b, r)_A = (s_j)_{j \in A} \,]. \tag{2}$$

In a secret sharing scheme, usually we consider that there is an additional player 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 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 surjective linear mapping.

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

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

and the *total information ratio* of Σ is

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

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

For an access structure Γ, we define the *optimal information ratio* $\sigma(\Gamma)$ as the infimum of the information ratio of the 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 finite field $\mathbb{F}$ we define $\lambda_{\mathbb{F},\ell}(\Gamma)$ and $\lambda^{\mathrm{T}}_{\mathbb{F},\ell}(\Gamma)$ as the infimum of the information ratios and total information ratios of the $(\mathbb{F}, \ell)$-linear secret sharing schemes for Γ, respectively.

3 Combinatorial results

This is a technical section in which we provide combinatorial results about the addition and deletion of subsets in access structures and in minimal access structures. These results will be used in the following sections to construct formulas, circuits and secret sharing schemes to obtain lower bounds on their complexity. 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 [25] 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 $\operatorname{dist}(\mathcal{B}, \mathcal{B}') = |\mathcal{B} \setminus \mathcal{B}'| + |\mathcal{B}' \setminus \mathcal{B}|$.

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 $\mathcal{B}^c = \mathcal{P}(P) \setminus \mathcal{B}$, and for every $i \in P$ we define $\mathcal{B}(i) = \{A \setminus \{i\} \,:\, i \in A \in \mathcal{B}\}$. The *degree* of $i \in P$ in $\mathcal{B}$, denoted by $\deg_i \mathcal{B}$, is defined by $|\mathcal{B}(i)|$, and the *degree* of $\mathcal{B}$ $\deg(\mathcal{B})$ is defined as the maximum of $\deg_i \mathcal{B}$ among $i \in P$. For every set $A \subseteq P$, we define the *closure* of a set A as $\operatorname{cl}(A) = \{A \cup B \,:\, B \subseteq P \setminus A\}$. We also define the *closure* of $\mathcal{B}$ as $\operatorname{cl}(\mathcal{B}) = \cup_{A \in \mathcal{B}} \operatorname{cl}(A)$. 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 $\operatorname{cl}(\mathcal{B}) = \mathcal{B}$. If Γ is an access structure, then $\operatorname{cl}(\min \Gamma) = \Gamma$ and Γ^c is monotone decreasing. For an access structure Γ on P, we define its *dual* as

$$\Gamma^* = \{P \setminus A \,:\, A \subseteq P,\, A \notin \Gamma\}.$$

The union and intersection of access structures, and the dual of an access structure are access structures as well. The minimal authorized subsets of Γ^* are in correspondence with the maximal subsets not in Γ and vice versa. That is, $\min \Gamma^* = \{P \setminus B \,:\, B \in \max \Gamma^c\}$ and $\max(\Gamma^{*c}) = \{P \setminus A \,:\, A \in \min \Gamma\}$. Hence $\Gamma^{**} = \Gamma$. For any two access structures Γ and Γ', $(\Gamma \cup \Gamma')^* = \{P \setminus A : A \notin \Gamma\} \cap \{P \setminus A : A \notin \Gamma'\} = \Gamma^* \cap \Gamma'^*$. Analogously, $(\Gamma \cap \Gamma')^* = \Gamma^* \cup \Gamma'^*$.

Now we define three parametrized families of access structures. As we show in the following sections, these access structures admit short formulas and efficient secret sharing schemes. For any $A \subseteq P$, we define the access structures

$$F_A = \{B \subseteq P \,:\, B \not\subseteq A\}, \qquad S_A = \{B \subseteq P \,:\, A \subsetneq B\}, \qquad T_A = \{B \subseteq P \,:\, A \subseteq B\}.$$

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 [25]. 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 $\min F_A = \{\{i\} \,:\, i \notin A\}$. Observe that $F_A = T^*_{P \setminus A}$.

3.1 Decomposition of Access Structures

Proposition 3.1 is the basis of the main results in this work, and Proposition 3.2 is a complementary result.

Proposition 3.1. *Let Γ, Γ' be two access structures on P. Then*

$$\Gamma' = \Big(\Gamma \cap \bigcap_{A \in \max(\Gamma \setminus \Gamma')} F_A\Big) \cup \bigcup_{A \in \min(\Gamma' \setminus \Gamma)} T_A.$$

Proof. Let $\Gamma'' = \Gamma \cap \Gamma'$. Since $\Gamma' = \Gamma'' \cup (\Gamma' \setminus \Gamma)$ and Γ' is monotone increasing,

$$\Gamma' = \mathrm{cl}(\Gamma') = \mathrm{cl}(\Gamma'') \cup \mathrm{cl}(\Gamma' \setminus \Gamma) = \Gamma'' \cup \bigcup_{A \in \Gamma' \setminus \Gamma} T_A = \Gamma'' \cup \bigcup_{A \in \min(\Gamma' \setminus \Gamma)} T_A.$$

We dedicate the rest of the proof to show that $\Gamma'' = \Gamma \cap \bigcap_{A \in \max(\Gamma \setminus \Gamma')} F_A$. By the properties of the dual of access structures described above,

$$\begin{aligned} \Gamma''^* &= (\Gamma \cap \Gamma')^* = \Gamma^* \cup \Gamma'^* = \Gamma^* \cup \{B \subseteq P : B \in \Gamma'^* \text{ and } B \notin \Gamma^*\} \\ &= \Gamma^* \cup \{P \setminus A : A \in \Gamma \setminus \Gamma'\}. \end{aligned}$$

Using that $\Gamma''^* = \mathrm{cl}(\Gamma''^*)$, we obtain that

$$\begin{aligned} \Gamma''^* &= \mathrm{cl}(\Gamma^*) \cup \mathrm{cl}(\{P \setminus A : A \in \Gamma \setminus \Gamma'\}) = \Gamma^* \cup \textstyle\bigcup_{A \in \Gamma \setminus \Gamma'} T_{P \setminus A} \\ &= \Gamma^* \cup \textstyle\bigcup_{A \in \max(\Gamma \setminus \Gamma')} T_{P \setminus A}. \end{aligned}$$

Therefore,

$$\Gamma'' = (\Gamma''^*)^* = \Gamma^{**} \cap \textstyle\bigcap_{A \in \max(\Gamma \setminus \Gamma')} T^*_{P \setminus A} = \Gamma \cap \textstyle\bigcap_{A \in \max(\Gamma \setminus \Gamma')} F_A.$$

□

Proposition 3.2. *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*

$$\Gamma' = \tilde{\Gamma} \cup \bigcup_{A \in \Gamma \setminus \Gamma'} \mathrm{cl}((\min S_A) \cap \Gamma') \cup \bigcup_{A \in \min(\Gamma' \setminus \Gamma)} T_A.$$

Proof. Let $\Gamma'' = \Gamma \cap \Gamma'$. As in the proof of Proposition 3.1, we can describe Γ' as $\Gamma' = \Gamma'' \cup \bigcup_{A \in \min(\Gamma' \setminus \Gamma)} T_A$. We dedicate the rest of the proof to show that $\Gamma'' = \tilde{\Gamma} \cup \bigcup_{A \in \Gamma \setminus \Gamma'} \mathrm{cl}((\min S_A) \cap \Gamma')$. Since $\Gamma = \min \Gamma \cup \bigcup_{A \in \Gamma} \min S_A$, we have that

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

Let $\mathcal{B}_1 = \Gamma \setminus \Gamma'$, $\mathcal{B}_2 = \min(\Gamma \cap \Gamma')$, and $\mathcal{B}_3 = \Gamma \cap \Gamma' \setminus \min(\Gamma \cap \Gamma')$. Observe that $\mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3 = \Gamma$. Let $\mathcal{A}_i = \bigcup_{A \in \mathcal{B}_i} \mathrm{cl}((\min S_A) \cap \Gamma')$ for $i = 1, 2, 3$. We claim that $\Gamma'' = \tilde{\Gamma} \cup \mathcal{A}_1$. First we prove that $\mathcal{A}_3 \subseteq \mathcal{A}_2$, and then we prove that $\mathcal{A}_2 \subseteq \tilde{\Gamma} \cup \mathcal{A}_1$.

For every $B \in \mathcal{B}_3$ there exists a set $B' \in \mathcal{B}_2$ satisfying $B \subseteq \mathrm{cl}(B')$. In this situation, $\mathrm{cl}(\min S_B) \subseteq \mathrm{cl}(\min S_{B'})$. Taking into account that $(\min S_A) \cap \Gamma' = \min S_A$ for every $A \in \mathcal{B}_2 \cup \mathcal{B}_3$, we obtain $\mathcal{A}_3 \subseteq \mathcal{A}_2$.

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 $A \in \min(\Gamma \cap \Gamma')$, $B \in \Gamma \setminus (\Gamma \cap \Gamma') = \Gamma \setminus \Gamma' = \mathcal{B}_1$. Then $\mathrm{cl}(\min S_A) \subseteq \mathrm{cl}(A) \subseteq \mathrm{cl}((\min S_B) \cap \Gamma')$. Therefore $\mathcal{A}_2 \subseteq \tilde{\Gamma} \cup \mathcal{A}_1$, which concludes the proof. □

3.2 Decomposition of Minimal Access Structures

In this section we consider the problem of modifying minimal access structures. Next we introduce a notion of covering that will be used to find useful descriptions of minimal access structures that are close.

Definition 3.3. 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 3.4. 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 a $(\{A\}, \mathcal{B} \setminus \{A\}) - covering$.

Next, we present in Lemma 3.5 a necessary and sufficient condition for the existence of coverings.

Lemma 3.5. *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. □

Beimel, Farràs and Mintz constructed efficient secret sharing schemes for very dense graphs [4]. The next lemma abstracts some of the techniques they used in [4, Lemma 5.2] and [4, Lemma 5.4]. We include its proof in the appendix.

Lemma 3.6. *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 $2^k k^k d^{k-1} \ln n$.*

This result has also consequences in graph theory, which corresponds to the case $k = 2$. It implies that every graph $G = (V, E)$ with $E \subseteq \binom{P}{2}$ admits an *equivalence cover* of degree $16d \ln n$, where d is the degree of $\binom{P}{2} \setminus E$ (see [4] for more details). The next proposition is the result we will use to construct formulas, circuits, and secret sharing schemes for access structures.

Proposition 3.7. *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. □

4 Secret Sharing Constructions

Benaloh and Leichter [8] presented a general construction for secret sharing. Given an access structure Γ, 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. Given a monotone Boolean formula computing f, it is possible to construct a linear secret sharing scheme for Γ by just translating ANDs and ORs into secret sharing operations.

In this section we extend the construction of Benaloh and Leichter by allowing the composition of any kind of schemes. Namely, we introduce the operations AND and OR of arbitrary secret sharing schemes. These operations represent two natural settings. 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 K, and then the r is shared by means of Σ_1 and $r+s$ is shared independently by means of Σ_2.

Before defining these operations, we present secret sharing schemes for the families of access structures F_A, S_A and T_A introduced in Section 3, for $A \subseteq P$, $A \neq \emptyset$. The secret sharing schemes we present are ideal and 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 ring. In the case that K is not a ring, we will consider the bijection between K and $\mathbb{Z}_m$, the construction will be defined over $\mathbb{Z}_m$. Without loss of generality, let $P = \{1, \ldots, n\}$ and $A = \{1, \ldots, t\}$ for some $t < n$.

- 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 $P \setminus A$. Consider $K_j = \emptyset$ 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 $\Pi(k)_j = k$ for $t+1 \leq j \leq n$.

- S_A: 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 $\Pi(k, r)_j = r_j$ for $1 \leq j \leq t$ and $\Pi(k, r)_j = k - \sum_{i=1}^{t} r_i$ 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 $\min \Gamma \subseteq \min S_A$.

- T_A: Since $\min T_A = \{A\}$, we just need to define the shares of the participants in A. Consider $K_j = K$ for $j \in A$, $K_j = \emptyset$ 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 $\Pi(k, r)_j = r_j$ for $1 \leq j < t$ and $\Pi(k, r)_t = k - \sum_{i=1}^{t-1} r_i$. For $A = P$, we can construct an analogous scheme.

Given a secret sharing scheme Σ on 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 $\min(\Gamma|_A) = \{B \in \min \Gamma : B \subseteq A\}$.

4.1 ANDs and ORs of Secret Sharing Schemes

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

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

for $i = 1, \ldots, n$; and μ is the product of μ^1 and μ^2. If a subset of P is authorized in Σ^1 or in Σ^2, then it is authorized in Σ. Moreover, the ones forbidden both in Σ^1 and Σ^2 are also forbidden in Σ. Therefore the access structure of $\Sigma_1 \vee \Sigma_2$ is the union of the access structures of Σ^1 and Σ^2.

Now we define the *AND* of Σ^1 and Σ^2. First 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

$$\Pi(k, r_1, r_2, r_3)_i = (\Pi^1(\Pi^3(k, r_3)_1, r_1)_i, \Pi^2(\Pi^3(k, r_3)_2, r_2)_i)$$

for $i = 1, \ldots, n$; and μ is the product of μ^1, μ^2, and μ^3. If a subset of P is authorized in both Σ^1 and Σ^2, then it is authorized in Σ. Moreover, the ones forbidden in Σ^1 or Σ^2 are also forbidden in Σ. Therefore the access structure of $\Sigma_1 \wedge \Sigma_2$ is the intersection of the access structures of Σ^1 and Σ^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. 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, $\sigma(\Gamma_1 \cup \Gamma_2), \sigma(\Gamma_1 \cap \Gamma_2) \leq \sigma(\Gamma_1) + \sigma(\Gamma_2)$ and $\sigma^{\mathrm{T}}(\Gamma_1 \cup \Gamma_2), \sigma^{\mathrm{T}}(\Gamma_1 \cap \Gamma_2) \leq \sigma^{\mathrm{T}}(\Gamma_1) + \sigma^{\mathrm{T}}(\Gamma_2)$. We have the analogous inequalities for the parameters $\lambda_{\mathbb{F},\ell}$ and $\lambda^{\mathrm{T}}_{\mathbb{F},\ell}$ for every finite field $\mathbb{F}$.

Now we present a well known construction for every access structure [27]. Consider the secret sharing schemes for the access structures T_A for every $A \in \min \Gamma$ and then we define Σ as the OR of these schemes. Then we obtain a scheme with $\sigma(\Sigma) = \deg(\min \Gamma)$. If we describe Γ as $(\Gamma^*)^* = (\cup_{A \in \max \Gamma^c} T_{P \setminus A})^* = \cap_{A \in \max \Gamma^c} F_A$ we obtain a description in terms of ANDs of access structures [27]. Then we can construct a secret sharing scheme Σ with $\sigma(\Sigma) = \deg(\max \Gamma^c)$.

Remark 4.1. All the results in this section can be adapted to other kinds of secret sharing schemes: statistical secret sharing schemes (see [2]), computational secret sharing schemes (see [7]), and perfect secret sharing schemes defined using the entropy function (see Definition B.1). The AND and OR operations defined above can be easily translated to these models, except for the latter, because it assumes that the secrets are chosen according to a specific probability distribution (see Section B for more details).

4.2 Secret Sharing Schemes for Close Access Structures

Theorem 4.2. *Let Γ, Γ' be two access structures. Then*

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

Proof. Let Σ be a secret sharing scheme for Γ. By Proposition 3.1, the access structure Γ' is realized by the secret sharing scheme

$$\Sigma' = \left(\Sigma \wedge \textstyle\bigwedge_{A \in \max(\Gamma \setminus \Gamma')} \Sigma_{F_A}\right) \vee \bigvee_{A \in \min(\Gamma' \setminus \Gamma)} \Sigma_{T_A},$$

where Σ_{F_A} and Σ_{T_A} are the ideal secret sharing schemes described above for F_A and T_A, respectively. Then $\sigma(\Sigma') \leq \sigma(\Sigma) + |\Gamma \setminus \Gamma'| + |\Gamma' \setminus \Gamma| = \sigma(\Sigma) + \operatorname{dist}(\Gamma, \Gamma')$. □

In the proof of the last theorem we construct a secret sharing scheme for Γ' using ANDs and ORs of a scheme for Γ and schemes for access structures of the kind T_A and F_A. Since these access structures admit ideal $(\mathbb{F}, 1)$-linear secret sharing schemes for any finite field $\mathbb{F}$ and for any A, if we have a $(\mathbb{F}, 1)$-linear secret sharing scheme for Γ then we obtain a $(\mathbb{F}, 1)$-linear secret sharing scheme for Γ'. We can also extend this result to $(\mathbb{F}, \ell)$-linear secret sharing schemes for every $\ell > 1$. Therefore, we obtain the following result.

Corollary 4.3. *Let Γ, Γ' be two access structures, and let $\mathbb{F}$ be a finite field. For every $\ell \geq 1$, $|\lambda_{\mathbb{F},\ell}(\Gamma) - \lambda_{\mathbb{F},\ell}(\Gamma')| \leq \operatorname{dist}(\Gamma, \Gamma')$*

In the next example we show that for distance equal to one, we cannot improve the general bounds in Theorem 4.2 and in Corollary 4.3. We present access structures Γ_n, Γ'_n and Γ''_n with $\operatorname{dist}(\Gamma''_n, \Gamma_n) = \operatorname{dist}(\Gamma''_n, \Gamma'_n) = 1$ and with $|\sigma(\Gamma''_n) - \sigma(\Gamma_n)| = |\sigma(\Gamma''_n) - \sigma(\Gamma'_n)| = 1 - 1/(n-2)$ for $n \geq 3$.

Example 4.4. Consider the access structures Γ_n and Γ'_n on $P = \{1, \ldots, n\}$ with $\min \Gamma_n = \{\{1, i\} : i > 1\}$ on $\min \Gamma'_n = \{\{1\}, \{2, \ldots, n\}\}$. 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 $\min \Gamma''_n = \{\{1, i\} : i > 1\} \cup \{\{2, \ldots, n\}\}$. 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 4.2 and Corollary 4.3 $\sigma(\Gamma''_n) \leq 2$ and $\lambda(\Gamma''_n) \leq 2$. It was proved in [21] that $\lambda(\Gamma''_n) = \sigma(\Gamma''_n) = 2 - 1/(n-2)$ for $n \geq 3$.

Proposition 4.5. *Let Γ, Γ' be two access structures. Let $\tilde{\Gamma}$ be the access structure with $\min \tilde{\Gamma} = (\min \Gamma) \cap \Gamma'$. Then*

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

Proof. Let Σ and $\tilde{\Sigma}$ be secret sharing schemes for Γ and $\tilde{\Gamma}$, respectively. We use Proposition 3.2 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 above for S_A we can construct an ideal secret sharing scheme $\operatorname{cl}((\min S_A) \cap \Gamma')$, which we call Σ''_A. Then the access structure Γ' is realized by the secret sharing scheme

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

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

In general, the bound presented in the previous proposition is not better than the one in Theorem 4.2. However, it is interesting because the construction is different and because it relates the optimal information ratio of Γ and $\tilde{\Gamma}$. The access structure $\tilde{\Gamma}$ may be of special interest. For example, if Γ and Γ' satisfy that $\min \Gamma$ and $\min \Gamma'$ are in $\binom{P}{k}$ for some k (like graph access structures), then $\tilde{\Gamma}$ is the access structure with $\min \tilde{\Gamma} = \min \Gamma \cap \min \Gamma' = \min \Gamma \setminus (\Gamma \setminus \Gamma')$. In this situation, the relation between $\sigma(\Gamma)$ and $\sigma(\tilde{\Gamma})$ has been studied in previous works as [4].

4.3 Secret Sharing Schemes for Access Structures with Close Minimal Access Structures

Now we present another decomposition of access structures that provide different bounds on the information ratio of access structures. In particular, these bounds are useful for access structures whose minimal access structures are close. The main result of this subsection is Theorem 4.9. The quality of the bounds in this theorem depends on the degree of a covering. In Lemma 3.6 we provide a bound on the degree of coverings. In Example 4.10 we show an access structure for which this technique provides an optimal secret sharing scheme.

Lemma 4.6. *Let Γ, Γ' be two access structures with $\min \Gamma \subseteq \min \Gamma'$. Let Σ be a secret sharing scheme for Γ. Then there exists a secret sharing scheme Σ' for Γ' with*

$$\sigma(\Sigma') \leq \sigma(\Sigma) + \deg(\min \Gamma' \setminus \min \Gamma) \text{ and } \sigma^T(\Sigma') \leq \sigma^T(\Sigma) + n \deg(\min \Gamma' \setminus \min \Gamma).$$

Proof. Let Σ be a secret sharing scheme for Γ and let Σ'' be the trivial scheme for $\min \Gamma' \setminus \min \Gamma$, that is, $\Sigma'' = \bigvee_{A \in \min \Gamma' \setminus \min \Gamma} \Sigma_{T_A}$. Then the scheme $\Sigma' = \Sigma \vee \Sigma''$ realizes Γ' and its information ratio and total information ratio hold the desired bounds. □

Lemma 4.7. *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*

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

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 $\Sigma|_B$ for $B \in \mathcal{C}$. By Proposition 3.7, Σ' realizes Γ'. In this scheme, each $i \in P$ receives $\deg_i(\mathcal{C})$ shares. Since $\deg_i(\mathcal{C}) \le d$, $\sigma(\Sigma') \le d\sigma(\Sigma)$, and $\sigma^{\mathrm{T}}(\Sigma') = \sum_{B\in\mathcal{C}} \sigma^{\mathrm{T}}(\Sigma|_B) \le d\sigma^{\mathrm{T}}(\Sigma)$. □

Example 4.8. Let Γ, Γ' be two access structures with $\mathrm{dist}(\min\Gamma, \min\Gamma') = 1$ and $\min\Gamma' \subseteq \min\Gamma$. As we saw in Example 3.4, 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 4.9. *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*

$$\sigma(\Gamma') \le d\sigma(\Gamma) + \deg(\min\Gamma' \setminus \min\Gamma), \text{and}$$

$$\sigma^T(\Gamma') \le d\sigma^T(\Gamma) + n\deg(\min\Gamma' \setminus \min\Gamma).$$

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 A.1. Given a secret sharing scheme Σ for Γ, there is a secret sharing scheme Σ'' for Γ'' with $\sigma(\Sigma'') \le d\sigma(\Sigma)$ by Lemma 4.7. Then using Lemma 4.6 we obtain a secret sharing scheme for Γ' of the desired total information ratio. □

Example 4.10. Let P be a set of $n = 2\ell+1$ participants for some $\ell > 0$, $P = \{a, b_0, \ldots, b_{\ell-1}, c_0, \ldots, c_{\ell-1}\}$. Let Γ be the 2-threshold access structure on P and let Γ' be the access structure on P with $\min\Gamma' = \{\{p,q\} \subseteq P\} \setminus \{\{a, c_i\} : 0 \le i \le \ell-1\}$. Then $\mathcal{C} = \{C_1, C_2\} = \{\{a, b_0, \ldots, b_{\ell-1}\}, \{b_0, \ldots, b_{\ell-1}, c_0, \ldots, c_{\ell-1}\}\}$ is a $(\min\Gamma \setminus \min\Gamma', \min\Gamma')$-covering. Using the construction described in Lemma 4.7, we obtain that $\Sigma' = \Sigma|_{C_1} \vee \Sigma|_{C_2}$ is a secret sharing scheme for Γ'. It satisfies $\sigma^{\mathrm{T}}(\Sigma') = \sigma^{\mathrm{T}}(\Sigma|_{C_1}) + \sigma^{\mathrm{T}}(\Sigma|_{C_2}) = \ell + 1 + 2\ell = 3\ell + 1$. By [4, Theorem 7.1], $\sigma^{\mathrm{T}}(\Gamma) \ge n + \ell = 3\ell + 1$. Therefore $\sigma^{\mathrm{T}}(\Gamma') = n + \ell$.

5 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, then we can compute the entropy of the secret and the shares. Then we can obtain bounds on the information ratio using the Shannon information inequalities and other information inequalities. For the sake of completeness, we present in Section B an alternative definition of secret sharing that defines the secret and the shares as random variables.

We study the lower bound on $\sigma(\Gamma)$ introduced by Martí-Farré and Padró [33], which is denoted by $\kappa(\Gamma)$. The main result in this section is Theorem 5.7, which shows a property of κ that is analogous to the one in Theorem 4.2. 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, 35] for more details).

We use notation introduced in [19, 34] to describe the polymatroids and the associated access structures. 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 $\Delta_F(Y{:}Z) = \Delta_F(Y{:}Z|\emptyset)$. To simplify the notation, for $x \in Q$, we will write $F(x)$ instead of $F(\{x\})$.

Definition 5.1. 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 $X \subseteq Q$, then we say that $\mathcal{S}$ is a *matroid*.

Proposition 5.2 ([19])**.** *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 $y, z \in Q \setminus X$.*

Now we describe the family of Γ-polymatroids for an access function Γ. These polymatroids are then used to compute $\kappa(\Gamma)$.

Definition 5.3. 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 for every $A \subseteq P$ satisfies the following properties.

- If $A \in \Gamma$ then $\Delta_f(p_0{:}A) = f(p_0)$.
- If $A \notin \Gamma$ then $\Delta_f(p_0{:}A) = 0$.

A Γ-polymatroid is said to be normalized if $f(p_0) = 1$.

Definition 5.4. For an access structure Γ on P we define $\kappa(\Gamma)$ as the infimum of $\sigma_0(\mathcal{S}) = \max_{p \in P} f(p)$ over all normalized Γ-polymatroids $\mathcal{S} = (Q, f)$.

Theorem 5.5 ([33])**.** *For every access structure Γ, $\sigma(\Gamma) \geq \kappa(\Gamma)$.*

The main result in this section is Theorem 5.7. Its proof is constructive, and requires the construction of polymatroids for the union and the intersection of access structures. Below we define the AND and OR operations on polymatroids associated to access structures. We show in Lemma 5.6 that these operations are well defined and that the resulting polymatroids are associated to the intersection and union of access structures, respectively. The proof is rather tedious and so it is moved to Section C.

Let $\mathcal{S}_1 = (Q, f_1)$ and $\mathcal{S}_2 = (Q, f_2)$ be two normalized polymatroids. We define the normalized polymatroids $\mathcal{S}_1 \vee \mathcal{S}_2 = (Q, f_1 \vee f_2)$ and $\mathcal{S}_1 \wedge \mathcal{S}_2 = (Q, f_1 \wedge f_2)$ as follows. For every $A \subseteq P$,

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

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

Lemma 5.6. *Let Γ_1 and Γ_2 be two access structures on P. Let $\mathcal{S}_1$ be a Γ_1-polymatorid and $\mathcal{S}_2$ a Γ_2-polymatorid. Then $\mathcal{S}_1 \vee \mathcal{S}_2$ is a $\Gamma_1 \cup \Gamma_2$-polymatroid, and $\mathcal{S}_1 \wedge \mathcal{S}_2$ is a $\Gamma_1 \cap \Gamma_2$-polymatroid.*

Theorem 5.7. *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 in Section C. It is constructive and uses the previous lemma. Roughly speaking, given a Γ-polymatroid, we compose it with polymatroids for other access structures and we obtain Γ'-polymatroid.

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 $\kappa(\Gamma) = 1$ [12, 33]. As a consequence of Theorem 5.7, the value of κ of access structures that are close to matroid ports is small. Martí-Farré and Padró [33] showed that if an access structure Γ is not a matroid port, then $\kappa(\Gamma) \geq 3/2$ (see [33] for more details). We can also say that if an access structure Γ is not a matroid port and is at distance one of a matroid port, then $3/2 \leq \kappa(\Gamma) \leq 2$. The access structures presented Example 4.4 have the property that σ and κ coincide. Hence, for access structures at a distance 1 we cannot improve this bound.

Csirmaz [15] found a family of access structures $\{\Gamma_n\}_{n\geq 0}$ with $\kappa(\Gamma_n) \geq O(n/\log n)$, but also proved that $\kappa(\Gamma) \leq n$ for every access structure Γ. Therefore, the previous theorem only provide useful bounds for access structures that are very close. However, it illustrates the nature of the Shannon inequalities restrictions with regard to the access structure. Recently, this method has been extended to non-Shannon inequalities, for instance in [6, 34]. For an access structure Γ on P and for a family of information inequalities or rank inequalities I, we define $\kappa_I(\Gamma)$ as the infimum of $\max_{x\in P} f(p)$ over all normalized Γ-polymatroids satisfying the restrictions of I. An interesting problem is to study whether κ_I behaves as κ.

6 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 [2] 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's rank measure [37] that is adapted to the context of secret sharing and access structures.

6.1 Razborov's Rank Measure

Let Γ be an access structure, and let $U, V \subseteq \mathcal{P}(P)$ be two families of subsets with $U \subseteq \Gamma$ and $V \subseteq \Gamma^c$. A (U, V)-*rectangle* is a Cartesian product $U_0 \times V_0$ for which $U_0 \subseteq U$ and $V_0 \subseteq V$. For each $i \in P$, define the 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 6.1 ([37])**.** Let $\Gamma \subseteq \mathcal{P}(P)$ 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 $\mathbb{F}$. The *rank measure of* Γ *with respect to* A is given by

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

and $\mu_A(\Gamma) = 0$ if $\text{rank}(A) = 0$.

Razborov [37] 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 7). Later, Gál [24] 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 6.2. *Let $\Gamma \subseteq \mathcal{P}(P)$ 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 $\mathbb{F}$. Then,*

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

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

Theorem 6.3. *Let $\Gamma, \Gamma' \subseteq \mathcal{P}(P)$ be access structures, $U \subseteq \Gamma$, $V \subseteq \Gamma^c$. Let $\mathbb{F}$ be a field and let A be a $|U| \times |V|$ matrix over $\mathbb{F}$. Then, there exist $U', V' \subseteq \mathcal{P}(P)$ with $U' \subseteq \Gamma'$, $V' \subseteq \Gamma'^c$ and a $|U'| \times |V'|$ matrix A' over $\mathbb{F}$ for which*

$$\mu_{A'}(\Gamma') \geq \mu_A(\Gamma) - \text{dist}(\Gamma, \Gamma').$$

Proof. Set $U' = U \cap \Gamma'$ and $V' = V \cap \Gamma'^c$, and let A' be the restriction of A to $|U'| \times |V'|$. Observe that $|U \backslash U'| \leq |\Gamma \backslash \Gamma'|$ because $U \backslash U' = U \backslash \Gamma'$ 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 entries of A indexed by $U \backslash U' \times V \backslash V'$, we have $\text{rank}(A) \leq \text{rank}(A') + |U \backslash U'| + |V \backslash V'|$. Therefore

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

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

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

□

Note that the behavior of the rank function bound is different from that of $\lambda^{\text{T}}_{\mathbb{F},1}$. If we extend the bound on Corollary 4.3 to λ^{T} we have that for every two access structures Γ and Γ', $|\lambda^{\text{T}}_{\mathbb{F},\ell}(\Gamma) - \lambda^{\text{T}}_{\mathbb{F},\ell}(\Gamma')| \leq n \cdot \text{dist}(\Gamma, \Gamma')$.

Recently, in [14], the rank function bound has been used to prove that there exists an access structure that requires linear schemes of information ratio $2^{\Omega(n^{1/14} \log(n))}$. Currently, this is the best lower bound for linear secret sharing schemes.

6.2 Subcritical families

The next technique provides lower bounds on the size of the shares for linear secret sharing schemes. It was introduced in [3].

Definition 6.4. 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 6.5. *Let $\mathcal{H}$ be a critical subfamily of an access structure Γ. Then $\lambda^T(\Gamma) \geq |\mathcal{H}|$.*

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

Lemma 6.6. *Let $\mathcal{H}$ be the critical subfamily of an access structure Γ. Let Γ' be access structures 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 $\mathcal{H}''$ of Γ' and Γ'', respectively, with $|\mathcal{H}'|, |\mathcal{H}''| \geq |\mathcal{H}| - \ell$.*

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

7 Formulas and Circuits

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 4.2 and 4.9 and Proposition 4.5 for the leafsize and the size of monotone Boolean functions. For an introduction to this area, see [30, 42], for example.

7.1 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 $\{0,1\}^n \to \mathcal{P}(P) : (x_i)_{i \in P} \mapsto \{i \in P : x_i = 1\}$. Then we define Γ_f as the collection of elements $A \in \mathcal{P}(P)$ such that $f(A) = 1$. A Boolean function f is *monotone* if and only if Γ_f is an access structure. In this case, set $\min f = \min \Gamma_f$. For two monotone Boolean functions f, f' on the same domain, we define the *distance* between f and f' as $\operatorname{dist}(f, f') = \operatorname{dist}(\Gamma_f, \Gamma'_f)$.

For a monotone Boolean function $f : \mathcal{P}(P) \to \{0,1\}$, we define the *dual* of f as the function $f^* : \mathcal{P}(P) \to \{0,1\}$ with $f^*(A) = \neg f(P \backslash A)$. Note that $\Gamma_{f^*} = (\Gamma_f)^*$. Therefore, f is monotone if and only if f^* is monotone.

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* to be the Boolean function $f|_B : \mathcal{P}(P) \to \{0,1\}$ characterized by $f|_B(A) = f(A \cap B)$. In other words, the restriction of the Boolean function $f : \{0,1\}^n \to \{0,1\}$ to the subset $B \subseteq P$ is

the Boolean function $f|_B : \{0,1\}^n \to \{0,1\}$ defined by $f|_B(x) = f(x')$, where $x'_i = x_i$ for all $i \in B$ and $x'_i = 0$ elsewhere. We have that $\Gamma_{f|_B} = \mathrm{cl}(\min f \cap \mathcal{P}(B))$.

If the domain of a Boolean function f is $\{0,1\}^n$, we say f is *fanin-n*. 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 circuits, formulas and some related concepts.

Definition 7.1. Let Ω be a set of Boolean functions. A *circuit S over Ω* is a sequence $(g_1, \ldots, g_m)$ of Boolean functions such that

- The first n Boolean functions are input variables, and
- for every other g_j, there exists $\Phi \in \Omega$ and $k_1, \ldots, k_{d_j} < j$ such that $g_j = \Phi(g_{k_1}, \ldots, g_{k_{d_j}})$.

A Boolean function g in a circuit is *fanout-r* if there exist r posterior functions that are computed using g. A *formula F over Ω* is a circuit over Ω whose fanout of functions is at most 1.

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

Let F_f and F_g be formulas computing monotone Boolean functions f and g, respectively. Then, $F_f \wedge F_g$ is a formula computing the Boolean function $h = f \wedge g = \max\{f, g\}$, and $\Gamma_h = \Gamma_f \cap \Gamma_g$. Similarly, $F_f \vee F_g$ is a formula computing the Boolean function $h' = f \vee g = \min\{f, g\}$, and $\Gamma_{h'} = \Gamma_f \cup \Gamma_g$. 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 $i \in B$. If F computes a function f, then $F|_B$ computes $f|_B$.

7.2 Bounds on the Size of Formulas and Circuits

The *size* (resp. *leafsize*) of a circuit (resp. formula) is defined as the number of non-input Boolean functions (resp. input variables) in it. If f is a Boolean function, we denote by $S(f)$ (resp. $S_+(f)$) the minimal size of a deMorgan (resp. monotone) circuit computing f. Similarly, we denote by $L(f)$ (resp. $L_+(f)$) the minimal leafsize of a deMorgan (resp. monotone) formula computing f. Since all results in this article concerning the complexity measure S and L hold verbatim for S_+ and L_+ respectively, we state them only for S and L.

We now present bounds as those in Theorems 4.2 and 4.9 and Proposition 4.5 for the leafsize and the size of monotone Boolean functions. The following proposition shows that similar monotone Boolean functions are close in size. The proofs of the following results are in Section D.

Proposition 7.2. *For every two monotone Boolean functions f and f',*

$$|L(f) - L(f')| \leq n \cdot \mathrm{dist}(f, f') \quad \textit{and} \quad |S(f) - S(f')| \leq n \cdot \mathrm{dist}(f, f').$$

Proposition 7.3. *Let f, f' be two monotone Boolean functions. Let $\tilde{f}$ be the monotone Boolean function with $\min \tilde{f} = \min f \cap \Gamma_{f'}$. Then*

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

Proposition 7.4. *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*

$$L(f') \leq d \cdot L(f) + n \cdot |\min f' \setminus \min f|, \textit{ and}$$
$$S(f') \leq d \cdot (S(f) + 1) + n \cdot |\min f' \setminus \min f| - 1.$$

7.3 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 every monotone Boolean functions f, g.

For every submodular formal complexity measure μ and for every monotone Boolean function f, $L(f) \geq \mu(f)$ [38]. See [30, 38] for more details about submodular formal complexity measures.

Proposition 7.5. *Let μ be a submodular formal complexity measure. Then for every two monotone Boolean functions f and f',*

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

The Razborov's rank measure μ_A in Section 6, described in terms of submodular Boolean functions, is also submodular [38]. However, the bound we obtained for μ_A for close access structures is much better than the one in the previous proposition. Notice that both λ^{T} and σ^{T} are not submodular functions (see Section C.1 for more details).

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 $\mu_{A'}(f')$. The difference $L(f) - L(f')$ can be much bigger than ℓ, but the difference $\mu_A(f) - \mu_{A'}(f')$ is at most ℓ.

References

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

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

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

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

[5] A. Beimel, O. Farràs, N. Peter. Secret Sharing Schemes for Dense Forbidden Graphs. *SCN 2016*. To appear.

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

[7] 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*,172–184, 2007.

[8] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology, CRYPTO 1988*, vol. 403 of *LNCS*, pages 27–35, 1990.

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

[10] C. Blundo, A. De Santis, R. de Simone, and U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptogr.*, 11(2):107–122, 1997.

[11] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

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

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

[14] S. A. Cook, T. Pitassi, R. Robere, B. Rossman. Exponential Lower bounds for Monotone Span Programs. *Electronic Colloquium on Computational Complexity*, Report No.64, 2016.

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

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

[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) 316–334.

[18] O. Farràs, T. Hansen, T. Kaced, C. Padró. Optimal Non-Perfect Uniform Secret Sharing Schemes. *Advances in Cryptology, CRYPTO 2014. Lecture Notes in Comput. Sci.* **8617** (2014) 217–234.

[19] O. Farràs, T. Hansen, T. Kaced, C. Padró. On the Information Ratio of Non-Perfect Secret Sharing Schemes. Available at https://eprint.iacr.org/2014/124.

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

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

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

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

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

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

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

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

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

[29] S. Jukna. On Graph Complexity. *Combinatorics, Probability & Computing* **15(6)**: (2006) 855–876.

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

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

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

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

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

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

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

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

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

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

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

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

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

A Proof of Lemma 3.6

In this section we provide a proof of Lemma 3.6. The main ideas of this proof are from the proof of [4, Lemma 5.4]. We need to introduce the following result, whose proof is direct, and the definition of a coloring of family of subsets.

Lemma A.1. *Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}(P)$. A $(\mathcal{B}_1, \mathcal{B}_2)$-covering is also a $(\mathcal{B}_1, \mathcal{B}'_2)$-covering for every $\mathcal{B}'_2 \subseteq \mathcal{B}_2$.*

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 $\mu(u) \neq \mu(v)$.

Proof of Lemma 3.6. Due to Lemma 3.5, 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 A.1, it is enough to restrict our proof to the case $\mathcal{B}_2 = \tilde{\mathcal{B}_1} = \binom{P}{k} \setminus \mathcal{B}_1$.

In order to construct a $(\mathcal{B}_1, \tilde{\mathcal{B}_1})$-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. If all the elements in a subset $A \subseteq P$ have the same color by μ, then $B \nsubseteq A$ 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 $\mathcal{C}_i = \{A \subseteq P : A \text{ is a maximal monochromatic subset in } \mu_i\}$. Now we show that $\mathcal{C} = \cup_{i=1}^{r} \mathcal{C}_i$ is a $(\mathcal{B}_1, \tilde{\mathcal{B}_1})$-covering with probability at least $1 - 1/(k!)$.

Let $A = \{v_1, \ldots, v_k\} \in \tilde{\mathcal{B}_1}$. 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 $P \setminus A$. We prove that conditioned on this coloring, the probability that A is monochromatic 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 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 $(\mathcal{B}_1, \tilde{\mathcal{B}_1})$-covering is less than $\binom{n}{k}/n^k \leq 1/k!$. In particular, such covering exists. □

B An Alternative Definition of Secret Sharing

In this section we present another definition of secret sharing. This definition and the one in Section 2 are equivalent (see [2]). In this definition, we assume that secrets are chosen in K according to a certain probability distribution μ'. Then the distribution scheme Σ and μ' determine a random variable S_i for every $i \in P$. For every $A = \{i_1, \ldots i_r\} \subseteq Q = P \cup \{p_0\}$, we call $S_A = S_{i_1} \times \ldots \times S_{i_r}$.

The Shannon entropy of the random variable S_A is denoted by $H(S_A)$. In addition, for such random variables, one can consider the *conditional entropy* $H(S_A|S_B) = H(S_{A \cup B}) - H(S_B)$, the *mutual information* $I(S_A{:}S_B) = H(S_A) - H(S_A|S_B)$, and the *conditional mutual information* $I(S_A{:}S_B|S_C) = H(S_A|S_C) - H(S_A|S_{B \cup C})$. For an introduction to information theory, see [13].

Definition B.1. Let K be a finite set of secrets, where $|K| \geq 2$. A distribution scheme (Π, μ) with domain of secrets K together with a random variable S_0 on K is a *secret sharing scheme* realizing an access structure Γ if the following requirements hold for every $A \subset P$:

- If $A \in \Gamma$ then $I(S_0{:}S_A) = H(S_0)$.
- If $A \notin \Gamma$ then $I(S_0{:}S_A) = 0$.

Definition 2.3 and Definition B.1 are equivalent, and so the access structure determined according to one definition coincides with the one determined according to the other definition. The access structure of a secret sharing scheme is independent of the distribution of the secrets. That is, if a scheme realizes an access structure with respect to one distribution on the secrets, then it realizes the access structure with respect to any other distribution with the same support (see [2] for more details).

The results in Section 4 can be extended to secret sharing schemes defined according to Definition B.1, but there are some details that have to be taken into account. It is not possible to perform the OR operation of two secret sharing schemes with different probability distributions on the secrets. Also, it is not possible to perform an AND of secret sharing schemes whose secret distribution is not uniform. If we restrict the study to the secret sharing schemes in which the secret is chosen according to the uniform probability distribution, then we can define ANDs and ORs in a straightforward way.

In the information theoretic context the size of the shares is measured in terms of the entropy of the secret and the shares by means of $\max_{i\in P} H(S_i)/H(S_0)$. If we suppose that the distribution of the secret is uniform on K, then $\log|K| = H(S_0)$. Then since $\log|S_i| \geq H(S_i)$ for every $i \in P$, for every secret sharing scheme Σ on P, $\sigma(\Sigma) \geq \max_{i\in P} H(S_i)/H(S_0)$.

C Proofs of Section 5

This section is dedicated to the proof of Lemma 5.6 and Theorem 5.7. First we present a technical lemma, whose proof is straightforward.

Lemma C.1. *Let $\mathcal{S} = (Q, h)$ be a normalized Γ-polymatroid for some access structure Γ. Then*

p1) $f(A \cup \{p_0\}) = f(A) + 1 - \Delta_f(p_0{:}A)$ *for every* $A \subseteq P$.

p2) $\Delta_f(p{:}p|A) = f(p \cup A) - f(A)$.

p3) $\Delta_f(p{:}A \cup \{q\}) \geq \Delta_f(p{:}A)$ *for every* $A \subseteq Q$, $p, q \in Q \setminus A$.

p4) $\Delta_f(p_0{:}A \cup \{p,q\}) + \Delta_f(p_0{:}A) - \Delta_f(p_0{:}A \cup \{p\}) - \Delta_f(p_0{:}A \cup \{q\}) = \Delta_f(p{:}q|A \cup \{p_0\}) - \Delta_f(p{:}q|A)$ *for every* $A \subseteq Q$, $p, q \in Q \setminus A$.

Proof of Lemma 5.6. Let $\mathcal{S}_1 = (Q, f_1)$ be a normalized Γ-polymatroid, and let $\mathcal{S}_2 = (Q, f_2)$ be a normalized Γ'-polymatroid. Let $\mathcal{S}_3 = \mathcal{S}_1 \vee \mathcal{S}_2$, $\mathcal{S}_4 = \mathcal{S}_1 \wedge \mathcal{S}_2$, $g = f_1 \vee f_2$, and $h = f_1 \wedge f_2$. First we prove that $\mathcal{S}_3$ and $\mathcal{S}_4$ are polymatroids. We use the characterization of polymatorid in Proposition 5.2 to prove it. Namely, we prove that $\Delta_g(p{:}q|A) \geq 0$ and $\Delta_h(p{:}q|A) \geq 0$ for every $p, q \in Q$ and $A \subseteq Q$. We divide the proof into different cases.

Let $A \subseteq P$ and let $\{p, q\} \subseteq P \setminus A$. By property p1) of Lemma C.1 we have $\Delta_g(p{:}p|A) \geq 0$ and $\Delta_h(p{:}p|A) \geq 0$.

g1)

$$\begin{aligned}\Delta_g(p{:}q|A) =& g(A\cup\{p\}) + g(A\cup\{q\}) - g(A\cup\{p,q\}) - g(A)\\ =& f_1(A\cup\{p\}) + f_2(A\cup\{p\}) + f_1(A\cup\{q\}) + f_2(A\cup\{q\})\\ & - f_1(A\cup\{p,q\}) - f_2(A\cup\{p,q\}) - f_1(A) - f_2(A)\\ & - \min\{\Delta_{f_1}(p_0{:}A\cup\{p\}), \Delta_{f_2}(p_0{:}A\cup\{p\})\}\\ & - \min\{\Delta_{f_1}(p_0{:}A\cup\{q\}), \Delta_{f_2}(p_0{:}A\cup\{q\})\}\\ & + \min\{\Delta_{f_1}(p_0{:}A\cup\{p,q\}), \Delta_{f_2}(p_0{:}A\cup\{p,q\})\}\\ & + \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\}\\ =& \Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) + a - b,\end{aligned}$$

where

- $a = \min\{\Delta_{f_1}(p_0{:}A\cup\{p,q\}), \Delta_{f_2}(p_0{:}A\cup\{p,q\})\} + \min\{\Delta_{f_1}(p_0{:}A),\ \Delta_{f_2}(p_0{:}\ A)\}$, and
- $b = \min\{\Delta_{f_1}(p_0{:}A\cup\{p\}), \Delta_{f_2}(p_0{:}A\cup\{p\})\} + \min\{\Delta_{f_1}(p_0{:}A\cup\{q\}),\ \Delta_{f_2}(p_0{:}A\cup\{q\})\}$.

If $a = 0$ then $\Delta_{f_1}(p_0{:}A\cup\{p,q\}) = 0$ or $\Delta_{f_2}(p_0{:}A\cup\{p,q\}) = 0$. By property p3) of Lemma C.1, it implies that $b = 0$. If $a = 2$ then $\Delta_{f_1}(p_0{:}A) = \Delta_{f_2}(p_0{:}\ A) = 1$, and so using the same property we obtain that $b = 2$.

Now suppose that $a < b$. The unique possible case is $a = 1$ and $b = 2$. In this case, there exists some $i \in \{1, 2\}$ for which $\Delta_{f_i}(p_0{:}A\cup\{p,q\}) = \Delta_{f_i}(p_0{:}A\cup\{p\}) = \Delta_{f_i}(p_0{:}A\cup\{q\}) = 1$ and $\Delta_{f_i}(p_0{:}A) = 0$. We have

$$a - b = \Delta_{f_i}(p_0{:}A\cup\{p,q\}) + \Delta_{f_i}(p_0{:}A) - \Delta_{f_i}(p_0{:}A\cup\{p\}) - \Delta_{f_i}(p_0{:}A\cup\{q\}),$$

which is equal to $\Delta_{f_i}(p{:}q|A\cup\{p_0\}) - \Delta_{f_i}(p{:}q|A)$ by property p4) of Lemma C.1. Hence $\Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) + a - b \geq 0$.

Therefore, we can conclude that$\Delta_g(p{:}q|A) \geq 0$.

h1) $\Delta_h(p{:}q|A) = \Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) \geq 0$.

Let $A \subseteq P$ and let $p \in P \setminus A$. By property p1) of Lemma C.1, $\Delta_g(p_0{:}p_0|A) \geq 0$ and $\Delta_h(p_0{:}p_0|A) \geq 0$.

g2)

$$\begin{aligned}\Delta_g(p{:}p_0|A) &= g(A\cup\{p\}) + g(A\cup\{p_0\}) - g(A\cup\{p,p_0\}) - g(A)\\ &= g(A\cup\{p\}) + g(A) + 1 - \Delta_g(p_0{:}A) - (g(A\cup\{p\}) + 1 - \Delta_g(p_0{:}A) + g(A))\\ &= \Delta_g(p_0{:}A\cup\{p\}) - \Delta_g(p_0{:}A)\\ &= \max\{\Delta_{f_1}(p_0{:}A\cup\{p\}), \Delta_{f_2}(p_0{:}A\cup\{p\})\} - \max\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\},\end{aligned}$$

which is nonnegative by property p3) of Lemma C.1.

h2)

$$\begin{aligned}\Delta_h(p{:}p_0|A) &= h(A\cup\{p\}) + h(A\cup\{p_0\}) - h(A\cup\{p,p_0\}) - h(A)\\ &= h(A\cup\{p\}) + h(A) + 1 - \Delta_h(p_0{:}A) - (h(A\cup\{p\}) + 1 - \Delta_h(p_0{:}A) + h(A))\\ &= \Delta_h(p_0{:}A\cup\{p\}) - \Delta_h(p_0{:}A)\\ &= \min\{\Delta_{f_1}(p_0{:}A\cup\{p\}), \Delta_{f_2}(p_0{:}A\cup\{p\})\} - \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\},\end{aligned}$$

which is non-negative by property p3) of Lemma C.1.

Let $A \subseteq P$ and let $\{p, q\} \subseteq P \setminus A$. By property p1) of Lemma C.1, $\Delta_g(p{:}p|A \cup \{p_0\}) \geq 0$ and $\Delta_h(p{:}p|A \cup \{p_0\}) \geq 0$.

g3)

$$\begin{aligned}
\Delta_g(p{:}q|A \cup \{p_0\}) &= g(A \cup \{p, p_0\}) + g(A \cup \{q, p_0\}) - g(A \cup \{p, q, p_0\}) - g(A \cup \{p\}) \\
&= g(A \cup \{p\}) + 1 - \Delta_g(p_0{:}A \cup \{p\}) \\
&+ g(A \cup \{q\}) + 1 - \Delta_g(p_0{:}A \cup \{q\}) \\
&- (g(A \cup \{p, q\}) + 1 - \Delta_g(p_0{:}A \cup \{p, q\})) \\
&- (g(A) + 1 - \Delta_g(p_0{:}A)) \\
&= g(A \cup \{p\}) + g(A \cup \{q\}) - g(A \cup \{p, q\}) - g(A) \\
&+ \Delta_g(p_0{:}A) + \Delta_g(p_0{:}A \cup \{p, q\}) \\
&- \Delta_g(p_0{:}A \cup \{p\}) - \Delta_g(p_0{:}A \cup \{q\}) \\
&= \Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) \\
&- (\Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) - \Delta_{f_1}(p{:}q|A \cup \{p_0\}) - \Delta_{f_2}(p{:}q|A \cup \{p_0\})) \\
&= \Delta_{f_1}(p{:}q|A \cup \{p_0\}) + \Delta_{f_2}(p{:}q|A \cup \{p_0\}) \\
&\geq 0.
\end{aligned}$$

h3)

$$\begin{aligned}
\Delta_h(p{:}q|A \cup \{p_0\}) &= h(A \cup \{p, p_0\}) + h(A \cup \{q, p_0\}) - h(A \cup \{p, q, p_0\}) - h(A \cup \{p\}) \\
&= h(A \cup \{p\}) + 1 - \Delta_h(p_0{:}A \cup \{p\}) \\
&+ h(A \cup \{q\}) + 1 - \Delta_h(p_0{:}A \cup \{q\}) \\
&- (h(A \cup \{p, q\}) + 1 - \Delta_h(p_0{:}A \cup \{p, q\})) \\
&- (h(A) + 1 - \Delta_h(p_0{:}A)) \\
&= \Delta_h(p{:}q|A) + \Delta_h(p_0{:}A \cup \{p, q\}) + \Delta_h(p_0{:}A) \\
&- \Delta_h(p_0{:}A \cup \{p\}) - \Delta_h(p_0{:}A \cup \{q\}) \\
&= \Delta_{f_1}(p{:}q|A) + \Delta_{f_2}(p{:}q|A) + a - b,
\end{aligned}$$

where

- $a = \min\{\Delta_{f_1}(p_0{:}A \cup \{p, q\}), \Delta_{f_2}(p_0{:}A \cup \{p, q\})\} + \min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}\ A)\}$, and
- $b = \min\{\Delta_{f_1}(p_0{:}A \cup \{p\}), \Delta_{f_2}(p_0{:}A \cup \{p\})\} + \min\{\Delta_{f_1}(p_0{:}A \cup \{q\}), \Delta_{f_2}(p_0{:}A \cup \{q\})\}$.

Note that $\Delta_h(p{:}q|A \cup \{p_0\}) = \Delta_g(p{:}q|A)$, and we already proved that $\Delta_g(p{:}q|A) \geq 0$ in g1).

It concludes the proof that $\mathcal{S}_3$ and $\mathcal{S}_4$ are polymatroids.

Now we prove that indeed $\mathcal{S}_3$ is a $\Gamma_1 \cup \Gamma_2$-polymatroid and $\mathcal{S}_4$ is a $\Gamma_1 \cap \Gamma_2$-polymatroid. A set $A \subseteq P$ is in $\Gamma_1 \cup \Gamma_2$ if and only if $\Delta_{f_1}(p_0{:}A) = 1$ or $\Delta_{f_2}(p_0{:}A) = 1$, that is, if and only if $\max\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\} = 1$. Hence $\mathcal{S}_3$ is a $\Gamma_1 \cup \Gamma_2$-polymatroid. A set $A \subseteq P$ is in $\Gamma_1 \cap \Gamma_2$ if and only if $\Delta_{f_1}(p_0{:}A) = 1$ and $\Delta_{f_2}(p_0{:}A) = 1$, that is, if and only if $\min\{\Delta_{f_1}(p_0{:}A), \Delta_{f_2}(p_0{:}A)\} = 1$. Hence $\mathcal{S}_4$ is a $\Gamma_1 \cap \Gamma_2$-polymatroid. □

Proof of Theorem 5.7. The proof of this theorem is analogous to the proof of Theorem 4.2. 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 S_A-polymatroid $\mathcal{S}_{S_A} = (Q, h)$

as the one with $h(B) = |B \cap A| + \min\{|B \cap (P \setminus A), 1\}$ for every $B \subseteq P$, and $\Delta_h(p_0 : B) = 1$ if and only if $A \subseteq B$ and $|B| < |A|$. Finally, we define 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 $h(B) = 0$ else, and $\Delta_h(p_0 : B) = 1$ if and only if $|B \cap (P \setminus A)| > 0$. Note that $\sigma_0(\mathcal{S}_{T_A}) = \sigma_0(\mathcal{S}_{S_A}) = \sigma_0(\mathcal{S}_{F_A}) = 1$.

Let $\mathcal{S}$ be a Γ-polymatroid. By Proposition 3.1, the following construction is a Γ'-polymatroid:

$$\mathcal{S}' = \left(\mathcal{S} \wedge \bigwedge_{A \in \max(\Gamma \setminus \Gamma')} \mathcal{S}_{F_A}\right) \vee \bigvee_{A \in \min(\Gamma' \setminus \Gamma)} \mathcal{S}_{T_A}.$$

Then $\kappa(\Gamma') \leq \kappa(\Gamma) + |\Gamma \setminus \Gamma'| + |\Gamma' \setminus \Gamma| = \kappa(\Gamma) + \mathrm{dist}(\Gamma, \Gamma')$. □

C.1 Submodularity

Example C.2. Consider the access structures Γ, Γ', Γ'', and Γ''' on $P = \{1, 2, 3, 4\}$ with $\min \Gamma = \binom{P}{2} \setminus \{\{1, 4\}\}$, $\min \Gamma' = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}\}$, $\min \Gamma'' = \binom{P}{2}$, and $\min \Gamma''' = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$. Observe that $\Gamma'' = \Gamma \cup \Gamma'$, and $\Gamma''' = \Gamma \cap \Gamma'$. It is known that $\sigma^{\mathrm{T}}(\Gamma) = \sigma^{\mathrm{T}}(\Gamma') = \sigma^{\mathrm{T}}(\Gamma'') = 4$ and $\sigma^{\mathrm{T}}(\Gamma''') = 5$, and so

$$\sigma^{\mathrm{T}}(\Gamma) + \sigma^{\mathrm{T}}(\Gamma') < \sigma^{\mathrm{T}}(\Gamma'') + \sigma^{\mathrm{T}}(\Gamma''') = \sigma^{\mathrm{T}}(\Gamma \cup \Gamma') + \sigma^{\mathrm{T}}(\Gamma \cap \Gamma').$$

The previous example shows access structures for which σ^{T} does not satisfy the submodularity property. For these access strucuctures, σ^{T} and κ^{T} (the bound defined analogously from κ) coincide, and they also coincide with $\lambda^{\mathrm{T}}_{\mathbb{F},\ell}$ for all ℓ and for all finite field $\mathbb{F}$ with $|\mathbb{F}| > 4$. Therefore κ^{T} and $\lambda^{\mathrm{T}}_{\mathbb{F},\ell}$ are not submodular either.

D Proofs of Section 7

In this section we show the proofs of the Propositions 7.2, 7.3 and 7.4. First 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 some Boolean function f to $B \in \mathcal{P}(P)$.

Note that $T_A = \cap_{i \in A} T_{\{i\}}$. Hence $\wedge_{i \in A} x_i$ is a formula for f_{T_A}, of size $|A|$. Since $F_A = (T_{P \setminus A})^*$, by using De Morgan's laws we get $f_{F_A} = f^*_{T_{P \setminus A}}$, and so $\vee_{i \in P \setminus A} x_i$ is a formula for f_{F_A} of size $n - |A|$. Since $S_A = T_A \cap F_A$, by using the two previous formulas we have that $(\wedge_{i \in A} x_i) \wedge \left(\vee_{i \in P \setminus A} x_i\right)$ is a formula for f_{S_A} of size 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) circuit (resp. formula) for f, and removing redundant input variables and Boolean functions, we get a circuit (resp. formula) for $f|_B$. Therefore, $S(f|_B) \leq S(f)$ and $L(f|_B) \leq L(f)$.

Proof of Proposition 7.2. Let F be a formula computing f. Using Proposition 3.1 with $\Gamma = \Gamma_f$ and $\Gamma' = \Gamma_{f'}$ we see that $F' = (F \wedge \bigwedge_{A \in \max(\Gamma \setminus \Gamma')} G_A) \vee \bigvee_{A \in \min(\Gamma' \setminus \Gamma)} H_A$ is a formula computing f', where G_A and H_A are the formulas for F_A and T_A described above, respectively. Hence,

$$\begin{aligned} L(f') &\leq L(f) + \textstyle\sum_{A \in \max(\Gamma \setminus \Gamma')} |P \setminus A| + \sum_{A \in \min(\Gamma' \setminus \Gamma)} |A| \\ &\leq L(f) + n \cdot \mathrm{dist}(\Gamma, \Gamma'). \end{aligned}$$

The result for S is analogous. □

Proof of Proposition 7.3. Using Proposition 3.2 with $\Gamma = \Gamma_f$, $\Gamma' = \Gamma_{f'}$ and $\tilde{\Gamma} = \Gamma_{\tilde{f}}$ we have

$$\Gamma' = \left(\tilde{\Gamma} \cup \bigcup_{A \in \Gamma' \setminus \Gamma} \mathrm{cl}\left(\min S_A \cap \Gamma'\right)\right) \cup \bigcup_{A \in \min(\Gamma \setminus \Gamma')} T_A.$$

Now note that $\mathrm{cl}\left(\min S_A \cap \Gamma'\right) = T_A \cap \bigcup_{i \notin A : A \cup \{i\} \in \Gamma'} T_{\{i\}}$, hence this access structure admits the formula $\left(\bigwedge_{i \in A} x_i\right) \wedge \bigvee_{i \notin A : A \cup \{i\} \in \Gamma'} x_i$, which has size at most n. The rest of the proof is analogous to the proof of Proposition 7.2. The result for S can be proved in a similar way. □

Proof of Proposition 7.4. Let $\mathcal{C}$ be a $(\min f \setminus \min f', \min f \cap \min f')$-covering, and take $A \in \min f$. In this case, $A \in \min f'$ if and only if there exists $B \in \mathcal{C}$ such that $A \in \mathcal{P}(B)$. Hence $\min f \cap \min f' = \bigcup_{B \in \mathcal{C}} (\min f \cap \mathcal{P}(B))$. Now, since $\min f' = (\min f \cap \min f') \cup (\min f' \setminus \min f)$,

$$\begin{aligned}
\Gamma_{f'} &= \mathrm{cl}(\min f') \\
&= \mathrm{cl}(\min f \cap \min f') \cup \mathrm{cl}(\min f' \setminus \min f) \\
&= \left(\bigcup_{B \in \mathcal{C}} \mathrm{cl}(\min f \cap \mathcal{P}(B))\right) \cup \bigcup_{A \in \min f' \setminus \min f} T_A \\
&= \left(\bigcup_{B \in \mathcal{C}} \Gamma_{f|_B}\right) \cup \bigcup_{A \in \min f' \setminus \min f} T_A.
\end{aligned}$$

Hence, if H_A is the formula for T_A described above, the formula

$$F' = \left(\bigvee_{B \in \mathcal{C}} F|_B\right) \vee \bigvee_{A \in \min f' \setminus \min f} G_A$$

computes f'. The result for S is analogous. □

Proof of Proposition 7.5. Let $\Gamma = \Gamma_f$ and $\Gamma = \Gamma_{f'}$. Let g and h be the monotone Boolean functions associated to the access structures $\cap_{A \in \max \Gamma \setminus \Gamma'} F_A$ and $\cup_{A \in \min \Gamma' \setminus \Gamma} T_A$, 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 $\mu(f_{F_A})$. Then

$$\begin{aligned}
\mu(g) + \mu(h) &= \mu(\cap_{A \in \max \Gamma \setminus \Gamma'} F_A) + \mu(\cup_{A \in \min \Gamma' \setminus \Gamma} T_A) \\
&\leq \textstyle\sum_{A \in \max(\Gamma \setminus \Gamma')} (n - |A|) + \sum_{A \in \min(\Gamma' \setminus \Gamma)} |A| \\
&\leq n \cdot |\max(\Gamma \setminus \Gamma')| + n \cdot |\min(\Gamma' \setminus \Gamma)| \\
&\leq n \cdot \mathrm{dist}(f, f').
\end{aligned}$$

□