Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing

Oriol Farràs[1], Tarik Kaced[2], Sebastià Martín[3], and Carles Padró[3]

[1]Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
[2]Sorbonne Université, LIP6, Paris, France
[3]Universitat Politècnica de Catalunya, Barcelona, Spain

November 25, 2019

Abstract

We present a new improvement in the linear programming technique to derive lower bounds on the information ratio of secret sharing schemes. We obtain non-Shannon-type bounds without using information inequalities explicitly. Our new technique makes it possible to determine the optimal information ratio of linear secret sharing schemes for all access structures on 5 participants and all graph-based access structures on 6 participants. In addition, new lower bounds are presented also for some small matroid ports and, in particular, the optimal information ratios of the linear secret sharing schemes for the ports of the Vamos matroid are determined.

Key words. Secret sharing, Information inequalities, Rank inequalities, Common information, Linear Programming.

1 Introduction

Linear programming involving information inequalities has been extensively used in different kinds of information theoretic problems. An early instance is the verification of Shannon information inequalities [66], and we find more examples in secret sharing [15, 55], network coding [64, 67], and other topics [65].

In this work, we present a new improvement of the linear programming technique in the search for lower bounds on the information ratio of secret sharing schemes. Namely, instead of known non-Shannon information inequalities, we propose to use constraints based on the properties from which those inequalities are deduced.

Secret sharing, which was independently introduced by Shamir [61] and Blakley [9], is a very useful tool that appears as a component in many different kinds of cryptographic protocols. The reader is referred to [4] for a survey on secret sharing and its applications. In a *secret sharing scheme*, a *secret value* is distributed into *shares* among a set of *participants* in such a way that

Oriol Farràs is supported by the Spanish Government through TIN2014-57364-C2-1-R and by the Catalan government through 2017SGR-705. Tarik Kaced acknowledges the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-16-CE23-0016-01 (project PAMELA). Sebastià Martín and Carles Padró are supported by Spanish Government through MTM2016-77213-R.

only the *qualified sets* of participants can recover the secret value. This work deals exclusively with *unconditionally secure* and *perfect* secret sharing schemes, in which the shares from any unqualified set do not provide any information on the secret value. In this case, the family of qualified sets of participants is called the *access structure* of the scheme.

In a *linear secret sharing scheme*, the secret and the shares are vectors over some finite field, and both the computation of the shares and the recovering of the secret are performed by linear maps. Because of their homomorphic properties, linear schemes are used in many applications of secret sharing. Moreover, most of the known constructions of secret sharing schemes yield linear schemes.

The *information ratio* of a secret sharing scheme is the ratio between the length of the shares and the length of the secret. The optimization of this parameter, both for linear and general secret sharing schemes, has attracted a lot of attention. This problem has been analyzed for several families of access structures. For example, access structures defined by graphs [5, 10, 12, 16, 18, 20, 30, 32], access structures on a small number of participants [20, 30, 31, 32, 39, 55, 62], bipartite access structures [25, 54], the ones having few minimal qualified sets [33, 46, 48], or ports of non-representable matroids [7, 47, 51, 55].

That optimization problem is related to the search for asymptotic lower bounds on the length of the shares, which is one of the main open problems in secret sharing. The reader is referred to the survey by Beimel [4] for more information about this topic. For *linear* secret sharing schemes, building up on the superpolynomial lower bounds in [3, 6], exponential lower bounds have been proved recently [56, 58]. Nevertheless, for the general case, no proof for the existence of access structures requiring shares of superpolynomial size has been found. Moreover, the best of the known lower bounds is the one given by Csirmaz [14, 15], who presented a family of access structures on an arbitrary number n of participants whose optimal information ratio is $\Omega(n/\log n)$.

Almost all known lower bounds on the optimal information ratio have been obtained by the same method, which is called here the *linear programming (LP) technique*. In particular, the asymptotic lower bound found by Csirmaz [14, 15] and most of the lower bounds for the aforementioned families of access structures. The LP-technique is based on the fact, pointed out by Karnin, Greene and Hellman [42], that a secret sharing scheme can be defined as a collection of random variables such that their joint entropies satisfy certain constraints derived from the access structure.

The technique was first used by Capocelli, De Santis, Gargano and Vaccaro [12]. In particular, they presented the first examples of access structures with optimal information ratio strictly greater than 1. Csirmaz [15] refined the method by introducing some abstraction revealing its combinatorial nature. This was achieved by using the connection between Shannon entropies and polymatroids discovered by Fujishige [26, 27]. The lower bounds on the optimal information ratio that can be obtained by using that connection between Shannon entropies and polymatroids or, equivalently, by using only Shannon information inequalities are called here *Shannon-type* lower bounds. The known exact values of the optimal information ratio have been determined by finding, for each of the corresponding access structures, both a Shannon-type lower bound and a linear secret sharing scheme whose information ratio equals that bound.

A further improvement, which was first applied in [7], consists in adding to the game constraints that cannot be derived from Shannon information inequalities. Specifically, the so-called *non-Shannon information inequalities* and *non-Shannon rank inequalities*. The former provide lower bounds for the general case, while the bounds derived from the latter apply to linear secret schemes. That addition made it possible to find several new lower bounds [7, 16, 51, 55] and also the first examples of access structures whose optimal information ratios are strictly greater than any Shannon-type lower bound [7], namely the ports of the Vamos matroid.

Finally, Metcalf-Burton [51] and Padró, Vázquez and Yang [55] realized that the method consists of finding lower bounds on the solutions of certain linear programming problems, which can be solved if the number of participants is small. In particular, the best Shannon-type lower bound for any given access structure is the optimal value of a certain linear programming problem. Again, new lower bounds for a number of access structures [25, 48, 51, 55] were obtained as a consequence of that improvement.

Some limitations of the LP-technique in the search for asymptotic lower bounds have been found. Namely, the best lower bound that can be obtained by using all information inequalities that were known at the beginning of this decade is linear in the number of participants [8, 15], while at most polynomial lower bounds can be found by using all known or unknown inequalities on a bounded number of variables [49].

Summarizing, while the LP-technique has important limitations when trying to find asymptotic lower bounds, it has been very useful in the search for lower bounds for finite and infinite families of access structures, providing in many cases tight bounds. More details about the LP-technique and its application are discussed in Section 2.

Yet another improvement to the LP-technique is presented in this work. Instead of using the known non-Shannon information and rank inequalities, we use the properties from which most of them have been derived. Specifically, most of the known non-Shannon information inequalities are obtained by using the *copy lemma* [22, 69] or the *Ahlswede-Körner lemma* [1, 2, 41, 45]. These two techniques to infer information inequalities are compared in [41]. All known non-Shannon rank inequalities, which provide lower bounds on the information ratio of *linear* secret sharing schemes, are inferred from the *common information property* [23]. We derive from the Ahlswede-Körner lemma and the common information property some constraints to be added to the linear programming problems that are used to find lower bounds. Inspired by our results, Gürpinar and Romashchenko [35] used the copy lemma in a similar way.

The bounds that are obtained from the Ahlswede-Körner lemma apply to general secret sharing schemes, while the ones computed with the common information property apply to linear schemes and also to the more general class of *abelian* secret sharing schemes, which are based on homomorphisms between finite abelian groups. Jafari and Khazaei [40] recently proved that, for some access structures, abelian schemes have better information ratio than the linear ones.

We applied that improvement to several access structures on a small number of players and we found new lower bounds that could not be found before by using the known information and rank inequalities. Specifically, the access structures on five participants, the graph-based access structures on six participants, and some ports of non-representable matroids have been the testbeds for our improvement on the LP-technique.

Jackson and Martin [39] determined the optimal information ratios of most of the access structures on five participants. The use of computers to solve the corresponding linear programming problems provided better Shannon-type lower bounds for some of the unsolved cases [55]. In addition, constructions of linear secret sharing schemes were presented in [31] improving some upper bounds. After those developments, only eight cases remained unsolved. Moreover, the values of the optimal information ratios for all solved cases were determined by a linear secret sharing scheme matching a Shannon-type lower bound. The negative result in [55, Proposition 7.1] clearly indicated that some of the open cases could not be solved in that way. Nevertheless, adding non-Shannon information and rank inequalities to the linear programs did not produce any new lower bound [55]. In contrast, our enhanced LP-technique provides better lower bounds for those unsolved cases, which are tight for *linear* secret sharing schemes. In particular, the optimal information ratio of linear secret sharing schemes is now determined for every access structure on five participants. Even though we present new lower bounds, some

values are still unknown for general schemes. So, we partially concluded the project initiated by Jackson and Martin in [39]. Moreover, we found the smallest examples of access structures for which the optimal information ratio does not coincide with the best Shannon-type lower bound.

A similar project was undertaken by van Dijk [20] for graph-based access structures on six participants, that is, access structures whose minimal qualified sets have exactly two participants. Most of the cases were solved in the initial work [20], and several advances were presented subsequently [13, 30, 32, 44, 55]. At this point, only nine cases remained unsolved. We have been able to find for them new lower bounds for linear schemes by using our enhanced LP-technique. Once our new lower bounds were made public, Gharahi and Khazaei [34] presented constructions of linear secret sharing schemes proving that they are tight. Therefore, our results made it possible to determine the optimal information rate of linear secret sharing schemes for all graph-based access structures on six participants.

In addition, we present new lower bounds for access structures with four minimal qualified sets on six participants [33, 48] and for the ports of four non-representable matroids on eight points. In particular, we determine the optimal information ratio of linear schemes for the ports of the Vamos matroid and the matroid Q_8. Our bound on the optimal information ratio for one of the ports of the Vamos matroid has been improved in [35] by using the copy lemma instead of the Ahlswede-Körner lemma.

All the lower bounds that are presented in this paper have been found by solving linear programming problems with conveniently chosen additional constraints derived from the common information property and the Ahlswede-Körner lemma. Since the number of variables and constraints is exponential in the number of participants, this can be done only for access structures on small sets. However, several lower bounds for infinite families of access structures have been obtained by using the LP-technique without solving linear programming problems [10, 15, 17, 18, 54]. Nevertheless, a better understanding of those tools is needed to apply our improvement of the LP-technique in a similar way. Since the known limitations of the LP-technique do not imply the contrary, it may be even possible to improve Csirmaz's [14, 15] asymptotic lower bound $\Omega(n/\log n)$.

The paper is organized as follows. A detailed discussion on the LP-technique is given in Section 2. Our improvement on the method is described in Section 3. The new lower bounds that have been obtained by applying our technique are presented in Section 5. A variant of the common information property and its dual are introduced in Section 4. Constructions of linear secret sharing schemes that are used to prove the tightness of some of those bounds are given in Section 6. We conclude the paper in Section 7 with some open problems and suggestions for future work.

2 Lower Bounds in Secret Sharing from Linear Programming

We begin by introducing some notation. For a finite set Q, we use $\mathcal{P}(Q)$ to denote its *power set*, that is, the set of all subsets of Q. We use a compact notation for set unions, that is, we write XY for $X \cup Y$ and Xy for $X \cup \{y\}$. In addition, we write $X \setminus Y$ for the set difference and $X \setminus x$ for $X \setminus \{x\}$.

2.1 Entropic and Linear Polymatroids

Only discrete random variables are considered in this paper. For a finite set Q, consider a random vector $(S_x)_{x\in Q}$. For every $X \subseteq Q$, we use S_X to denote the subvector $(S_x)_{x\in X}$, and

$H(S_X)$ will denote its Shannon entropy. Given three random variables $(S_i)_{i\in\{1,2,3\}}$, the *entropy of S_1 conditioned on S_2* is

$$H(S_1|S_2) = H(S_{12}) - H(S_2),$$

the *mutual information* of S_1 and S_2 is

$$I(S_1{:}S_2) = H(S_1) - H(S_1|S_2) = H(S_1) + H(S_2) - H(S_{12})$$

and, finally, the *conditional mutual information* is defined by

$$I(S_1{:}S_2|S_3) = H(S_1|S_3) - H(S_1|S_{23}) = H(S_{13}) + H(S_{23}) - H(S_{123}) - H(S_3).$$

A fundamental fact about Shannon entropy is that the conditional mutual information is always nonnegative, and this implies the following connection between Shannon entropy and polymatroids, which was first described by Fujishige [26, 27].

Definition 2.1. A *polymatroid* is a pair (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.

(P1) $f(\emptyset) = 0$.

(P2) f is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $f(X) \leq f(Y)$.

(P3) f is *submodular*: $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y)$ for every $X, Y \subseteq Q$.

A polymatroid is called *integer* if its rank function is integer-valued. If $\mathcal{S} = (Q, f)$ is a polymatroid and α is a positive real number, then $(Q, \alpha f)$ is a polymatroid too, which is called a *multiple* of $\mathcal{S}$.

Theorem 2.2 (Fujishige [26, 27])**.** *Let $(S_x)_{x\in Q}$ be a random vector. Consider the mapping $h\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(X) = H(S_X)$ if $\emptyset \neq X \subseteq Q$. Then h is the rank function of a polymatroid with ground set Q.*

Definition 2.3. The polymatroids that can be defined from a random vector as in Theorem 2.2 are called *entropic*. Consider a field $\mathbb{K}$, a vector space V with finite dimension over $\mathbb{K}$ and a collection $(V_x)_{x\in Q}$ of vector subspaces of V. It is clear from basic linear algebra that the map f defined by $f(X) = \dim \sum_{x\in X} V_x$ for every $X \subseteq Q$ is the rank function of a polymatroid. Every such polymatroid is said to be $\mathbb{K}$-*linear*.

Because of the connection given in Theorem 2.2, if f is the rank function of a polymatroid, we use the notation

$$f(Y{:}Z|X) = f(XY) + f(XZ) - f(XYZ) - f(X)$$

and, in particular, $f(Y{:}Z) = f(Y{:}Z|\emptyset) = f(Y) + f(Z) - f(YZ)$ and $f(Y|X) = f(Y{:}Y|X) = f(XY) - f(X)$ for every subsets X, Y, Z of the ground set.

We discuss in the following the well known connection between entropic and linear polymatroids, as described in [36]. Let $\mathbb{K}$ be a finite field and V a vector space with finite dimension over $\mathbb{K}$. Let S be the random variable determined by the uniform probability distribution on the dual space V^*. For every vector subspace $W \subseteq V$, the restriction of S to W determines a random variable $S|_W$ that is uniformly distributed on its support W^*, and hence $H(S|_W) = \log|\mathbb{K}| \dim W^* = \log|\mathbb{K}| \dim W$. Let $(V_x)_{x\in Q}$ be a collection of subspaces of V. For

every $X \subseteq Q$, we notate $V_X = \sum_{x \in X} V_x$. This collection of subspaces determines the $\mathbb{K}$-*linear random vector* $(S_x)_{x \in Q} = (S|_{V_x})_{x \in Q}$. Observe that $S_X = S|_{V_X}$ for every $X \subseteq Q$, and hence

$$H(S_X) = \log |\mathbb{K}| \dim V_X = \log |\mathbb{K}| \dim \sum_{x \in X} V_x.$$

This implies that the $\mathbb{K}$-linear polymatroid determined by the collection of subspaces $(V_x)_{x \in Q}$ is a multiple of the entropic polymatroid defined by the $\mathbb{K}$-linear random vector $(S_x)_{x \in Q} = (S|_{V_x})_{x \in Q}$. By taking also into account that every linear polymatroid admits a linear representation over some finite field [23, 57], from this discussion we can conclude the well known fact that every linear polymatroid is the multiple of an entropic polymatroid.

A more general class of random vectors can be described in terms of abelian groups. Consider a finite abelian group G and a collection $(H_x)_{x \in Q}$ of subgroups of G. For every $X \subseteq Q$, put $H_X = \bigcap_{x \in X} H_x$. The uniform probability distribution on G and the projections $\pi_x \colon G \to G/H_x$ determine an *abelian random vector* $(S_x)_{x \in X}$. Clearly, $H(S_X) = \log |G| - \log |H_X|$ for every $X \subseteq Q$. Linear random vectors are abelian. Indeed, for a vector space V and a collection $(V_x)_{x \in Q}$ of vector subspaces, take $G = V^*$ and $H_x = V_x^\perp = \{\alpha \in V^* \,:\, \alpha(V_x) = \{0\}\}$.

2.2 Secret Sharing

Definition 2.4. Let P be a set of *participants*. An *access structure* Γ on P is a *monotone increasing* family of subsets of P, that is, if $A \subseteq B \subseteq P$ and $A \in \Gamma$, then $B \in \Gamma$. The members of Γ are the *qualified sets* of the structure. An access structure is determined by the family $\min \Gamma$ of its *minimal qualified sets*. A participant is *redundant* in an access structure if it is not in any minimal qualified set. All access structures in this paper are assumed to have no redundant participants. The *dual* Γ^* of an access structure Γ on P is formed by the sets $A \subseteq P$ such that its complement $P \smallsetminus A$ is not in Γ.

Definition 2.5. Let Γ be an access structure on a set of *participants* P. Consider a special participant $p_o \notin P$, which is usually called *dealer*, and the set $Q = Pp_o$. A *secret sharing scheme* on P with access structure Γ is a random vector $\Sigma = (S_x)_{x \in Q}$ such that the following properties are satisfied.

1. $H(S_{p_o}) > 0$.
2. If $A \in \Gamma$, then $H(S_{p_o}|S_A) = 0$.
3. If $A \notin \Gamma$, then $H(S_{p_o}|S_A) = H(S_{p_o})$.

The random variable S_{p_o} corresponds to the *secret value*, while the *shares* received by the participants are given by the random variables S_x with $x \in P$. Condition 2 implies that the shares from a qualified set determine the secret value while, by Condition 3, the shares from an unqualified set and the secret value are independent.

Definition 2.6. Let $\mathbb{K}$ be a finite field. A secret sharing scheme $\Sigma = (S_x)_{x \in Q}$ is $\mathbb{K}$-*linear* or, respectively, *abelian* if it is a is $\mathbb{K}$-linear or, respectively, abelian random vector.

Definition 2.7. The *information ratio* $\sigma(\Sigma)$ of the secret sharing scheme Σ is

$$\sigma(\Sigma) = \max_{x \in P} \frac{H(S_x)}{H(S_{p_o})}$$

and its *average information ratio* $\widetilde{\sigma}(\Sigma)$ is

$$\widetilde{\sigma}(\Sigma) = \frac{1}{n} \sum_{x \in P} \frac{H(S_x)}{H(S_{p_o})}.$$

Definition 2.8. The *optimal information ratio* $\sigma(\Gamma)$ of an access structure Γ is the infimum of the information ratios of all secret sharing schemes for Γ. The *optimal average information ratio* $\widetilde{\sigma}(\Gamma)$ is defined analogously. The values $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ are defined by restricting the optimization to *linear* secret sharing schemes.

2.3 Lower Bounds from Shannon Information Inequalities

We describe next how to find linear programming problems whose optimal values are lower bounds on those parameters. Let Γ be an access structure on a set P and take, as usual, $Q = Pp_o$. Given a secret sharing scheme $\Sigma = (S_x)_{x\in Q}$ with access structure Γ, consider the entropic polymatroid (Q, h) determined by the random vector $(S_x)_{x\in Q}$, that is, $h(X) = H(S_X)$ for every $X \subseteq Q$. Take $\alpha = 1/h(p_o)$ and the polymatroid (Q, f) with $f = \alpha h$. The rank function f can be seen as a vector $(f(X))_{X\subseteq Q} \in \mathbb{R}^{\mathcal{P}(Q)}$ that satisfies the linear constraints

(N) $f(p_o) = 1$,

(Γ1) $f(Xp_o) = f(X)$ for every $X \subseteq P$ with $X \in \Gamma$,

(Γ2) $f(Xp_o) = f(X) + 1$ for every $X \subseteq P$ with $X \notin \Gamma$,

and also the polymatroid axioms (P1)–(P3) in Definition 2.1. Observe that constraints (Γ1), (Γ2) are derived from the chosen access structure Γ. Constraints (P1)–(P3) are equivalent to the so-called *Shannon information inequalities*, that is, the ones implied by the fact that the conditional mutual information is nonnegative. Therefore, the vector f is a feasible solution of Linear Programming Problem 2.9.

Linear Programming Problem 2.9. The optimal value of this linear programming problem is, by definition, $\widetilde{\kappa}(\Gamma)$:

$$\begin{aligned} \text{Minimize} \quad & (1/n)\sum_{x\in P} f(x) \\ \text{subject to} \quad & (\text{N}), (\Gamma1), (\Gamma2), (\text{P1}), (\text{P2}), (\text{P3}) \end{aligned}$$

Since this applies to every secret sharing scheme Σ with access structure Γ and the objective function equals $\widetilde{\sigma}(\Sigma)$, the optimal value $\widetilde{\kappa}(\Gamma)$ of this linear programming problem is a lower bound on $\widetilde{\sigma}(\Gamma)$. Similarly, a lower bound on $\sigma(\Gamma)$ is provided by the optimal value $\kappa(\Gamma)$ of the Linear Programming Problem 2.10.

Linear Programming Problem 2.10. The optimal value of this linear programming problem is, by definition, $\kappa(\Gamma)$:

$$\begin{aligned} \text{Minimize} \quad & v \\ \text{subject to} \quad & v \geq f(x) \text{ for every } x \in P \\ & (\text{N}), (\Gamma1), (\Gamma2), (\text{P1}), (\text{P2}), (\text{P3}) \end{aligned}$$

The parameters $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ were first introduced in [47]. They are the best lower bounds on $\sigma(\Gamma)$ and, respectively, $\widetilde{\sigma}(\Gamma)$ that can be obtained by using only Shannon information inequalities, that is, they are the best possible Shannon-type lower bounds. If the number of participants is small, they can be computed by solving the corresponding linear programming problems. This approach has been used in [25, 48, 55]. In more general situations, lower bounds on $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ can be derived from the constraints without solving the linear programming problems, as in [10, 12, 17, 18, 20, 39] and many other works. In particular, the result in the following theorem, which is the best of the known general asymptotic lower bounds, was found in this way.

Theorem 2.11 (Csirmaz [14, 15])**.** *For every n, there exists an access structure Γ_n on n participants such that $\widetilde{\kappa}(\Gamma_n)$ is $\Omega(n/\log n)$.*

Since not all polymatroids are entropic, the lower bounds $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ are not tight in general. Moreover, Csirmaz [15] proved that $\kappa(\Gamma) \leq n$ for every access structure Γ on n participants, which indicates that those lower bounds may be very far from tight. That result was proved by showing feasible solutions of the linear programming problems with small values of the objective function.

Duality simplifies the search for bounds in secret sharing. Indeed, if Γ^* is the dual of the access structure Γ, then $\kappa(\Gamma^*) = \kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma^*) = \widetilde{\kappa}(\Gamma)$ [47]. More interestingly, the optimal information ratio for linear secret sharing schemes is invariant by duality, that is, $\lambda(\Gamma^*) = \lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma^*) = \widetilde{\lambda}(\Gamma)$ [38]. The same result has been recently proved for abelian secret sharing [40]. In contrast, it is not known whether the analogous relation applies to general secret sharing (that is, to the parameters σ and $\widetilde{\sigma}$) or not.

2.4 Ideal Secret Sharing Schemes and Matroid Ports

The extreme case $\kappa(\Gamma) = 1$ deserves some attention because it is related to *ideal* secret sharing schemes. Since we are assuming that there are no redundant participants, it is easy to prove that every feasible solution f of the Linear Programming Problems 2.9 and 2.10 satisfies $f(x) \geq 1$ for every $x \in P$. Therefore, $1 \leq \widetilde{\kappa}(\Gamma) \leq \kappa(\Gamma)$ for every access structure Γ, and hence the average information ratio of every secret sharing scheme is at least 1.

Definition 2.12. A secret sharing scheme $\Sigma = (S_x)_{x\in Q}$ is *ideal* if its information ratio is equal to 1, which is best possible. *Ideal access structures* are those that admit an ideal secret sharing scheme.

Definition 2.13. A *matroid* $M = (Q, r)$ is an integer polymatroid such that $r(X) \leq |X|$ for every $X \subseteq Q$. The *port of the matroid M at $p_o \in Q$* is the access structure on $P = Q \setminus p_o$ whose qualified sets are the sets $X \subseteq P$ satisfying $r(Xp_o) = r(X)$.

The following theorem is a consequence of the results by Brickell and Davenport [11], who discovered the connection between ideal secret sharing and matroids.

Theorem 2.14. *Let $\Sigma = (S_x)_{x\in Q}$ be an ideal secret sharing scheme on P with access structure Γ. Then the mapping given by $f(X) = H(S_X)/H(S_{p_o})$ for every $X \subseteq Q$ is the rank function of a matroid M with ground set Q. Moreover, Γ is the port of the matroid M at p_o.*

As a consequence, every ideal access structure is a matroid port. The first counterexample for the converse, the ports of the Vamos matroid, was presented by Seymour [60]. Additional results on matroid ports and ideal secret sharing schemes were proved in [47] by using the forbidden minor characterization of matroid ports by Seymour [59].

Theorem 2.15 ([47])**.** *Let Γ be an access structure. Then Γ is a matroid port if and only if $\kappa(\Gamma) = 1$. Moreover, $\kappa(\Gamma) \geq 3/2$ if Γ is not a matroid port.*

In particular, there is a gap in the values of the parameter κ. Namely, there is no access structure Γ with $1 < \kappa(\Gamma) < 3/2$. Therefore, the optimal information ratio of an access structure that is not a matroid port is at least $3/2$.

2.5 Lower Bounds from Non-Shannon Information and Rank Inequalities

Better lower bounds can be obtained by adding to the Linear Programming Problems 2.9 and 2.10 new constraints derived from *non-Shannon information inequalities*, which are satisfied by every entropic polymatroid but are not derived from the basic Shannon information inequalities. Zhang and Yeung [69] presented such an inequality for the first time, and many others have been found subsequently [22, 24, 50, 68]. This approach was first applied in [7] to prove that the optimal information ratio of the ports of the Vamos matroid is larger than 1, the first known examples of matroid ports with that property. They are as well the first known examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$, and also the first known examples with $1 < \sigma(\Gamma) < 3/2$. Other lower bounds for the ports of the Vamos matroid and other non-linear matroids have been presented [51, 55].

When searching for bounds for linear secret sharing schemes, that is, bounds on $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, one can improve the linear program by using *rank inequalities*, which apply to configurations of vector subspaces or, equivalently, to the joint entropies of linear random vectors. It is well-known that every information inequality is also a rank inequality. The first known rank inequality that cannot be derived from the Shannon inequalities was found by Ingleton [37]. Other such rank inequalities have been presented afterwards [23, 43]. Better lower bounds on the information ratio of linear secret sharing schemes have been found for some families of access structures by using non-Shannon rank inequalities [7, 16, 55].

On the negative side, Beimel and Orlov [8] proved that the best lower bound that can be obtained by using all information inequalities on four and five variables, together with all inequalities on more than five variables that were known by then, is at most linear on the number of participants. Specifically, they proved that every linear programming problem that is obtained by using these inequalities admits a feasible solution with a small value of the objective function. That solution is related to the one used by Csirmaz [15] to prove that $\kappa(\Gamma)$ is at most the number of participants. Another negative result about the power of information inequalities to provide asymptotic lower bounds was presented in [49]. Namely, every lower bound that is obtained by using rank inequalities on at most r variables is $O(n^{r-2})$, and hence polynomial on the number n of participants. Since all information inequalities are rank inequalities, this negative result applies to the search for asymptotic lower bounds for both linear and general secret sharing schemes.

3 Improved Linear Programming Technique

Our improvements on the LP-technique are presented in this section. Instead of adding non-Shannon information and rank inequalities to the linear programming problems, which is the strategy described in Section 2.5, we add constraints that are obtained by using some properties from which those inequalities are derived.

3.1 Common Information

According to [23], all known non-Shannon rank inequalities are derived from the so-called *common information property*. We say that a random variable S_3 *conveys the common information* of the random variables S_1 and S_2 if $H(S_3|S_2) = H(S_3|S_1) = 0$ and $H(S_3) = I(S_1{:}S_2)$. In general, given two random variables, it is not possible to find a third one satisfying those conditions [28]. Nevertheless, this is possible for every pair of random variables that are defined from subgroups of an abelian group and, in particular, for every pair of $\mathbb{K}$-linear random variables.

Proposition 3.1. *Consider a finite abelian group G, two subgroups H_1, H_2 of G, and $H_3 = H_1 + H_2$. Let S_1, S_2, S_3 be the random variables given by the uniform probability distribution on G and the projections $\pi_i \colon G \to G/H_i$ with $i = 1, 2, 3$. Then the random variable S_3 conveys the common information of the random variables S_1, S_2.*

Proof. Since $H_i \subseteq H_3$ for $i = 1, 2$,

$$H(S_3|S_i) = H(S_iS_3) - H(S_i) = \log|G| - \log|H_i \cap H_3| - (\log|G| - \log|H_i|) = 0$$

and, by one of the isomorphism theorems,

$$I(S_1{:}S_2) = \log|G| - (\log|H_1| + \log|H_2| - \log|H_1 \cap H_2|) = \log|G| - \log|H_1 + H_2| = H(S_3)$$

□

The following definition is motivated by the concept of common information of a pair of random variables.

Definition 3.2. Consider a polymatroid (Q, f) and two sets $A, B \subseteq Q$. Then every subset $X_o \subseteq Q$ such that

- $f(X_o|A) = f(X_o|B) = 0$, and
- $f(X_o) = f(A{:}B) = f(A) + f(B) - f(AB)$

is called a *common information for the pair* (A, B). If $X_o = \{x_o\}$, then the element x_o is also called a common information for the pair (A, B).

Definition 3.3. An *extension* of a polymatroid (Q, f) is any polymatroid (Q', f') with $Q \subseteq Q'$ and $f'(X) = f(X)$ for every $X \subseteq Q$. Usually, we are going to use the same symbol for the rank function of a polymatroid and that of an extension of it.

Definition 3.4. A polymatroid (Q, f) satisfies the *common information property* if, for every pair (A_0, A_1) of subsets of Q, there exists an extension (Qx_o, f) of it such that x_o is a common information for the pair (A_0, A_1).

Proposition 3.5. *Every linear polymatroid satisfies the common information property. Moreover, given a linear polymatroid (Q, f) and a pair (A_0, A_1) of subsets of Q, it can be extended to a* linear *polymatroid (Qx_o, f) such that x_o is a common information for the pair (A_0, A_1). In particular, the extension also satisfies the common information property. This result can be extended to the class of polymatroids that are determined by abelian random vectors.*

Proof. Straightforward from Proposition 3.1. □

We describe next how to modify the Linear Programming Problems 2.9 and 2.10 by using the common information property in order to obtain better lower bounds on the information ratio of linear secret sharing schemes. Let Γ be an access structure on a set P and $\Sigma = (S_x)_{x \in Q}$ an abelian secret sharing scheme for Γ. As usual, associated to Σ consider the polymatroid (Q, f) defined by $f(X) = H(S_X)/H(S_{p_o})$ for every $X \subseteq Q$. Since the scheme Σ is linear, (Q, f) is the multiple of a linear polymatroid, and hence it satisfies the common information property. Therefore, given any two sets $A_0, A_1 \subseteq Q$, we can find a polymatroid (Qx_o, f), an extension of (Q, f), such that x_o is a common information for the pair (A_0, A_1). Clearly, the vector $(f(X))_{X \subseteq Qx_o} \in \mathbb{R}^{\mathcal{P}(Qx_o)}$ is a feasible solution of the Linear Programming Problem 3.6.

Linear Programming Problem 3.6. The optimal value of this linear programming problem is a lower bound on $\widetilde{\lambda}(\Gamma)$:

$$\begin{aligned}
\text{Minimize} \quad & (1/n)\sum_{x\in P} f(x) \\
\text{subject to} \quad & (\mathrm{N}), (\Gamma 1), (\Gamma 2) \\
& f(x_o|A_0) = f(x_o|A_1) = 0 \\
& f(x_o) = f(A_0) + f(A_1) - f(A_0\, A_1) \\
& (\mathrm{P1}), (\mathrm{P2}), (\mathrm{P3}) \text{ on the set } Qx_o
\end{aligned}$$

Since this applies to every linear secret sharing scheme with access structure Γ, the optimal value of that linear programming problem is a lower bound on $\widetilde{\lambda}(\Gamma)$. Of course, we can use the common information for more than one pair of sets. Specifically, given k pairs $(A_{i0}, A_{i1})_{i\in[k]}$ of subsets of Q, the optimal value of the Linear Programming Problem 3.7 is a lower bound on $\widetilde{\lambda}(\Gamma)$. Obviously, analogous modifications on Linear Programming Problem 2.10 provide lower bounds on $\lambda(\Gamma)$.

Linear Programming Problem 3.7. The optimal value of this linear programming problem is a lower bound on $\widetilde{\lambda}(\Gamma)$:

$$\begin{aligned}
\text{Minimize} \quad & (1/n)\sum_{x\in P} f(x) \\
\text{subject to} \quad & (\mathrm{N}), (\Gamma 1), (\Gamma 2) \\
& f(x_i|A_{i0}) = f(x_i|A_{i1}) = 0, \\
& f(x_i) = f(A_{i0}) + f(A_{i1}) - f(A_{i0}\, A_{i1}) \text{ for every } i = 1, \ldots, k \\
& (\mathrm{P1}), (\mathrm{P2}), (\mathrm{P3}) \text{ on the set } Qx_1 \ldots x_k
\end{aligned}$$

Of course, by Proposition 3.5, those lower bounds apply also to abelian secret sharing schemes.

3.2 Ahlswede and Körner's Information

In Section 3.1, the common information property was used to improve lower bounds on the information ratio of linear secret sharing schemes and, more generally, schemes that are defined from abelian groups. For the general case, we are going to use a similar property motivated by the works of Ahlswede and Körner.

The known non-Shannon-type inequalities can be derived by using two techniques, the so-called Copy lemma [69] and the Ahlswede-Körner lemma as used in [45]. It turns out that the power of these two lemmas is equivalent [41]. In particular, both constructions can be used to derive the same non-Shannon inequalities. Hereafter, we choose to use a version of the Ahlswede and Körner (AK) lemma, as it makes the LP program slightly easier to formulate because the constraints needed for the construction of additional variables are shorter to write down. The original result by Ahlswede and Körner [1, 2, 19] is a statement about the achievable rate region of a certain communication problem. Here, we use the AK lemma as presented in [41, Lemma 2], a statement that in its part can be derived from the proof of [45, Lemma 5]. That result deals with sequences of random variables, and hence with *almost entropic polymatroids*.

Definition 3.8. We say that a polymatroid is *almost entropic* if it is the limit of a sequence of entropic polymatroids.

We introduce next the *AK-information property*, which will play the same role in the general case as the common information for linear schemes.

Definition 3.9. Consider a polymatroid (Q, f), and subsets $U, V, Z \subseteq Q$. Then every subset $Z_o \subseteq Q$ such that

- $f(Z_o|UV) = 0$,
- $f(U|Z_o) = f(U|Z)$,
- $f(V|Z_o) = f(V|Z)$,
- $f(UV|Z_o) = f(UV|Z)$

is called an *AK-information for the triple* (U, V, Z). Moreover, we say that a polymatroid (Q, f) satisfies the *AK-information property*, if, for every triple (U, V, Z) of subsets of Q, there exists an extension (Qz_o, f) such that z_o is an AK-information for the triple (U, V, Z).

The following version of the AK lemma is a straightforward consequence of [41, Lemma 2].

Proposition 3.10 (Ahlswede and Körner lemma)**.** *Let (Q, f) be an entropic polymatroid and consider $U, V, Z \subseteq Q$. Then there exists a sequence $(Qz_o, f_N)_{N>0}$ of entropic polymatroids satisfying the following properties.*

- *The sequence $(Qz_o, (1/N)f_N)_{N>0}$ converges to a polymatroid (Qz_o, f') that is an extension of (Q, f).*
- *The element z_o in (Qz_o, f') is an AK-information for the triple (U, V, Z).*

Loosely speaking, the AK lemma says that given any triple of random variables, we can always construct a new random variable that is as close as we want to their AK-information. The following result is a consequence of Proposition 3.10 and the fact that every multiple of an entropic polymatroid is almost entropic [66].

Proposition 3.11. *Every almost entropic polymatroid satisfies the AK-information property. More specifically, for every almost entropic polymatroid (Q, f) and sets $U, V, Z \subseteq Q$, there exists an almost entropic extension (Qz_o, f) such that z_o is an AK-information for the triple (U, V, Z).*

Of course, this proposition can be repeatedly applied to construct the AK-informations of various triples of subsets. Moreover, entropic polymatroids are trivially almost entropic, therefore we can add any AK-information constraint to the Linear Programming Problems 2.9 and 2.10 in order to obtain lower bounds on $\widetilde{\sigma}(\Gamma)$ and $\sigma(\Gamma)$. For instance, suppose we want to use k such AK-informations, then for $i \in \{1, \ldots, k\}$, let $U_i, V_i, Z_i \subseteq Q$, and let z_i be an AK-information for the triple (U_i, V_i, Z_i). Then the optimal value of the Linear Programming Problem 3.12 is a lower bound on $\widetilde{\sigma}(\Gamma)$. An analogous modification on the Linear Programming Problem 2.9 provides lower bounds on $\sigma(\Gamma)$.

Linear Programming Problem 3.12. The optimal value of this linear programming problem is a lower bound on $\widetilde{\sigma}(\Gamma)$:

$$\begin{array}{ll} \text{Minimize} & (1/n)\sum_{x\in P} f(x) \\ \text{subject to} & (\mathrm{N}), (\Gamma 1), (\Gamma 2), \\ & f(z_i|U_iV_i) = 0, \\ & f(U_i|z_i) = f(U_i|Z_i), \\ & f(V_i|z_i) = f(V_i|Z_i), \\ & f(U_iV_i|z_i) = f(U_iV_i|Z_i) \text{ for every } i = 1, \ldots, k \\ & (\mathrm{P}1), (\mathrm{P}2), (\mathrm{P}3) \text{ on the set } Qz_1 \ldots z_k \end{array}$$

3.3 Common Information Implies Ahlswede and Körner's Information

We describe next the connection between those two techniques. In particular, we prove that any bound from AK-information constraints can be also obtained from common information constraints, which is consistent with the fact that the bounds given by the first technique are more general.

Proposition 3.13. *Let $\mathcal{S} = (Q, f)$ be a polymatroid, $A, B \subseteq Q$, and $X_o \subseteq Q$ a common information for (A, B). Consider a subset $Y \subseteq Q$ such that $f(Y|A) = f(Y|B) = 0$. Then $f(Y|X_o) = 0$.*

Proof. We prove first that, in the conditions of the statement, $f(Y) \leq f(X_o)$. Indeed,

$$\begin{array}{rcl} f(X_o) - f(Y) & = & f(A) + f(B) - f(AB) - f(Y) \\ & = & f(AY) + f(BY) - f(ABY) - f(Y) \\ & = & f(A{:}B|Y) \geq 0 \end{array}$$

Therefore, $f(YX_o) \leq f(X_o)$ because $f(YX_o|A) = f(YX_o|B) = 0$, and we can conclude that $f(Y|X_o) = 0$. □

Proposition 3.14. *Let $\mathcal{S} = (Q, f)$ be a polymatroid, $A, B \subseteq Q$, and $X_o \subseteq Q$ a common information for (A, B). Then $f(C|X_o) = f(C|B)$ for every subset $C \subseteq A$.*

Proof. On one hand,

$$f(C|X_o) - f(C|B) = f(C|X_o) - f(C|BX_o) = f(C{:}B|X_o) \geq 0$$

On the other hand, take $D = A \setminus C$,

$$\begin{array}{rcl} f(C|B) - f(C|X_o) & = & f(CB) - f(B) - f(CX_o) + f(X_o) \\ & = & f(CB) - f(B) - f(CX_o) + f(A) + f(B) - f(AB) \\ & = & f(CBX_o) + f(AX_o) - f(CX_o) - f(ABX_o) \\ & = & f(CBX_o) + f(CDX_o) - f(CX_o) - f(CDBX_o) \\ & = & f(B{:}D|CX_o) \geq 0 \end{array}$$

and the proof is concluded. □

The next two propositions relate common information and AK-information. The first one follows directly from Proposition 3.14.

Proposition 3.15. *Consider a polymatroid (Q, f) and subsets $U, V, Z \subseteq Q$. Let $X_o \subseteq Q$ be a common information for the pair (UV, Z). Then X_o is an AK-information for the triple (U, V, Z). As a consequence, every polymatroid satisfying the common information property satisfies the AK-information property too.*

Proposition 3.16. *Consider a polymatroid (Q, f) and subsets $U, V, Z \subseteq Q$. Let $Z_o \subseteq Q$ be an AK-information for (U, V, Z). Then $f(Z_o) = f(UV{:}Z)$. In particular, Z_o is a common information for (UV, Z) if and only if $f(Z_o|Z) = 0$.*

Proof. $f(UV{:}Z) = f(UV) - f(UV|Z) = f(UV) - f(UV|Z_o) = f(Z_o) - f(Z_o|UV) = f(Z_o)$ □

4 Common Information and Duality

As we mentioned in Section 2.3, every lower bound on the optimal information ratio of abelian or linear secret sharing schemes for an access structure Γ applies also to the dual Γ^*. Duality in secret sharing is related to duality in polymatroids. The reader is refereed to [47] for more information on this topic. The *dual* of a polymatroid (Q, f) is the polymatroid (Q, f^*) defined by

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

for every $X \subseteq Q$. The dual of a $\mathbb{K}$-linear polymatroid is also $\mathbb{K}$-linear and, as a consequence of the results in [40], the same applies to polymatroids associated to abelian random vectors. Nevertheless, it is not known whether this result can be extended to entropic polymatroids or not. The behavior of the common information property with respect to duality is not obvious. In this section, we define two new properties related to common information that are dual of each other. Every linear polymatroid satisfies both.

For a polymatroid (Q, f) and $x \in Q$, the polymatroids $(Q \setminus x, f_{\setminus x})$ and $(Q \setminus x, f_{/x})$ are defined respectively by $f_{\setminus x}(X) = f(X)$ and $f_{/x}(X) = f(X|x)$ for every $X \subseteq Q \setminus x$. Every polymatroid that can be obtained from (Q, f) by applying several times those operations is called a *minor* of (Q, f).

Definition 4.1. Consider a polymatroid (Q, f) and three pairwise disjoint sets $A, B, C \subseteq Q$. The polymatroid (Q, f) admits a *restricted common information* for the pair (AC, BC) if there is a polymatroid (Qx_o, g) satisfying the following properties.

1. $f = g_{\setminus x_o}$.
2. $g(x_o) = f(A{:}B|C)$.
3. $g(x_o{:}A) = g(x_o{:}B) = 0$ while $g(x_o{:}C) = g(x_o)$.

Proposition 4.2. *Every linear polymatroid (Q, f) admits a restricted common information for every pair (AC, BC) such that the extension (Qx_o, g) is also linear.*

Proof. Consider a collection $(V_x)_{x \in Q}$ of subspaces of a vector space V defining a linear polymatroid (Q, f). Given three pairwise disjoint sets $A, B, C \subseteq Q$, take a subspace $W \subseteq V$ such that $V_{ABC} = V_C + W$ and $V_C \cap W = \{0\}$. Extend the polymatroid (Q, f) by adding a new element x_o associated to the subspace W. □

We discuss next some properties of the dual polymatroids (Q, f^*) and (Qx_o, g^*). By a well known property about minors of polymatroids, $f^* = g^*_{/x_o}$.

Lemma 4.3. *Take $D = Q \smallsetminus ABC$. Then the following properties hold.*

- $g(x_o) = g^*(x_o) = f^*(A{:}B|D) = g^*(A{:}B|Dx_o)$.
- $g^*(x_o{:}AD) = g^*(x_o)$ *and* $g^*(x_o{:}BD) = g^*(x_o)$.
- $g^*(x_o{:}ABD) = 0$.
- $g^*(A{:}B|D) = 0$.

Proof. An easy but somewhat long calculation. □

These properties lead to the following definition.

Definition 4.4. Let $A, B, C \subseteq Q$ be pairwise disjoint sets. A polymatroid (Q, f) admits a *dual restricted common information* for a pair (AC, BC) of subsets of Q if there exists a polymatroid (Qx_o, g), satisfying the following properties.

1. $f = g_{/x_o}$.
2. $g(x_o) = f(A{:}B|C)$.
3. $g(A{:}B|C) = 0$.
4. $g(x_o{:}AC) = g(x_o{:}BC) = g(x_o)$ while $g(x_o{:}ABC) = 0$.

Proposition 4.5. *Every linear polymatroid (Q, f) admits a dual restricted common information for every pair (AC, BC) such that the polymatroid (Qx_o, g) is also linear.*

Proof. Apply Proposition 4.2 to the dual polymatroid (Q, f^*) and the pair (AD, BD) with $D = Q \smallsetminus ABC$. □

5 New Lower Bounds

We present here the new lower bounds on the optimal information ratio that were obtained by using our improvement on the LP-technique. All of them deal with access structures on small sets of participants and were computed by solving the linear programming problems introduced in Section 3.

5.1 Access Structures on Five Participants

Jackson and Martin [39] determined the optimal information ratios of most access structures on five participants. The case of four participants had been previously solved by Stinson [62]. After some additional contributions [21, 31, 55], both $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$ were determined for 172 of the 180 access structures on five participants. All these results were obtained by finding the exact values or lower bounds on $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$, and then constructing linear secret sharing schemes whose (average) information ratios equaled the lower bounds. Therefore, $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma)$ and $\widetilde{\kappa}(\Gamma) = \widetilde{\sigma}(\Gamma) = \widetilde{\lambda}(\Gamma)$ for each of those 172 access structures. The unsolved cases correspond to the access structures Γ_{30}, Γ_{40}, Γ_{53}, and Γ_{73} (we use the same notation as in [39]) and their duals Γ_{153}, Γ_{150}, Γ_{152}, and Γ_{151}, respectively. Following [39], we take these access structures on the set $\{a, b, c, d, e\}$. The minimal qualified sets of the first four are given in the following.

- $\min \Gamma_{30} = \{ab, ac, bc, ad, bd, ae, cde\}$.

- $\min \Gamma_{40} = \{ab, ac, bc, ad, be, cde\}$.
- $\min \Gamma_{53} = \{ab, ac, ad, bcd, be, ce\}$.
- $\min \Gamma_{73} = \{ab, ac, bd, ce, ade\}$.

We list in the following what is known for them. These results apply also to the corresponding dual access structures.

- $\widetilde{\kappa}(\Gamma) = \widetilde{\sigma}(\Gamma) = \widetilde{\lambda}(\Gamma) = 7/5$ for Γ_{30} and Γ_{40}.
- $\widetilde{\kappa}(\Gamma) = \widetilde{\sigma}(\Gamma) = \widetilde{\lambda}(\Gamma) = 3/2$ for Γ_{53}.
- $3/2 = \widetilde{\kappa}(\Gamma) \leq \widetilde{\sigma}(\Gamma) \leq \widetilde{\lambda}(\Gamma) \leq 8/5$ for Γ_{73}.
- $3/2 = \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma) \leq 5/3$ for Γ_{30}, Γ_{53} and Γ_{73}.
- $3/2 = \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma) \leq 12/7$ for Γ_{40}.

The values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$, which coincide with the lower bounds given in [21, 39], were determined in [55] by solving the Linear Programming Problems 2.9 and 2.10. The upper bounds were given in [39], except the one on $\widetilde{\lambda}(\Gamma_{53})$, which was proved in [31].

By [55, Proposition 7.1], there is no linear scheme for Γ_{53} or Γ_{73} with information ratio equal to $3/2$, and there is no linear scheme for Γ_{73} with average information ratio equal to $3/2$. Therefore, it appears that a new technique is required to solve these cases. Our improvement of the LP-technique provided new lower bounds. Namely, by solving problems as the Linear Programming Problems 3.6 and 3.12 with the specified settings, we obtain the bounds in Tables 1 and 2, respectively.

Access structure	A_0	A_1	New lower bound
Γ_{30}, Γ_{40}, Γ_{53}, Γ_{73}	a	d	$5/3 \leq \lambda(\Gamma)$
Γ_{73}	a	d	$23/15 \leq \widetilde{\lambda}(\Gamma)$

Table 1: Results on five participants using common information.

The values of $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ can be now determined for all access structures on 5 participants by combining the lower bounds in Table 1 with the existing upper bounds and the ones derived from the constructions in Section 6. Observe that Γ_{30}, Γ_{40}, Γ_{53}, Γ_{73} and their duals are precisely the access structures on least participants satisfying $\kappa(\Gamma) < \lambda(\Gamma)$.

Access structure	Z	U	V	New lower bound
Γ_{30}, Γ_{40}, Γ_{53}, Γ_{73}	a	d	e	$14/9 \leq \sigma(\Gamma)$
Γ_{73}	a	d	e	$53/35 \leq \widetilde{\sigma}(\Gamma)$

Table 2: Results on five participants using AK information for the subsets (Z, Y_1, Y_2).

From the bounds in Table 2, we see that Γ_{30}, Γ_{40}, Γ_{53}, Γ_{73} are among the smallest access structures with $\kappa(\Gamma) < \sigma(\Gamma)$. Unfortunately, all our attempts to obtain lower bounds on $\sigma(\Gamma)$ for their duals by using AK-informations have been unsuccessful.

5.2 Graph-Based Access Structures on Six Participants

If all minimal qualified sets of an access structure have two participants, it can be represented by a graph whose vertices and edges correspond to the participants and the minimal qualified sets, respectively. Van Dijk [20] determined the optimal information ratio of most graph-based access structures on 6 participants and provided lower and upper bounds for the remaining cases. After several other authors improved those results [13, 30, 32, 44, 55], only nine cases remained unsolved. Since the known values of $\sigma(\Gamma)$ have been determined by finding lower bounds on $\kappa(\Gamma)$ and upper bounds on $\lambda(\Gamma)$, we have $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma)$ in the solved cases. The unsolved cases correspond to the following graph-based access structures on $P = \{1, 2, 3, 4, 5, 6\}$.

- $\min \Gamma_{55} = \{12, 23, 34, 45, 56, 61, 26, 25\}$
- $\min \Gamma_{59} = \{12, 23, 34, 45, 56, 61, 24, 13\}$
- $\min \Gamma_{70} = \{12, 23, 34, 45, 56, 61, 24, 25, 26\}$
- $\min \Gamma_{71} = \{12, 23, 34, 45, 56, 61, 26, 35, 36\}$
- $\min \Gamma_{75} = \{12, 23, 34, 45, 56, 61, 26, 46, 14\}$
- $\min \Gamma_{77} = \{12, 23, 34, 45, 56, 61, 26, 35, 13\}$
- $\min \Gamma_{84} = \{12, 23, 34, 45, 56, 61, 13, 15, 35, 25\}$
- $\min \Gamma_{91} = \{12, 23, 34, 45, 56, 61, 15, 25, 35, 46\}$
- $\min \Gamma_{93} = \{12, 23, 34, 45, 56, 61, 15, 35, 46, 24\}$

The known lower and upper bounds for those access structures are

- $3/2 = \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma) \leq 8/5$ for $\Gamma = \Gamma_{91}$ and $\Gamma = \Gamma_{93}$, and
- $3/2 = \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma) \leq 5/3$ for the other seven access structures.

The values of κ were determined by solving the corresponding linear programming problems, and they are equal to the lower bounds in [20]. All upper bounds were presented in [20], except the one for Γ_{93}, which was given in [44].

By using the common information property with the settings specified in Table 3, we found the new lower bound $\lambda(\Gamma) \geq 8/5$ for all those access structures, which is tight for Γ_{91} and Γ_{93}. In particular, those nine graph-based access structures satisfy $\kappa(\Gamma) < \lambda(\Gamma)$. We have to mention here that all our attempts to improve the known lower bounds on $\sigma(\Gamma)$ for those graph-based access structures by using linear programming problems with AK-informations did not give any result.

After a preprint of this work was in circulation, Gharahi and Khazaei [34] proved that all lower bounds on $\lambda(\Gamma)$ in Table 3 are tight by presenting constructions of linear secret sharing schemes for the corresponding graph-based access structures. Therefore, the exact value of $\lambda(\Gamma)$ is now determined for all graph-based access structures on six participants.

Access Structure	A_0	A_1	New lower bound
$\Gamma_{55}, \Gamma_{70}, \Gamma_{75}, \Gamma_{84}$	3	6	$8/5 \leq \lambda(\Gamma)$
Γ_{71}	5	p_o3	$8/5 \leq \lambda(\Gamma)$
Γ_{91}, Γ_{93}	6	p_o5	$8/5 \leq \lambda(\Gamma)$

Access structure	A_{00}	A_{01}	A_{10}	A_{11}	New lower bound
Γ_{59}	3	6	5	p_o4	$8/5 \leq \lambda(\Gamma)$
Γ_{77}	4	p_o3	2	p_o6	$8/5 \leq \lambda(\Gamma)$

Table 3: New bounds for graph-based access structures on six participants using common information.

5.3 Access Structures with Four Minimal Qualified Sets on Six Participants

Bounds on the optimal information ratio of the access structures with four minimal qualified sets were presented in [48]. The lower bounds were obtained from linear programming with Shannon information inequalities. Upper bounds providing exact values for all but four of those access structures on six players were given in [33]. All those access structures satisfy $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma)$. The dual of two of the unsolved cases ($357ADE$ and $357BDE$ in the notation introduced in [48]) are graph-based access structures, and hence their optimal information ratio for linear secret sharing schemes is known, namely $8/5$. By using common information, we otained the new lower bound on $\lambda(\Gamma) \geq 8/5$ for the other two unsolved cases ($167ADE$ and $3579BE$). The known upper bounds do not match this lower bound. Those four access structures satisfy $\kappa(\Gamma) < \lambda(\Gamma)$. We were not able to find new bounds on $\sigma(\Gamma)$ by using AK-information.

5.4 Ports of Non-Representable Matroids

Recall from Section 2.4 that Γ is a matroid port if and only if $\kappa(\Gamma) = 1$. Moreover, $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 1$ if Γ is the port of a linear matroid. In this section, we apply our techniques to find new lower bounds on the optimal information ratio of some ports of non-linear matroids on eight points, which are access structures on seven participants. All matroids on seven points are linear. Hence, the matroids we consider here are amongst the smallest non-linear matroids.

We describe next several matroids (Q, r) on eight points with $r(Q) = 4$ that admit convenient geometric representations on a cube. All of them satisfy that

- $r(X) = |X|$ for every $X \subseteq Q$ with $|X| \leq 3$,
- $r(X) = 4$ for every $X \subseteq Q$ with $|X| \geq 5$, and
- $3 \leq r(X) \leq 4$ for every $X \subseteq Q$ with $|X| = 4$.

In particular, they are *paving* matroids (see [52]). Observe that such a matroid can be described by giving the subsets $X \subseteq Q$ with $|X| = 4$ and $r(X) = 3$, that is, by giving its 4-*points planes*.

Consider the 3-dimensional cube with vertices on the points $(x, y, z) \in \{0, 1\}^3$. By using the binary representation, identify each of those vertices to an integer in $\{0, 1, \ldots, 7\}$. For instance, $(0, 1, 0)$ is identified to 2 and $(1, 1, 0)$ to 6. Consider the following 14 sets of vertices.

- The six faces of the cube: $0123, 0145, 0246, 1357, 2367, 4567$,
- the six diagonal planes: $0167, 0257, 0347, 1256, 1346, 2345$, and

- the two twisted planes: $0356, 1247$.

The matroid whose 4-points planes are those fourteen sets is the *binary affine cube* $AG(3,2)$. This matroid is $\mathbb{K}$-linear if and only if the field $\mathbb{K}$ has characteristic 2 [52].

All matroids that are obtained from $AG(3,2)$ by relaxing one of the 4-points planes (that is, by changing the value of its rank to 4) are isomorphic to the matroid $AG(3,2)'$ [52]. We consider here the one obtained by the relaxation of one of the twisted planes, say 1247. The matroid $AG(3,2)'$ is a smallest non-linear matroid [52]. The port of $AG(3,2)'$ at $p_o = 0$ is the access structure $\mathcal{A}$ on the set $\{1,\ldots,7\}$ with minimal qualified sets

$$\min \mathcal{A} = \{123, 145, 167, 246, 257, 347, 356, 1247\}$$

Every port of $AG(3,2)'$ is either isomorphic to $\mathcal{A}$ or to its dual $\mathcal{A}^*$, which has minimal qualified sets

$$\min \mathcal{A}^* = \{123, 145, 167, 246, 257, 347, 1356, 2356, 3456, 3567\}$$

By relaxing the other twisted plane 0356 we obtain from $AG(3,2)'$ the matroid R_8, the *real affine cube*. The 4-points planes of this matroid are the six faces and the six diagonal planes. It is $\mathbb{K}$-linear if and only if $\mathbb{K}$ has characteristic different from 2 [52] .

If, instead, the 4-points set 1256 is relaxed in $AG(3,2)'$, one obtains the smallest non-linear matroid F_8 [52]. The port of F_8 at $p_o = 0$ is the access structure $\mathcal{F}$ on $\{1,\ldots,7\}$ with minimal qualified sets

$$\min \mathcal{F} = \{123, 145, 167, 246, 257, 347, 356, 1247, 1256\}$$

The port of F_8 at $p_o = 3$ is isomorphic to $\mathcal{F}$. The ports of F_8 at $p_o = 1$ and $p_o = 2$ are both isomorphic to $\mathcal{F}^*$, whose minimal qualified sets are

$$\min \mathcal{F}^* = \{123, 145, 167, 246, 257, 1356, 2356, 3456, 3567, 1347, 2347, 3457, 3467\}$$

All the other ports of F_8 are isomorphic to the port of F_8 at $p_o = 4$, and hence isomorphic to the access structure $\widehat{\mathcal{F}}$ on $\{1,\ldots,7\}$ with minimal qualified sets

$$\min \widehat{\mathcal{F}} = \{123, 145, 246, 167, 257, 347, 1256, 1356, 2356, 3456, 3567\}$$

Observe that $\widehat{\mathcal{F}}$ is isomorphic to its dual access structure $\widehat{\mathcal{F}}^*$.

The relaxation of one of the diagonal planes of the real affine cube R_8, say 1256, produces the matroid Q_8, again a smallest non-linear matroid [52]. Let $\mathcal{Q}$ be the port of Q_8 at $p_o = 0$. Its minimal qualified sets are

$$\min \mathcal{Q} = \{123, 145, 246, 167, 257, 347, 1256, 1247, 1356, 2356, 3456, 3567\}$$

All ports of Q_8 are isomorphic to $\mathcal{Q}$ or to its dual $\mathcal{Q}^*$. The access structure $\mathcal{Q}^*$ has minimal qualified sets

$$\{123, 145, 246, 167, 257, 1247, 1347, 1356, 2347, 2356, 3456, 3457, 3467, 3567\}$$

Finally, the *Vamos matroid* V_8 is another smallest non-linear matroid [52]. Its 4-points planes are 0123, 0145, 2345, 2367, and 4567. The minimal qualified sets of the port $\mathcal{V}$ of the Vamos matroid V_8 at $p_o = 0$ are the 3-sets $123, 145$ and all 4-sets not containing them, except $2345, 2367, 4567$. Every port of V_8 is isomorphic either to $\mathcal{V}$ or to $\mathcal{V}^*$. The minimal qualified sets of $\mathcal{V}^*$ are the 3-sets $123, 145, 167$ and all 4-sets not containing them, except $2367, 4567$. The known bounds on the optimal information ratio of the ports of those non-linear matroids are summarized as follows.

- $67/59 \leq \sigma(\mathcal{V}) \leq 4/3$.
- $9/8 \leq \sigma(\mathcal{V}^*) \leq 4/3$.
- $5/4 \leq \lambda(\mathcal{V}) = \lambda(\mathcal{V}^*) \leq 4/3$.
- $19/17 \leq \sigma(\Gamma)$ if $\Gamma = \mathcal{A}$ or $\Gamma = \mathcal{Q}$.
- $9/8 \leq \sigma(\Gamma)$ if $\Gamma = \mathcal{A}^*$ or $\Gamma = \mathcal{Q}^*$.
- $5/4 \leq \lambda(\Gamma)$ if Γ is one of the structures $\mathcal{A}$, $\mathcal{A}^*$, $\mathcal{Q}$, $\mathcal{Q}^*$.

The lower bounds were obtained in [7, 29, 51, 55] by using the LP-technique enhanced with the Ingleton inequality or with several non-Shannon information inequalities. The upper bounds for the ports of the Vamos matroid were presented in [47].

By solving the LP problems 3.7 and 3.12 for those access structures with the given choices, the lower bounds in Tables 4 and 5 are obtained. Except for $\sigma(\mathcal{V}^*)$, they improve all existing lower bounds. By using the copy lemma instead of the Ahlswede-Körner lemma, one of the bounds for the Vamos matroid has been recently improved [35]. Specifically, $\sigma(\mathcal{V}) \geq 1.142566$. In particular, we have determined the exact value of $\lambda(\mathcal{V}) = \lambda(\mathcal{V}^*) = 4/3$, and also the exact value $\lambda(\mathcal{Q}) = \lambda(\mathcal{Q}^*) = 4/3$ by combining those lower bounds with the construction we present in Section 6.

Access structure	A_0	A_1	New lower bound
$\mathcal{A}, \mathcal{F}, \widehat{\mathcal{F}}$	06	17	$4/3 \leq \lambda(\Gamma)$
$\mathcal{Q}$	04	15	$4/3 \leq \lambda(\Gamma)$
$\mathcal{V}$	01	23	$4/3 \leq \lambda(\Gamma)$

Table 4: Results on matroid ports using common information.

Access structure	Z_1	U_1	V_1	Z_2	U_2	V_2	New lower bound
$\mathcal{A}$	03	12	56				$9/8 \leq \sigma(\Gamma)$
$\mathcal{A}^*$	03	12	47	12	47	56	$33/29 \leq \sigma(\Gamma)$
$\mathcal{F}, \mathcal{Q}$	04	15	37				$9/8 \leq \sigma(\Gamma)$
$\mathcal{F}^*$	04	15	26	14	27	36	$42/37 \leq \sigma(\Gamma)$
$\widehat{\mathcal{F}}$	04	15	37	14	27	36	$42/37 \leq \sigma(\Gamma)$
$\mathcal{Q}^*$	04	15	26	15	26	37	$33/29 \leq \sigma(\Gamma)$
$\mathcal{V}$	01	23	45	23	45	67	$33/29 \leq \sigma(\Gamma)$
$\mathcal{V}^*$	01	23	45				$9/8 \leq \sigma(\Gamma)$

Table 5: Results on matroid ports using AK information for the subsets (Z_1, Y_{11}, Y_{12}) and (Z_2, Y_{21}, Y_{22}).

6 Constructions

We present here linear secret sharing schemes for the access structures Γ_{40} and Γ_{73} on five participants and also for the matroid port $\mathcal{Q}$. These constructions and the lower bounds for

linear schemes that have been obtained with our enhancement of the LP-technique determine the exact values of $\lambda(\Gamma_{40})$, $\widetilde{\lambda}(\Gamma_{73})$, and $\lambda(\mathcal{Q})$. As a consequence, the exact values of $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ are now determined for all access structures on five participants.

We present first a linear scheme with information ratio 5/3 for the access structure Γ_{40} on five participants. For a finite field $\mathbb{K}$ with characteristic larger than 5, consider the $\mathbb{K}$-linear secret sharing scheme that is determined by the $\mathbb{K}$-linear code with generator matrix

$$\left(\begin{array}{c|cc|cc|c|c} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 2 & 0 \end{array}\right)$$

Namely, every codeword corresponds to a distribution of shares. The vertical bars indicate which positions of the codeword correspond to the secret and to every participant. In this case, a codeword

$$(s_{p_o} \,|\, s_{a1}, s_{a2} \,|\, s_{b1}, s_{b2} \,|\, s_c \,|\, s_d \,|\, s_e) \in \mathbb{K}^8$$

corresponds to a distribution of shares in which the secret value is $s_{p_o} \in \mathbb{K}$, the share for a is $(s_{a1}, s_{a2}) \in \mathbb{K}^2$, and so on. The access structure of this linear scheme is Γ_{40}. Another $\mathbb{K}$-linear secret sharing scheme for Γ_{40} is given by the $\mathbb{K}$-linear code with generator matrix

$$\left(\begin{array}{cc|ccc|ccc|cccc|ccc|ccc} 1 & -1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 2 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 3 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ -1 & 2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

By concatenating these two schemes, we obtain a scheme for Γ_{40} with information ratio 5/3.

If $\mathbb{K}$ is a field with characteristic 2, the $\mathbb{K}$-linear code with generator matrix

$$\left(\begin{array}{ccc|ccccc|ccccc|ccccc|cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right)$$

defines a $\mathbb{K}$-linear secret sharing scheme with access structure Γ_{73}. Its average information ratio is equal to 23/15.

We present next a construction of a linear secret sharing scheme with information ratio 4/3 for the access structure $\mathcal{Q}$. It is obtained by combining four ideal secret sharing schemes in a λ-decomposition with $\lambda = 3$. The reader is referred to [53, 63] for more information about λ-decompositions. Let $\mathbb{K}$ be a finite field with characteristic different from 2. The first scheme

is the one given by the $\mathbb{K}$-linear code with generator matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Its access structure $\mathcal{R}$ is the port at $p_o = 0$ of the matroid R_8, the real affine cube. One can see that all minimal qualified sets of $\mathcal{Q}$ except 1256 are also qualified sets of $\mathcal{R}$. On the other hand, the unqualified sets of $\mathcal{Q}$ are also unqualified sets of $\mathcal{R}$. The second and third pieces in the decomposition are ideal schemes given by $\mathbb{K}$-linear codes with generator matrices of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & z_2 & 1 & z_4 & 1 & z_6 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

If $z_2 = 0$ and $z_4 = z_6 = -1$, that linear code represents the matroid that is obtained from R_8 by relaxing the 4-points planes 0347 and 1256. Therefore, we obtain a secret sharing scheme in which 347 is not qualified. If, instead, we take $z_2 = -1$ and $z_4 = z_6 = 0$, the matroid represented by that $\mathbb{K}$-linear code is obtained from R_8 by relaxing the 4-point planes 1256, 0246, and 0257. In the corresponding secret sharing scheme, the sets 246 and 257 are unqualified. The fourth scheme is given by the $\mathbb{K}$-linear code with generator matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & -1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

which represents the matroid that is obtained from R_8 by relaxing the 4-points planes 1256, 0145, and 0167. The sets 145 and 167 are not qualified in the corresponding scheme. Observe that every minimal qualified set of $\mathcal{Q}$ appears in at least 3 of those 4 ideal linear secret sharing schemes. Therefore, we get a linear secret sharing scheme for $\mathcal{Q}$ with information ratio 4/3.

7 Open Problems

The first line of future work worth mentioning is to fully conclude the projects initiated by Jackson and Martin [39] and van Dijk [20] by determining the values of $\sigma(\Gamma)$, $\widetilde{\sigma}(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ for all access structures on five participants and all graph-based access structures on six participants.

Another open question is to determine whether the restricted common information property and its dual provide better lower bounds on the information ratio of linear secret sharing schemes or not.

The main direction for future research is to obtain a better understanding of the techniques introduced here in order to improve, if possible, the known asymptotic lower bounds on $\sigma(\Gamma)$. Notice that it is not necessary to solve the corresponding linear programming problem to determine a lower bound. Instead, any feasible solution of the dual linear programming problem provides a lower bound. This strategy, which was suggested by one of the reviewers of a previous version of this work, has been used, not explicitly, by the authors that have derived lower bounds from the constraints without solving the linear programming problem.

References

[1] Ahlswede, R., Körner, J.: On the connection between the entropies of input and output distributions of discrete memoryless channels. Proceedings of the 5th Brasov Conference on Probability Theory, Brasov, 1974. Editura Academiei, Bucuresti, 13-23 (1977)

[2] Ahlswede, R., Körner, J.: Appendix: On Common Information and Related Characteristics of Correlated Information Sources. *General Theory of Information Transfer and Combinatorics.* pp. 664–677. Springer, Berlin Heidelberg (2006)

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

[4] Beimel, A.: Secret-Sharing Schemes: A Survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011)

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

[6] Beimel, A., Gál, A., Paterson, M.: Lower bounds for monotone span programs. Comput. Complexity 6, 29–45 (1997)

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

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

[9] Blakley, G.R.: Safeguarding cryptographic keys. AFIPS Conference Proceedings 48, 313–317 (1979)

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

[11] Brickell, E.F., Davenport, D.M.: On the Classification of Ideal Secret Sharing Schemes. J. Cryptology, 4 123-134 (1991)

[12] Capocelli, R.M., De Santis, A. Gargano, L., Vaccaro, U.: On the Size of Shares for Secret Sharing Schemes. J. Cryptology 6, 157–167 (1993)

[13] Chen, B.L., Sun, H.M.: Weighted Decomposition Construction for Perfect Secret Sharing Schemes. Comput. Math. Appl., 43 877–887 (2002)

[14] Csirmaz, L.: The dealer's random bits in perfect secret sharing schemes. Studia Sci. Math. Hungar. 32, 429-437 (1996)

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

[16] Csirmaz, L.: An impossibility result on graph secret sharing. Des. Codes Cryptogr. 53, 195–209 (2009)

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

[18] Csirmaz, L., Tardos, G.: Optimal Information Rate of Secret Sharing Schemes on Trees. IEEE Trans. Inform. Theory 59, 2527–2530 (2013)

[19] Csiszar, I., Körner, J.: Information theory : coding theorems for discrete memoryless systems. Academic Press ; Akademiai Kiado, New York : Budapest, (1981)

[20] van Dijk, M.: On the information rate of perfect secret sharing schemes. Des. Codes Cryptogr. 6, 143–169 (1995)

[21] van Dijk, M.: More information theoretical inequalities to be used in secret sharing? Inform. Process. Lett. 63, 41–44 (1997)

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

[23] Dougherty, R., Freiling, C., Zeger, K.: Linear rank inequalities on five or more variables. Available at arXiv.org, arXiv:0910.0284v3 (2009)

[24] Dougherty, R., Freiling, C., Zeger, K.: Non-Shannon Information Inequalities in Four Random Variables. Available at arXiv.org, arXiv:1104.3602v1 (2011)

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

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

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

[28] Gács, P., Körner, J.: Common information is far less than mutual information. Problems of Contr. and Inf. Th. 2, 149-162 (1973)

[29] Gharahi, M: On the Complexity of Perfect Secret Sharing Schemes. Ph.D. Thesis (in Persian), Iran University of Science and Technology (2013)

[30] Gharahi, M., Dehkordi, M.H: The complexity of the graph access structures on six participants, Des. Codes Cryptogr. 67, 169–173 (2013)

[31] Gharahi, M., Dehkordi, M.H: Average complexities of access structures on five participants. Adv. in Math. of Comm. 7, 311–317 (2013)

[32] Gharahi, M., Dehkordi, M.H: Perfect secret sharing schemes for graph access structures on six participants. J. Mathematical Cryptology 7, 143–146 (2013)

[33] Gharahi, M., Khazaei, S.: Reduced access structures with four minimal qualified subsets on six participants. Adv. Math. Commun. 12, 199–214 (2018).

[34] Gharahi, M., Khazaei, S.: Optimal Linear Secret Sharing Schemes for Graph Access Structures on Six Participants. Theoret. Comput. Sci. 771, 1–8 (2019)

[35] Emirhan Gürpinar, Andrei E. Romashchenko: How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma. ISIT 2019: 1377–1381. Also available at arxiv.org: CoRR abs/1901.07476 (2019)

[36] Hammer, D., Romashchenko, A.E., Shen, A., Vereshchagin, N.K.: Inequalities for Shannon entropy and Kolmogorov complexity. Journal of Computer and Systems Sciences 60, 442–464 (2000)

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

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

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

[40] Jafari, A., Khazaei, S.: On Abelian Secret Sharing: duality and separation. Cryptology ePrint Archive, Report 2019/575 (2019)

[41] Kaced, T.: Equivalence of Two Proof Techniques for Non-Shannon Inequalities. arXiv:1302.2994 (2013)

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

[43] Kinser., R.: New inequalities for subspace arrangements. J. Combin. Theory Ser. A 118, 152–161 (2011)

[44] Li, Q., Li, X.X., Lai, X.J., Chen, K.F.: Optimal assignment schemes for general access structures based on linear programming. Des. Codes Cryptogr. 74, 623–644 (2015)

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

[46] Martí-Farré, J., Padró, C.: Secret Sharing Schemes with Three or Four Minimal Qualified Subsets. Des. Codes Cryptogr. 34, 17–34 (2005)

[47] Martí-Farré, J., Padró, C.: On secret sharing schemes, matroids and polymatroids. J. Math. Cryptol. 4, 95-120 (2010)

[48] Martí-Farré, J., Padró, C., Vázquez, L.: Optimal Complexity of Secret Sharing Schemes with Four Minimal Qualified Subsets. Des. Codes Cryptogr. 61, 167–186 (2011)

[49] Martín, S., Padró, C., Yang, A.: Secret sharing, rank inequalities, and information inequalities. IEEE Trans. Inform. Theory 62, 599-609 (2016)

[50] Matúš, F.: Infinitely many information inequalities. In: *Proc. IEEE International Symposium on Information Theory, (ISIT)*, pp. 2101–2105 (2007)

[51] Metcalf-Burton, J.R.: Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. Discrete Math. 311, 651–662 (2011)

[52] Oxley, J.G: Matroid theory. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York (1992)

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

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

[55] Padró, C., Vázquez, L., Yang, A.: Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. Discrete Applied Mathematics 161, 1072–1084 (2013)

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

[57] Rado, R.: Note on independence functions. Proc. London Math. Soc. (3) 7, 300–320 (1957)

[58] Robere, R., Pitassi, T., Rossman, B., Cook S.A.: Exponential Lower Bounds for Monotone Span Programs. FOCS 2016: 406–415

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

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

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

[62] Stinson, D.R.: An explication of secret sharing schemes. Des. Codes Cryptogr. 2, 357-390 (1992)

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

[64] Thakor, S., Chan, T., Grant, A.: Capacity bounds for networks with correlated sources and characterisation of distributions by entropies. IEEE Trans. Inform. Theory 63, 3540-3553 (2017)

[65] Tian, C.: Characterizing the Rate Region of the $(4, 3, 3)$ Exact-Repair Regenerating Codes. Available at arXiv.org, arXiv:1312.0914 (2013)

[66] Yeung, R.W.: A first course in information theory. Kluwer Academic/Plenum Publishers, New York (2002)

[67] Yeung, R.W.: Information theory and network coding. Springer (2008)

[68] Zhang, Z.: On a new non-Shannon type information inequality. Commun. Inf. Syst. 3, 47–60 (2003)

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