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

Oriol Farràs, Tarik Kaced, Sebastià Martín, and Carles Padró

September 20, 2017

Abstract

We present a new improvement in the Linear Programming technique to derive bounds on information theoretic problems. In our case, we deal with the search for lower bounds on the information ratio of secret sharing schemes. We obtain non-Shannon-type bounds without using information inequalities explicitly. Our new techniques makes it possible to determine the optimal information ratio of linear secret sharing schemes for all access structures on 5 participants. New lower bounds are presented also for graph-based access structures on six participants and for some small matroidal access structures. In particular, we determine the optimal information ratio of the linear secret sharing schemes for the ports of the Vamos matroid.

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

1 Introduction

Linear programming involving information inequalities has been extensively used in several existence and optimization information theoretic problems. For instance in secret sharing [58], network coding [69], or repairable codes [67]. 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 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 [64] and Blakley [8], is a very useful tool that appears as a component in many different kinds of cryptographic protocols. In a *secret sharing scheme*, a *secret value* is distributed into *shares* among a set of *participants* in such a way that 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* (*average information ratio*) of a secret sharing scheme is the ratio between the maximum (average) length of the shares and the length of the secret. The optimization of these parameters has attracted a lot of attention. Specifically, for a given access

structure Γ, one is interested in determining its *optimal information ratios* $\sigma(\Gamma)$ and $\lambda(\Gamma)$, and also its *optimal average information ratios* $\widetilde{\sigma}(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$. Here, $\sigma(\Gamma)$ denotes the infimum of the information ratios of *all* secret sharing schemes with access structure Γ, while for $\lambda(\Gamma)$ only *linear* secret sharing schemes are taken into account. The corresponding parameters for the average information ratio are defined accordingly.

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 [2] for more information about this topic. For *linear* secret sharing schemes, building up on the superpolynomial lower bounds in [1, 4], exponential lower bounds have been proved recently [60]. 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 [13, 14], who presented a family of access structures on an arbitrary number n of participants whose optimal information ratio is $\Omega(n/\log n)$.

The optimization of the information ratios has been analyzed for several families of access structures. For example, access structures defined by graphs [3, 9, 11, 15, 17, 19, 30, 32], access structures on a small number of participants [19, 30, 31, 32, 37, 58, 65], bipartite access structures [25, 57], the ones having few minimal qualified sets [45, 47], or the ports of non-representable matroids [5, 46, 54, 58].

Almost all lower bounds on the optimal information ratios have been obtained by the same method, which is called here the *linear programming (LP) technique*. In particular, the asymptotic lower bound $\Omega(n/\log n)$ found by Csirmaz [14] 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 [40], 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 [11]. Csirmaz [14] 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]. A new parameter $\kappa(\Gamma)$ was introduced in [46]. It is the best lower bound 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. The parameter $\widetilde{\kappa}(\Gamma)$ is defined analogously. The known values of the optimal information ratios have been determined by finding a lower bound on $\kappa(\Gamma)$ that is equal to an upper bound on $\lambda(\Gamma)$. The lower bound is obtained by (implicitly or explicitly) applying the LP-technique, and the upper bound is given by presenting a linear secret sharing scheme for the given access structure. For the access structures in that situation, $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma)$. Analogously, the access structures for which the optimal average information ratio has been determined satisfy $\widetilde{\kappa}(\Gamma) = \widetilde{\sigma}(\Gamma) = \widetilde{\lambda}(\Gamma)$.

A further improvement, which was first applied in [5], consists in adding to the game the so-called *non-Shannon information and rank inequalities*, that is, inequalities that are satisfied by the entropy function but cannot be derived from the basic Shannon inequalities. This addition provided several new lower bounds [5, 15, 54, 58] and also the first examples of access structures satisfying $\kappa(\Gamma) < \sigma(\Gamma)$, namely the ports of the Vamos matroid. Finally, Metcalf-Burton [54] and Padró, Vázquez and Yang [58] 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 not too large. In particular, the parameters $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ can be determined by solving linear programming problems. Again, new lower bounds for a number of access structures [25, 47, 54, 58] were obtained as a consequence of that improvement. Some limitations

of the LP-technique in the search for asymptotic lower bounds have been found [6, 14, 48]. Namely, the best lower bound that can be obtained by using all known information inequalities is linear in the number of participants, while at most polynomial lower bounds can be found by using all known or unknown inequalities on a bounded number of variables.

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. More specifically, all known non-Shannon rank inequalities, which provide lower bounds on $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, are derived from the *common information property* [23], while most of the known non-Shannon information inequalities are obtained by the techniques described in [38]. We derive from these properties some constraints to be added to the linear programming problems that are used to find lower bounds. We apply this improvement to several access structures on a small number of players and we find 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 [37] 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 lower bounds for some of the unsolved cases [58]. In addition, constructions of linear secret sharing schemes were presented in [31] improving some upper bounds. After those developments, only four cases remained unsolved. All solved cases satisfy $\kappa(\Gamma) = \lambda(\Gamma)$ and $\widetilde{\kappa}(\Gamma) = \widetilde{\lambda}(\Gamma)$. The negative result in [58, Proposition 7.1] clearly indicated that the solution could not be found by the LP-technique with only Shannon information inequalities. Moreover, adding non-Shannon information and rank inequalities to the linear programs did not produce any new lower bound [58]. In contrast, our enhanced LP-technique provides better lower bounds on for those unsolved cases, which are tight for *linear* secret sharing schemes. In particular, the values of $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ are now determined for *all* access structures on five participants, but some values of $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$ are still unkown. So, we partially concluded the project initiated by Jackson and Martin in [37]. Moreover, we found some of the smallest access structures with $\kappa(\Gamma) < \sigma(\Gamma)$ or $\widetilde{\kappa}(\Gamma) < \widetilde{\sigma}(\Gamma)$ and all the smallest access structures with $\kappa(\Gamma) < \lambda(\Gamma)$ or $\widetilde{\kappa}(\Gamma) < \widetilde{\lambda}(\Gamma)$.

A similar project was undertaken by van Dijk [19] 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 [19], and several advances were presented subsequently [12, 30, 32, 43, 58]. At this point, only nine cases remain unsolved. We have been able to find for them new lower bounds on $\lambda(\Gamma)$ by using our enhanced LP-technique. Again, these structures satisfy $\kappa(\Gamma) < \lambda(\Gamma)$.

In addition, we present new lower bounds on $\sigma(\Gamma)$ and $\lambda(\Gamma)$ for the ports of four non-representable matroids on eight points. We prove that all those access structures satisfy $\kappa(\Gamma) < \sigma(\Gamma)$. In particular, we determine the exact value of $\lambda(\Gamma)$ for the ports of the Vamos matroid and the matroid Q_8.

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 techniques described in [38]. Since the number of variables and constraints is exponential in the numper of participants, this can be done only for access struc-

tures on small sets. We think that our improved LP-technique could be used to derive new lower bounds on $\sigma(\Gamma)$ for infinite families of access structures in a similar way as the LP-technique has been previously used to that end. Since the known limitations of the LP-technique do not imply the contrary, it may be even possible to improve Csirmaz's [14] 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 4. Some constructions of linear secret sharing schemes that are needed to determine the corresponding values of $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$ are given in Section 5. We conclude the paper in Section 6 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 $X \smallsetminus Y$ for the set difference and $X \smallsetminus x$ for $X \smallsetminus \{x\}$.

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 $f(X) \le f(Y)$.

(P3) f is *submodular*: $f(X \cup Y) + f(X \cap Y) \le f(X) + f(Y)$ 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*.

We discuss in the following the well known connection between entropic and linear polymatroids, as described in [33]. 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, 59], from this discussion we can conclude the well known fact that every linear polymatroid is the multiple of an entropic polymatroid.

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 $Q = P \cup \{p_o\}$. 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* if it is a is $\mathbb{K}$-linear 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. Obviously, $\sigma(\Gamma) \le \lambda(\Gamma)$ and $\widetilde{\sigma}(\Gamma) \le \widetilde{\lambda}(\Gamma)$.

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 $(Q, f) = (Q, \alpha h)$. 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, $\widetilde{\kappa}(\Gamma)$:

$$\begin{aligned} \text{Minimize} \quad & (1/n) \sum_{x\in P} f(x) \\ \text{subject to} \quad & (N), (\Gamma 1), (\Gamma 2), (P1), (P2), (P3) \end{aligned}$$

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, $\kappa(\Gamma)$:

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & v \geq f(x) \text{ for every } x \in P \\ & (N), (\Gamma 1), (\Gamma 2), (P1), (P2), (P3) \end{array}$$

The parameters $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ are the best lower bounds on $\sigma(\Gamma)$ and, respectively, $\widetilde{\sigma}(\Gamma)$ that can be obtained by using only Shannon information inequalities. 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, 47, 58]. 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 [9, 11, 16, 17, 19, 37] 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 [13, 14])**.** *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 [14] 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 $\lambda(\Gamma^*) = \lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma^*) = \widetilde{\lambda}(\Gamma)$ [36], and also $\kappa(\Gamma^*) = \kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma^*) = \widetilde{\kappa}(\Gamma)$ [46]. In contrast, it is not known whether the analogous relation applies 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 $f(x) \geq 1$ for every feasible solution of the Linear Programming Problems 2.9 and 2.10. 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 [10], 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 structures 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 [63]. Additional results on matroid ports and ideal secret sharing schemes were proved in [46] by using the forbidden minor characterization of matroid ports by Seymour [62].

Theorem 2.15 ([46])**.** *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 [71] presented such an inequality for the first time, and many others have been found subsequently [22, 24, 51, 70]. This approach was first applied in [5] 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 $1 < \sigma(\Gamma) < 3/2$. These results have been improved [54] and extended to other non-linear matroids [58].

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 [34]. Other such rank inequalities have been presented afterwards [23, 42]. 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 [5, 15, 58].

On the negative side, Beimel and Orlov [6] 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 are known to date, 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 [14] 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 [48]. 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

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 $\mathbb{K}$-linear random variables. Indeed, if $S_1 = S|_{V_1}$ and $S_2 = S|_{V_2}$ for some vector subspaces V_1, V_2 of a $\mathbb{K}$-vector space V, then $S_3 = S|_{V_1 \cap V_2}$ conveys the common information of S_1 and S_2. The following definition is motivated by the concept of common information of a pair of random variables.

Definition 3.1. Consider a polymatroid (Q, f) and two sets $A, B \subseteq Q$. Then every subset $X_o \subseteq Q$ such that

- $f(X_oA) - f(A) = f(X_oB) - f(B) = 0$, and
- $f(X_o) = f(A) + f(B) - f(AB)$

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 3.2. 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 3.3. *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.*

Proof. Let $(V_x)_{x \in Q}$ be a collection of vector subspaces representing a $\mathbb{K}$-linear polymatroid (Q, f), and consider two subsets $A_0, A_1 \subseteq Q$. By taking $V_{x_o} = V_{A_0} \cap V_{A_1}$, an extension of our polymatroid to Qx_o is obtained in which x_o is a common information for (A_0, A_1). Obviously, this new polymatroid is $\mathbb{K}$-linear too. □

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 $\Sigma = (S_x)_{x \in Q}$ a linear 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 $(f(X))_{X \subseteq Q} \in \mathbb{R}^{\mathcal{P}(Qx_o)}$ is a feasible solution of the Linear Programming Problem 3.4.

Linear Programming Problem 3.4. The optimal value of this linear programming problem is a lower bound on $\widetilde{\lambda}(\Gamma)$:

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

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 3.5 is a lower bound on $\widetilde{\lambda}(\Gamma)$. Obviously, analogous modifications on the Linear Programming Problem 2.10 provide lower bounds on $\lambda(\Gamma)$.

Linear Programming Problem 3.5. The optimal value of this linear programming problem is a lower bound on $\widetilde{\lambda}(\Gamma)$:

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

3.2 Ahlswede and Körner's Information

In the general case, the common information between any two random variables might not exist. Therefore, we use the general construction of Ahlswede and Körner from [18, p.352] This construction was used to derive non-Shannon-type inequalities [44]. It is equivalent in power to the Zhang-Yeung technique (also known as the copy Lemma) [38].

Lemma 3.6 (Ahlswede-Körner Lemma, [18])**.** *Let $x_1, \ldots, x_n, w$ be $n+1$ jointly distributed random variables. Consider their respective M independent and identically distributed copies $X_1, \ldots, X_n, W$. Then there exists a random variable W' such that:*

- $H(W'|X_1, \ldots, X_n) = 0$,
- $H(X_J|W') - M \cdot H(x_J|w) = o(M)$, *for all* $\varnothing \neq J \subseteq [n]$.

We say that a polymatroid is *almost entropic* if it is the limit of a sequence of entropic polymatroids (see for instance [39]). The Ahlswede and Körner lemma can be seen as a way of creating a new random variable that satisfies additional entropy constraints with respect to the original random variables. In the limit, the constraints stated in the lemma can be stated in the langage of polymatroids.

Definition 3.7. Consider a polymatroid (Q, f), and subsets $Y_1, \ldots, Y_m, Z \subseteq Q$. Then every subset $Z_o \subseteq Q$ such that

- $f(Z_o|Y_1, \ldots, Y_m) = 0$, and
- $f(Y_J|Z_o) = f(Y_J|Z)$ for $J \subseteq [m]$

is called an *AK information for the subsets* $(Z, Y_1, \ldots, Y_m)$.

Definition 3.8. A polymatroid (Q, f) satisfies the *AK information property* if, for every tuple of $m+1$ variables $(Z, Y_{[m]})$ of subsets of Q, there exists an extension (Qz_o, f) of it such that z_o is an AK information for the tuple $(Z, Y_{[m]})$.

The following property is a corollary of Lemma 3.6.

Proposition 3.9. *Every almost entropic polymatroid satisfies the AK information property. Moreover, given an almost entropic polymatroid (Q, f) and a tuple $(Z, Y_{[m]})$ of subsets of Q, it can be extended to an* almost entropic *polymatroid (Qz_o, f) such that z_o is an AK information for the tuple $(Z, Y_{[m]})$. In particular, the extension also satisfies the AK information property.*

Proof. Since the Ahlswede and Körner lemma can be applied to any random variables, we can create an AK information for any tuple of variables of the polymatroid. This AK information is itself a random variable, therefore the resulting polymatroid is also almost entropic. □

We can now define a counterpart to the common information LP formulation. The following is a linear program to derive bound using additional constraints from AK information. Specifically we add k new random variables z_i that materialize the AK information between the subsets Z_i and $Y_{i1}, \cdots, Y_{im_i}$.

Linear Programming Problem 3.10. The optimal value of this linear programming problem is a lower bound on $\widetilde{\lambda}(\Gamma)$:

$$\begin{aligned}
\text{Minimize} \quad & (1/n)\sum_{x\in P} f(x) \\
\text{subject to} \quad & (N), (\Gamma 1), (\Gamma 2) \\
& f(z_i|Y_{i1}, \ldots, Y_{im_i}) = 0 \text{ for every } i = 1, \ldots, k \\
& f(Y_{iJ}|z_i) = f(Y_{iJ}|Z_i) \text{ for every } i = 1, \ldots, k \text{ and } J \subseteq [m_i] \\
& (P1), (P2), (P3) \text{ on the set } Qz_1 \ldots z_k
\end{aligned}$$

A similar program can be used to get bounds for the optimal information ratio by changing accordingly the objective function.

4 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.

4.1 Access Structures on Five Participants

Jackson and Martin [37] determined the optimal information ratios of most access structures on five participants. After some additional contributions [20, 31, 58], 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 [37]) and their duals Γ_{153}, Γ_{150}, Γ_{152}, and Γ_{151}, respectively. Following [37], 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. Each result applies 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 [20, 37], were determined in [58] by solving the Linear Programming Problems 2.9 and 2.10. The upper bounds were given in [37], except the one on $\widetilde{\lambda}(\Gamma_{53})$, which was proved in [31].

By [58, 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 3.4 and 3.10 with the specified settings, we obtain the bounds in Tables 1 and 2, respectively. In particular, $\kappa(\Gamma) < \sigma(\Gamma)$ for all those access structures. Observe that they are the access structures on least participants having this property.

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.

Access structure	Z	Y_1	Y_2	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).

4.2 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 [19] 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 [12, 30, 32, 43, 58], 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 [19]. All upper bounds were presented in [19], except the one for Γ_{93}, which was given in [43].

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. In particular, they satisfy $\kappa(\Gamma) < \lambda(\Gamma)$. Moreover, the optimal information ratio of linear secret sharing schemes for the access structures Γ_{91} and Γ_{93} is now determined to be equal to $8/5$. 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.

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	$p_o 3$	$8/5 \leq \lambda(\Gamma)$
Γ_{91}, Γ_{93}	6	$p_o 5$	$8/5 \leq \lambda(\Gamma)$

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

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

4.3 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 [55]). 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 [55].

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 $AG(3, 2)'$ [55]. 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 [55]. 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 [55] .

If, instead, the 4-points set 1256 is relaxed in $AG(3, 2)'$, one obtains the smallest non-linear matroid F_8 [55]. 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 [55]. 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 [55]. 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.

- $19/17 \leq \sigma(\mathcal{V}) \leq 4/3$.
- $21/19 \leq \sigma(\mathcal{V}^*) \leq 4/3$.
- $5/4 \leq \lambda(\mathcal{V}) = \lambda(\mathcal{V}^*) \leq 4/3$.
- $19/17 \leq \sigma(\Gamma)$ 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 [5, 54, 58] by using the LP-technique enhanced with the Ingleton inequality or with several information inequalities. The upper bounds for the ports of the Vamos matroid were presented in [46].

By solving the LP problems 3.5 and 3.10 for those access structures with the given choices, the lower bounds in Tables 4 and 5 are obtained. In particular, we have determined the exact value of $\lambda(\mathcal{V}) = \lambda(\mathcal{V}^*) = 4/3$. In addition, the construction we present in Section 5 implies $\lambda(\mathcal{Q}) = \lambda(\mathcal{Q}^*) = 4/3$.

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	Y_{11}	Y_{12}	Z_2	Y_{21}	Y_{22}	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}).

5 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

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

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

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

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

Finally, we present 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 [56, 66] for more information about λ-decompositions. Let $\mathbb{K}$ be a finite field with characteristic different from 2. The first scheme is the one giving by the $\mathbb{K}$-linear code with generator matrix

$$\left(\begin{array}{cccccccc}
0&0&0&0&1&1&1&1\\
0&0&1&1&0&0&1&1\\
0&1&0&1&0&1&0&1\\
1&1&1&1&1&1&1&1
\end{array}\right)$$

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

$$\left(\begin{array}{cccccccc}
0&0&0&0&1&1&1&1\\
0&0&1&1&0&0&1&1\\
0&1&z_2&1&z_4&1&z_6&1\\
1&1&1&1&1&1&1&1
\end{array}\right)$$

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

$$\left(\begin{array}{cccccccc}
0&0&0&0&1&1&1&1\\
0&-1&1&1&0&0&1&1\\
0&1&0&1&0&1&0&1\\
1&1&1&1&1&1&1&1
\end{array}\right)$$

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.

6 Open Problems

The first open problem worth mentioning is to fully conclude the project initiated by Jackson and Martin [37] by determining the values of $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$ for all access structures on five participants.

Many examples of access structures with $\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma)$ are known., and also examples with $\kappa(\Gamma) < \sigma(\Gamma)$ and $\kappa(\Gamma) < \lambda(\Gamma)$. An open problem is to find the smallest examples with $\sigma(\Gamma) < \lambda(\Gamma)$, and also find examples in each of the following situations: $\kappa(\Gamma) = \sigma(\Gamma) < \lambda(\Gamma)$, $\kappa(\Gamma) < \sigma(\Gamma) = \lambda(\Gamma)$, and $\kappa(\Gamma) < \sigma(\Gamma) < \lambda(\Gamma)$.

Another interesting problem is to find matroid ports such that $\sigma(\Gamma)$ or $\lambda(\Gamma)$ are greater than $3/2$ or even arbitrarily large.

The main direction for future work is to obtain a better understanding of the techniques introduced here in order to improve, if possible, the known asymptotic lower bounds on $\sigma(\Gamma)$.

References

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

[2] 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)

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

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

[5] 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.

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

[7] Benaloh, J., Leichter, J.: Generalized Secret Sharing and Monotone Functions. *Advances in Cryptology—CRYPTO'88, Lecture Notes in Comput. Sci.* **403** (1990) 27–35.

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

[9] 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)

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

[11] 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)

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

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

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

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

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

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

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

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

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

[21] van Dijk, M.: A Linear Construction of Secret Sharing Schemes. Des. Codes Cryptogr. 12, 161-201 (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] Gál, A.: A characterization of span program size and improved lower bounds for monotone span programs. Comput. Complexity 10, 277–296 (2001)

[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] 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)

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

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

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

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

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

[39] Kaced, T., Romashchenko, A.: Conditional Information Inequalities for Entropic and Almost Entropic Points. Proc. IEEE Trans. Information Theory, 59 (11), 7149–7167 (2013)

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

[41] Karchmer, M., Wigderson, A.: On span programs. In: Proc. of the 8th IEEE Structure in Complexity Theory, pp.102–111 (1993).

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

[43] 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)

[44] 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)

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

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

[47] 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)

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

[49] Massey, J.L.: Minimal codewords and secret sharing. *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, 1993, 276–279.

[50] Matúš, F.: Adhesivity of Polymatroids. Discrete Mathematics 307, 2464–2477 (2007)

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

[52] Matúš, F., Csirmaz, L.: Entropy region and convolution. IEEE Trans. Inform. Theory 62, 6007–6018 (2016)

[53] Mayhew, D., Royle, G.F.: Matroids with nine elements. J. Combin. Theory Ser. B 98, 415-431 (2008)

[54] 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)

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

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

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

[58] 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)

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

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

[61] Schrijver, A.: Combinatorial optimization. Polyhedra and efficiency. Springer-Verlag, Berlin (2003)

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

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

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

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

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

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

[68] Welsh, D.J.A.: Matroid Theory. Academic Press, London (1976)

[69] Yan, X., Raymond W. Yeung, R.W., Zhang, Z.: The Capacity Region for Multi-source Multi-sink Network Coding. 2007 IEEE International Symposium on Information Theory, 116–120 (2007)

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

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