Secret Sharing, Rank Inequalities, and Information Inequalities*

Sebastià Martín[1], Carles Padró[1], and An Yang[2]

[1]Universitat Politècnica de Catalunya, Barcelona, Spain
[2]Nanyang Technological University, Singapore

November 27, 2015

Abstract

Beimel and Orlov proved that all information inequalities on four or five variables, together with all information inequalities on more than five variables that are known to date, provide lower bounds on the size of the shares in secret sharing schemes that are at most linear on the number of participants. We present here another two negative results about the power of information inequalities in the search for lower bounds in secret sharing. First, we prove that all information inequalities on a bounded number of variables can only provide lower bounds that are polynomial on the number of participants. And second, we prove that the rank inequalities that are derived from the existence of two common informations can provide only lower bounds that are at most cubic in the number of participants.

Key words. Secret sharing, Information inequalities, Rank inequalities, Polymatroids.

1 Introduction

Secret sharing schemes, which were independently introduced by Shamir [34] and Blakley [8], make it possible to distribute a *secret value* into *shares* among a set of *participants* in such a way that only the *qualified sets* of participants can recover the secret value, while no information at all on the secret value is provided by the shares from an unqualified set. The qualifed sets form the *access structure* of the scheme.

This work deals with the problem of the size of the shares in secret sharing schemes for general access structures. The reader is referred to [2] for an up-to-date survey on this topic. Even though there exists a secret sharing scheme for every access structure [24], all known general constructions are impractical because the size of the shares grows exponentially with the number of participants. The general opinion among the researchers in the area is that this is unavoidable. Specifically, the following conjecture, which was formalized by Beimel [2], is generally believed to be true. It poses one of the main open problems in secret sharing, and a very difficult and intriguing one.

Conjecture 1.1. *There exists an $\epsilon > 0$ such that for every integer n there is an access structure on n participants for which every secret sharing scheme distributes shares of length $2^{\epsilon n}$, that is, exponential in the number of participants.*

*The material in this paper was presented in part at *Crypto 2013*, Santa Barbara, California, USA, and an earlier version of this paper was published in the Proceedings of *Crypto 2013*. Most of this research work was done while the second author was with Nanyang Technological University, Singapore

Nevertheless, not many results supporting this conjecture have been proved. No proof for the existence of access structures requiring shares of super-polynomial length has been found. Moreover, the best of the known lower bounds is the one given by Csirmaz [12], who presented a family of access structures on an arbitrary number n of participants that require shares of length $\Omega(n/\log n)$ times the length of the secret.

In contrast, super-polynomial lower bounds on the length of the shares have been obtained for linear secret sharing schemes [1, 3, 4, 21]. 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 needed for many applications of secret sharing. Moreover, most of the known constructions of secret sharing schemes yield linear schemes.

As in the works by Csirmaz [12] and by Beimel and Orlov [6], we analyze here the limitations of the technique that has been almost exclusively used to find lower bounds on the size of the shares for general (that is, not necessarily linear) secret sharing. This is the case of the bounds in [9, 10, 12, 25] and many other papers. Even though it was implicitly used before, the method was formalized by Csirmaz [12]. Basically, it consists of finding lower bounds on the solutions of certain linear programs. This method provides lower bounds on the *information ratio* of secret sharing schemes, that is, on the ratio between the maximum size of the shares and the size of the secret. The constraints of those linear programs are derived from inequalities that are satisfied by the values of the joint entropies of the random variables defining a secret sharing scheme. These constraints can be divided into three classes.

1. The ones that are derived from the access structure, specifically, from the fact that the qualified subsets can recover the secret while the unqualified ones have no information about it.

2. The so-called *Shannon inequalities*, which are the ones implied by the fact that the conditional mutual information is nonnegative or, equivalently, by the fact that the joint entropies of a collection of random variables define a polymatroid [18, 19].

3. Finally, constraints derived from *non-Shannon information inequalities*, that is, linear inequalities that hold for every collection of random variables and are independent from the Shannon inequalities.

Csirmaz [12] found a negative result on that method. Namely, the lower bounds that are obtained by considering only the constraints in the first two classes are at most linear on the number of participants. This was proved by showing that every such linear program admits a feasible solution with a small value of the objective function. Notice that the existence of non-Shannon information inequalities was unknown when the method was formalized.

The first non-Shannon information inequality was presented by Zhang and Yeung [37], and many others have been found subsequently [14, 16, 28, 36]. The existence of such additional constraints gave some expectations for the search of lower bounds and, actually, improvements were obtained for some particular access structures [5, 30, 31].

When searching for lower bounds for linear secret sharing schemes, one can improve the linear program by using *rank inequalities*, which apply to configurations of vector subspaces or, equivalently, to the joint entropies of collections of random variables defined from linear maps. 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 [23]. Other rank inequalities have been presented afterwards [15, 27]. The use of rank inequalities improved the known lower bounds on the information ratio of linear secret sharing schemes for some particular families of access structures [5, 13, 31].

Information and rank inequalities can be classified by the number of random variables they involve. For example, the basic Shannon information inequality, from which all other Shannon information inequalities are derived, is equivalent to the conditional mutual information being nonnegative, and hence it is an inequality on three variables. Ingleton and Zhang-Yeung inequalities are on four variables. Nevertheless, an inequality on a certain number of variables can be applied to larger collections of random variables by grouping them, and hence it can be used to find bounds for secret sharing schemes on an arbitrary number of participants.

Some difficulties arise when using non-Shannon rank and information inequalities in the search for lower bounds. First, only a few methods are currently available to derive rank and information inequalities [15, 26], and it seems that many of them remain unknown. And second, except for a few cases, no spanning sets are known for the information or rank inequalities on a given number of variables. Besides, even for four variables, there are infinitely many independent information inequalities [28].

Moreover, the aforementioned negative result by Csirmaz [12] was generalized by Beimel and Orlov [6], who presented a negative result about the power of non-Shannon information inequalities to provide better lower bounds on the size of the shares. Namely, they proved that the lower bounds 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, are at most linear on the number of participants. Specifically, they proved that every linear program that is obtained by using these inequalities admits a feasible solution that is related to the solution used by Csirmaz [12] to prove his negative result. They used the fact that there exists a finite set of rank inequalities that, together with the Shannon inequalities, span all rank inequalities, and hence all information inequalities, on four or five variables [15, 22]. By executing a brute-force algorithm using a computer program, they checked that Csirmaz's solution is compatible with every rank inequality in that finite set. In addition, they manually executed their algorithm on a symbolic representation of the infinite sequence of information inequalities given by Zhang [36]. This sequence contains inequalities on arbitrarily many variables and generalizes the infinite sequences from previous works.

In particular, the results in [6] imply that all rank inequalities on four or five variables cannot provide lower bounds on the size of shares in *linear* secret sharing schemes that are better than linear on the number of participants. Unfortunately, their algorithm is not efficient enough to be applied on the known rank inequalities on six variables.

We present here another two negative results about the power of rank and information inequalities to provide lower bounds on the size of the shares in secret sharing schemes.

Our first result deals with rank and information inequalities on a bounded number of variables. We prove in Theorem 6.2 that 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 of lower bounds for both linear and general secret sharing schemes. Therefore, information inequalities on arbitrarily many variables are needed to find super-polynomial lower bounds by using the method described above. The proof is extremely simple and concise. Similarly to the proofs in [6, 12], it is based on finding feasible solutions to the linear programs that are obtained by using rank inequalities on a bounded number of variables. These solutions are obtained from a family of polymatroids that are uniform and Boolean. This family contains the polymatroids that were used in [6, 12]. In some sense, our result is weaker than the one in [6], because for $r = 4$ and $r = 5$, our feasible solutions do not prove that the lower bounds must be linear on the number of participants, but instead quadratic and cubic, respectively. But in another sense our result is much more general because it applies to all (known or unknown) rank inequalities. In addition, our proof provides a better understanding on the limitations of the use of information

inequalities in the search of lower bounds for secret sharing schemes.

Our second result shows that, in addition to the number of variables, also the methods used to derive rank and information inequalities can imply limitations in the search of lower bounds. Only a few techniques are known to find rank and information inequalities [11, 15, 26, 29]. In particular, non-Shannon rank inequalities have been found by using *common informations* [15, 22]. Specifically, all known sharp rank inequalities are derived from the existence of *two* common informations [15]. We prove in Theorem 8.5 that all lower bounds on the length of the shares that can be obtained from such rank inequalities are at most cubic on the number of participants. Even though its proof is much more involved, this result is based on the same ideas as Theorem 6.2.

2 Notation

We begin by introducing some notation. For a finite set E, we use $\mathcal{P}(E)$ to denote its *power set*, that is, the set of all subsets of E. 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 $X \setminus \{x\}$. For a function $f : \mathcal{P}(E) \to \mathbb{R}$ and subsets $X, Y, Z \subseteq E$, we define

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

In addition, we notate $\Delta_f(Y{:}Z) = \Delta_f(Y{:}Z|\emptyset)$ and $\Delta_f(y{:}z|X) = \Delta_f(\{y\}{:}\{z\}|X)$. For a positive integer r, we use $[r]$ to represent the set $\{1, \ldots, r\}$. All through the paper, P will denote a finite set of *participants*, $p_o \notin P$ a special participant, usually called *dealer*, and $Q = Pp_o = P \cup \{p_o\}$.

We use subsets of a given finite set as subindices for random variables, vector spaces, and sets with different meanings that are described next. Nevertheless, the context in which this notation is used should avoid any confusion. Let E be a finite set and $X \subseteq E$.

1. If $(S_x)_{x \in E}$ is a random vector, then S_X denotes the subvector $(S_x)_{x \in X}$.
2. Let V be a vector space over a field $\mathbb{K}$ and $(V_x)_{x \in E}$ a tuple of vector subspaces of V. We notate $V_X = \sum_{x \in X} V_x$.
3. Finally, for a finite set M and a family $(M_x)_{x \in E}$ of subsets of M, we write $M_X = \bigcup_{x \in X} M_x$.

Other issues about notation that should be taken into account by the reader are explained in the following.

- Γ. It denotes an access structure (Definition 4.1). We use the same symbol Γ for a family of subsets and for the associated Boolean function
- $\sigma(\Sigma)$ denotes the information ratio of a secret sharing scheme (Definition 4.3).
- $\sigma(\Gamma)$, $\lambda(\Gamma)$, $\kappa(\Gamma)$. The optimal information ratio of an access structure Γ and related parameters that are introduced in Definitions 4.3 and 4.5.
- $\mathcal{S}$, $\mathcal{Z}$, $\mathcal{T}$. These calligraphic letters are used for polymatroids (Definition 3.1).
- $\mathcal{S}(\Gamma)$, $\mathcal{Z}(\Gamma)$, $\mathcal{T}(\Gamma)$. This notation, which is introduced in Definition 4.8, is used for polymaroids that are related to an access structure Γ.
- $\mathcal{Z}(P, r)$, $M(P, r)$. A family of Boolean polymatroids and the sets defining them. See Definition 5.3.

3 Polymatroids, Rank Inequalities, and Information Inequalities

Some basic concepts and facts about polymatroids that are used in the paper are presented here. A more detailed presentation can be found in textbooks on the topic [33, 35].

Definition 3.1. A *polymatroid* is a pair $\mathcal{S} = (E, f)$ formed by a finite set E, the *ground set*, and a *rank function* $f\colon \mathcal{P}(E) \to \mathbb{R}$ satisfying the following properties.

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

A polymatroid is called *integer* if its rank function is integer-valued. If $\mathcal{S} = (E, f)$ is a polymatroid and c is a positive real number, then (E, cf) is a polymatroid too, which is called a *multiple* of $\mathcal{S}$. A polymatroid $(\widehat{E}, g)$ is called an *extension* of a polymatroid (E, f) if $E \subseteq \widehat{E}$ and $g(X) = f(X)$ for every $X \subseteq E$. In general, we will use the same symbol for the rank function of a polymatroid and the rank function of an extension of it.

The polymatroid axioms can be presented in a more compact way.

Remark 3.2. A map $f\colon \mathcal{P}(E) \to \mathbb{R}$ is the rank function of a polymatroid with ground set E if and only if $f(\emptyset) = 0$ and $\Delta_f(Y\colon Z|X) \geq 0$ for every $X, Y, Z \subseteq E$.

The following characterization of rank functions of polymatroids is a straightforward consequence of [33, Theorem 44.1].

Proposition 3.3. *A map $f\colon \mathcal{P}(E) \to \mathbb{R}$ is the rank function of a polymatroid with ground set E if and only if $f(\emptyset) = 0$ and $\Delta_f(y\colon z|X) \geq 0$ for every $X \subseteq E$ and $y, z \in E \setminus X$.*

In the following, four important classes of polymatroids are discussed. Namely, the entropic, the linear, the Boolean, and the uniform polymatroids.

Only discrete random variables are considered in this paper. Consider a finite set E and a random vector $(S_x)_{x\in E}$. For every $X \subseteq E$, the Shannon entropy of the random variable $S_X = (S_x)_{x\in X}$ is denoted by $H(S_X)$. Given three random variables $(S_i)_{i\in[3]}$, 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

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

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

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

A fundamental fact about Shannon entropy is that the conditional mutual information is always nonnegative, and this implies the following result by Fujishige [18, 19].

Theorem 3.4. *Let $(S_x)_{x\in E}$ be a random vector. Consider the mapping $h\colon \mathcal{P}(E) \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(X) = H(S_X)$ if $\emptyset \neq X \subseteq E$. Then h is the rank function of a polymatroid with ground set E.*

Proof. Observe that $\Delta_h(Y{:}Z|X) = I(S_Y{:}S_Z|S_X) \geq 0$ for every $X, Y, Z \subseteq E$ and apply Remark 3.2. □

Because of the connection between Shannon entropy and polymatroids given by Theorem 3.4, and by analogy to the conditional entropy, we write $f(X|Y) = f(XY) - f(Y)$ if (E, f) is a polymatroid and $X, Y \subseteq E$.

Definition 3.5. A polymatroid $\mathcal{S} = (E, h)$ is called *entropic* if there exists a random vector $(S_x)_{x\in E}$ such that $h(X) = H(S_X)$ for every $X \subseteq E$.

Definition 3.6. Let V be a vector space over a field $\mathbb{K}$ and $(V_x)_{x\in E}$ a tuple of vector subspaces of V. For $X \subseteq E$, we notate $V_X = \sum_{x\in X} V_x$. Then the map $f\colon \mathcal{P}(E) \to \mathbb{Z}$ defined by $f(X) = \dim V_X$ for every $X \subseteq E$ is the rank function of an integer polymatroid $\mathcal{S} = (E, f)$. The tuple $(V_x)_{x\in E}$ is called a $\mathbb{K}$-*linear representation* of the polymatroid $\mathcal{S}$, which is said to be $\mathbb{K}$-*linearly representable* or simply $\mathbb{K}$-*linear*.

We discuss in the following the well known connection between entropic and linear polymatroids, as described in [22]. Let $\mathbb{K}$ be a finite field. Let V be a $\mathbb{K}$-vector space and let V^* be its *dual space*, which is formed by all linear forms $\alpha : V \to \mathbb{K}$. Let S be the random variable given by the uniform probability distribution on V^*. For every vector subspace $W \subseteq V$, the restriction of S to W determines a random variable $S|_W$, which is uniformly distributed over its support W^*. Therefore, $H(S|_W) = \log|\mathbb{K}| \dim W^* = \log|\mathbb{K}| \dim W$. A random vector $(S_x)_{x\in E}$ is called $\mathbb{K}$-*linear* if $S_x = S|_{V_x}$ for some collection $(V_x)_{x\in E}$ of vector subspaces of a $\mathbb{K}$-vector space V. An entropic polymatroid is $\mathbb{K}$-*linearly entropic* if it is determined by a $\mathbb{K}$-linear random vector. The following result is a consequence of the previous discussion and the fact that every linear polymatroid admits a linear representation over some finite field [15, 32].

Proposition 3.7. *For a finite field $\mathbb{K}$, every $\mathbb{K}$-linearly entropic polymatroid is a multiple of a $\mathbb{K}$-linear polymatroid. In addition, every linear polymatroid is a multiple of an entropic polymatroid.*

Definition 3.8. Consider a finite set M and a family $(M_x)_{x\in E}$ of subsets of M. For every $X \subseteq E$, take $M_X = \bigcup_{x\in X} M_x$. Then the map defined by $f(X) = |M_X|$ for every $X \subseteq E$ is the rank function of an integer polymatroid $\mathcal{S}$ with ground set E. The family $(M_x)_{x\in E}$ is called a *Boolean representation* of $\mathcal{S}$. *Boolean polymatroids* are those admitting a Boolean representation.

A Boolean polymatroid admits a $\mathbb{K}$-linear representation for every field $\mathbb{K}$. Indeed, the set $\mathbb{K}^M$ of all functions $\mathbf{v}\colon M \to \mathbb{K}$ is a $\mathbb{K}$-vector space. For every $w \in M$, consider the vector $\mathbf{e}^w \in \mathbb{K}^M$ given by $\mathbf{e}^w(w) = 1$ and $\mathbf{e}^w(w') = 0$ if $w' \neq w$. Obviously, $(\mathbf{e}^w)_{w\in M}$ is a basis of $\mathbb{K}^M$. For every $x \in E$, consider the vector subspace $V_x = \langle \mathbf{e}^w : w \in M_x \rangle$. Clearly, these subspaces form a $\mathbb{K}$-linear representation of $\mathcal{S}$.

Definition 3.9. A polymatroid $\mathcal{S}$ with ground set E is *uniform* if every permutation on E is an automorphism of $\mathcal{S}$.

If (E, f) is a uniform polymatroid, then the rank $f(X)$ of a set $X \subseteq E$ depends only on its cardinality, that is, there exist values $0 = f_0 \leq f_1 \leq \cdots \leq f_n$, where $n = |E|$, such that $f(X) = f_i$ for every $X \subseteq E$ with $|X| = i$. By Proposition 3.3, such a sequence $(f_i)_{1\leq i\leq n}$ defines a uniform polymatroid if and only if $f_i - f_{i-1} \geq f_{i+1} - f_i$ for every $i = 1, \ldots, n-1$. Clearly, a uniform polymatroid is univocally determined by its *increment vector* $\delta = (\delta_1, \ldots, \delta_n)$, where $\delta_i = f_i - f_{i-1}$. Observe that $\delta \in \mathbb{R}^n$ is the increment vector of a uniform polymatroid if and only

if $\delta_1 \geq \cdots \geq \delta_n \geq 0$. All uniform integer polymatroids are linearly representable. Specifically, a uniform integer polymatroid is $\mathbb{K}$-linear if the field $\mathbb{K}$ has at least as many elements as the ground set [17].

Definition 3.10. Given a positive integer r, a collection $(A_i)_{i\in[r]}$ of subsets of a set E, and $I \subseteq [r]$, we notate $A_I = \bigcup_{i\in I} A_i$. An *information inequality*, respectively *rank inequality*, on r variables consists of a collection $(\alpha_I)_{I\in\mathcal{P}([r])}$ of real numbers such that

$$\sum_{I\subseteq[r]} \alpha_I f(A_I) \geq 0$$

for every entropic, respectively linear, polymatroid (E, f) and for every collection $(A_i)_{i\in[r]}$ of r subsets of E.

By Proposition 3.7, every information inequality is also a rank inequality. The *Shannon inequalities* are the information inequalities that can be derived from the fact that the conditional mutual information is nonnegative or, equivalently, from Theorem 3.4. The Ingleton inequality [23] was the first known example of a rank inequality that is not a Shannon inequality. The first known non-Shannon information inequality was presented by Zhang and Yeung [37]. Subsequently, many other rank and information inequalities have been found in [14, 15, 16, 27, 28, 36] and other works.

4 Polymatroids and Secret Sharing

We introduce in this section some basic concepts, terminology and notation about secret sharing and its connection to polymatroids. The reader is addressed to [2] for a more detailed presentation.

Let P be a finite set of *participants*, $p_o \notin P$ a special participant, usually called *dealer*, and $Q = Pp_o = P \cup \{p_o\}$. This notation will be used from now on.

Definition 4.1. An *access structure* Γ on P is a *monotone increasing* family of subsets of P, that is, if $X \subseteq Y \subseteq P$ and $X \in \Gamma$, then $Y \in \Gamma$. To avoid anomalous situations, we assume always that $\emptyset \notin \Gamma$ and $P \in \Gamma$. The members of Γ are called *qualified sets*. An access structure Γ is determined by the family $\min\Gamma$ of its *minimal qualified sets*. An access structure Γ on P can be identified with a monotone increasing Boolean function $\Gamma : \mathcal{P}(P) \to \{0, 1\}$, where $\Gamma(X) = 1$ if and only if $X \in \Gamma$. The reader must be aware that we are using the same symbol Γ for both a family of subsets and the associated Boolean function.

From the several definitions of secret sharing in the literature, we use the following one. The reader is referred to [2] for a detailed discussion about how to define secret sharing.

Definition 4.2. A *secret sharing scheme* Σ on P with access structure Γ is a random vector $(S_x)_{x\in Q}$ such that $H(S_{p_o}) > 0$ and $H(S_{p_o}|S_X) = 0$ if $X \in \Gamma$ while $H(S_{p_o}|S_X) = H(S_{p_o})$ if $X \notin \Gamma$. The random variables S_{p_o} and $(S_x)_{x\in P}$ correspond, respectively, to the *secret value* and the *shares* that are distributed among the participants in P. A secret sharing scheme is $\mathbb{K}$-*linear* if it is a $\mathbb{K}$-linear random vector.

Observe that the participants in a qualified set can recover the secret value from their shares, while the shares of the participants in an unqualified set provide no information at all about the secret value.

Definition 4.3. The *information ratio* $\sigma(\Sigma)$ of the secret sharing scheme Σ is defined by

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

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. In addition, $\lambda(\Gamma)$ denotes the infimum of the information ratios of all linear secret sharing schemes for Γ.

For every $x \in Q$, let $\mathbf{S}_x$ be the support of the random variable S_x. If the secret value S_{p_o} is uniformly distributed, then

$$\sigma(\Sigma) \leq \frac{\max_{x \in P} \log |\mathbf{S}_x|}{\log |\mathbf{S}_{p_o}|}.$$

That is, the information ratio is at most the ratio between the maximum length of the shares and the length of the secret. Assuming that the secret value is uniformly distributed is not restrictive. Indeed, every secret sharing scheme can be transformed into a scheme with that property, having the same access structure, and shares of the same length [2]. Therefore, lower bounds on the optimal information ratio $\sigma(\Gamma)$ provide lower bounds on the length of the shares in the secret sharing schemes with access structure Γ. Lower bounds on $\lambda(\Gamma)$ play the same role if we restrict our optimization problem to linear secret sharing schemes.

We discuss next in detail the method formalized by Csirmaz [12] to find lower bounds on the optimal information ratio. It is based on the connection between Shannon entropy and polymatroids described in Theorem 3.4. Let $\Sigma = (S_x)_{x \in Q}$ be a secret sharing scheme on P and let $\mathcal{S} = (Q, h)$ be the entropic polymatroid determined by the random vector $(S_x)_{x \in Q}$, that is, $h(X) = H(S_X)$ for every $X \subseteq Q$. Both the access structure Γ and the information ratio $\sigma(\Sigma)$ of Σ are determined by the polymatroid $\mathcal{S}$. Indeed, $\Gamma(X) = \Delta_h(p_o{:}X)/h(p_o)$ for every $X \subseteq P$ and $\sigma(\Sigma) = \max_{x \in P} h(x)/h(p_o)$. This motivates the following definition.

Definition 4.4. For an access structure Γ on P, a polymatroid (Q, f) such that

$$\Gamma(X) = \frac{\Delta_f(p_o{:}X)}{f(p_o)}$$

for every $X \subseteq P$ is called a Γ-*polymatroid*. A Γ-polymatroid is said to be *normalized* if $f(p_o) = 1$.

Definition 4.5. For an access structure Γ on P, we define $\kappa(\Gamma)$ as the infimum of $\max_{x \in P} f(x)$ over all normalized Γ-polymatroids (Q, f).

Proposition 4.6. *For every access structure Γ, the value $\kappa(\Gamma)$ is a lower bound on the optimal information ratio $\sigma(\Gamma)$.*

Proof. Let Σ be a secret sharing scheme with access structure Γ and let (Q, h) be the entropic polymatroid determined be the random vector Σ. For every $X \subseteq Q$, take $f(X) = h(X)/h(p_o)$. Then (Q, f) is a normalized Γ-polymatroid, and hence $\kappa(\Gamma) \leq \max_{x \in P} f(x) = \sigma(\Sigma)$. □

Most of the known lower bounds on the information ratio, as the ones from [9, 10, 12, 25], are lower bounds on $\kappa(\Gamma)$. In fact, this is the case for all lower bounds that can be obtained by using only Shannon inequalities. Clearly, the value $\kappa(\Gamma)$ can be determined by solving the linear programming problem that is described next. Therefore, the infimum in Definition 4.5 is a minimum and $\kappa(\Gamma)$ is a rational number.

Remark 4.7. The value $\kappa(\Gamma)$ is the optimal value of the linear programming problem:

- minimize v
- subject to
  1. $v \geq f(x)$ for every $x \in P$,
  2. $f(p_o) = 1$,
  3. $\Delta_f(p_o{:}X) = \Gamma(X)$ for every $X \subseteq P$, and
  4. $\Delta_f(y{:}z|X) \geq 0$ for every $X \subseteq Q$ and $y, z \in Q \smallsetminus X$.

Observe that the unknowns are $f(X)$ for $X \subseteq Q$ and the additional variable v.

In addition to the first two technical constraints, we have the constraints derived from the access structure (3) and the ones given by the Shannon information inequalities (4). Non-Shannon information inequalities and rank inequalities can be added as constraints to that linear program to find better lower bounds on $\sigma(\Gamma)$ and $\lambda(\Gamma)$, respectively. This has been done for several families of access structures [5, 13, 30, 31]. The objective of this work is to present some limitations of this method. It is achieved by proving that the linear programming problem above, augmented with some information and rank inequalities, admits feasible solutions with small values of the objective function. Specifically, we present in the following sections constructions of feasible solutions for the linear programming problems that include as constraints either rank inequalities on a bounded number of variables or rank inequalities that are derived from the existence of two common informations. We finish this section with a result that will greatly simplify our task.

Definition 4.8. An access structure Γ on a set P and a polymatroid $\mathcal{S} = (P, f)$ are said to be *compatible* if $\mathcal{S}$ can be extended to a normalized Γ-polymatroid $(Q, f) = (Pp_o, f)$. In this situation, the only extension of $\mathcal{S}$ that is a normalized Γ-polymatroid is denoted by $\mathcal{S}(\Gamma)$.

Remark 4.9. Clearly, $\kappa(\Gamma)$ is the minimum of $\max_{x \in P} f(x)$ over all polymatroids (P, f) that are compatible with Γ.

The following characterization of compatibility between access structures and polymatroids is a variant of a result by Csirmaz [12, Proposition 2.3].

Proposition 4.10. *A polymatroid $\mathcal{S} = (P, f)$ is compatible with an access structure Γ on P if and only if $\Delta_f(y{:}z|X) \geq \Delta_\Gamma(y{:}z|X)$ for every $X \subseteq P$ and $y, z \in P \smallsetminus X$, that is, if and only if $(P, f - \Gamma)$ is a polymatroid.*

Proof. Extend the rank function f of $\mathcal{S}$ to $\mathcal{P}(Q)$ by taking $f(Xp_o) = f(X) + 1 - \Gamma(X)$ for every $X \subseteq P$. This is the only possible extension of f that can produce a normalized Γ-polymatroid. Therefore, $\mathcal{S}$ is compatible with Γ if and only if (Q, f) is a polymatroid. By Proposition 3.3, (Q, f) is a polymatroid if and only if $\Delta_f(y{:}z|X) \geq 0$ for every $X \subseteq Q$ and $y, z \in Q \smallsetminus X$. Since (P, f) is a polymatroid, (Q, f) is a polymatroid if and only if the following conditions are satisfied.

1. $\Delta_f(y{:}z|Xp_o) \geq 0$ for every $X \subseteq P$ and $y, z \in P \smallsetminus X$.
2. $\Delta_f(p_o{:}z|X) \geq 0$ for every $X \subseteq P$ and $z \in Q \smallsetminus X$.

The second condition is always satisfied and the first one is equivalent to the condition in the statement. □

Remark 4.11. Observe that $\Delta_\Gamma(Y{:}Z|X) \in \{-1, 0, 1\}$ for every $X, Y, Z \subseteq P$. In addition, $\Delta_\Gamma(Y{:}Z|X) = 1$ if and only if $XY, XZ \in \Gamma$ and $X \notin \Gamma$.

5 A Family of Uniform Boolean Polymatroids

The feasible solutions that are required to prove our negative results are derived from a family of polymatroids that are both uniform and Boolean. These polymatroids appear in one of the most basic constructions of secret sharing schemes. Namely, a particular case of the construction of secret sharing schemes from monotone Boolean formulas proposed by Benaloh and Leichter [7].

In such a scheme, one begins with a pool of independent random bits. Every participant receives some of those random bits as its share while the secret value is the exclusive-or of some random bits from the pool. This kind of schemes is related to Boolean polymatroids, as we can see from a more formal description of this construction. For a finite set M, consider the random vector $(U_i)_{i\in M}$ corresponding to the uniform distribution on $\mathbb{F}_2^M$, where $\mathbb{F}_2$ is the finite field of two elements. Every participant $x \in P$ is associated to a set $M_x \subseteq M$, while another set $T \subseteq M$ is taken for the dealer p_o. Consider the random variable $S_{p_o} = \sum_{i\in T} U_i$ and, for every $x \in P$, the random variable $S_x = (U_i)_{i\in M_x}$. The random vector $(S_x)_{x\in Q}$ determines an $\mathbb{F}_2$-linear secret sharing scheme Σ. The access structure of Σ is formed by the sets $X \subseteq P$ such that $T \subseteq M_X = \bigcup_{x\in X} M_x$. The entropic polymatroid $\mathcal{S} = (Q, h)$ that is determined by Σ satisfies that $h(X) = |M_X|$ for every $X \subseteq P$. Therefore, the polymatroid (P, h) is Boolean. Clearly, this construction applies to any finite field.

Every access structure Γ admits such a secret sharing scheme. Indeed, consider $M = \mathcal{P}(P)$, and take $T = \mathcal{P}(P) \setminus \Gamma$ and $M_x = \{Y \subseteq P : x \notin Y\}$ for every $x \in P$. Clearly, $X \in \Gamma$ if and only if $T \subseteq M_X$. Therefore, for every finite field $\mathbb{K}$ and for every access structure Γ on a set of n participants, there exists a $\mathbb{K}$-linear secret sharing scheme for Γ with information ratio 2^{n-1}.

Inspired by the connection of the previous construction with Boolean polymatroids, we present next a family of polymatroids that contains, for every finite set P, a uniform Boolean polymatroid $\mathcal{Z} = (P, f)$ that is compatible with every access structure Γ on P. and such that the normalized Γ-polymatroid $\mathcal{Z}(\Gamma) = (Q, f)$ satisfies all rank inequalities on at most r variables. We skip the proofs of the following results, which are straightforward consequences of Proposition 4.10.

Proposition 5.1. *A polymatroid (P, f) is compatible with all access structures on P if and only if $\Delta_f(y{:}z|X) \geq 1$ for every $X \subseteq P$ and $y, z \in P \setminus X$.*

Proposition 5.2. *A uniform polymatroid on a set P of n participants is compatible with all access structures on P if and only if its increment vector $(\delta_1, \ldots, \delta_n)$ is such that $\delta_i \geq \delta_{i+1} + 1$ for $i = 1, \ldots, n-1$ and $\delta_n \geq 1$.*

Definition 5.3. Given a set P with $|P| = n$ and an integer $r \geq 2$, let $M(P, r) \subseteq \mathcal{P}(P)$ be the set of all subsets of P with at most r elements. For every $x \in P$, let $M_x(P, r)$ be the set formed by the subsets $M(P, r)$ that contain x. Finally, we define $\mathcal{Z}(P, r) = (P, f)$ as the Boolean polymatroid on P defined by the family $(M_x(P, r))_{x\in P}$.

As usual, we notate $M_X(P, r) = \bigcup_{x\in X} M_x(P, r)$ for every $X \subseteq P$. Clearly, every permutation on P is an automorphism of $\mathcal{Z}(P, r)$, and hence this polymatroid is uniform.

Proposition 5.4. *The polymatroid $\mathcal{Z}(P, r)$ is compatible with every access structure on P.*

Proof. By Proposition 5.2, it is enough to prove that the increment vector $\delta = (\delta_1, \ldots, \delta_n)$ of $\mathcal{Z}(P, r)$ is such that $\delta_i \geq \delta_{i+1} + 1$ for $i = 1, \ldots, n-1$ and $\delta_n \geq 1$. We can suppose that $P = [n] = \{1, \ldots, n\}$. Then δ_i is the number of subsets of P with at most r elements that contain i but do not contain any element in $\{1, \ldots, i-1\}$. Those subsets are in one-to-one correspondence with the subsets of $\{i+1, \ldots, n\}$ with at most $r-1$ elements. Clearly, this concludes the proof. □

By Proposition 5.4 with $r = 2$ and Remark 4.9, we have that $\kappa(\Gamma) \leq n$ for every access structure Γ on n participants [12]. The *Csirmaz function* introduced in [6, Definition 3.10] coincides with the rank function of $\mathcal{Z}(P, 2)$. The rank function of $\mathcal{Z}(P, 2)$ is the smallest among the rank functions of all uniform polymatroids on P that are compatible with all access structures on P [6, Lemma 3.11]. Finally, observe that [6, Lemma 6.2] is a straightforward consequence of the fact that $\mathcal{Z}(P, 2)$ is a Boolean polymatroid.

6 On Rank Inequalities on a Bounded Number of Variables

This section is devoted to prove our first main result, Theorem 6.2.

Proposition 6.1. *Let P be a set of n participants and Γ an access structure on P. For an integer $r \geq 3$, consider $\mathcal{Z}_{r-1} = \mathcal{Z}(P, r-1)$ and the normalized Γ-polymatroid $\mathcal{Z}_{r-1}(\Gamma)$. Then $\mathcal{Z}_{r-1}(\Gamma)$ satisfies all rank inequalities on r variables.*

Proof. Let f be the rank function of $\mathcal{Z}_{r-1}(\Gamma)$. Consider a family $(A_i)_{i\in[r]}$ of subsets of Q. We are going to prove that, for every rank inequality $(\alpha_I)_{I\in\mathcal{P}([r])}$ on r variables,

$$\sum_{I\subseteq[r]} \alpha_I f(A_I) \geq 0.$$

Take $B_i = A_i \setminus \{p_o\}$. If $B_i \in \Gamma$ for every $i \in [r]$, then $B_I \in \Gamma$ for every nonempty set $I \subseteq [r]$ and

$$\sum_{I\subseteq[r]} \alpha_I f(A_I) = \sum_{I\subseteq[r]} \alpha_I f(B_I) \geq 0$$

because $\mathcal{Z}_{r-1}$ is a Boolean polymatroid, and hence it is linearly representable. So we can assume that $B_i \notin \Gamma$ for some $i \in [r]$.

We affirm that the proof is concluded by finding $T \subseteq M(P, r-1)$ such that $B_I \in \Gamma$ if and only if $T \subseteq M_{B_I}(P, r-1)$. Indeed, by applying the method described at the beginning of Section 5 to the sets T and $(M_x(P, r-1))_{x\in P}$, one can construct, for every finite field $\mathbb{K}$, a $\mathbb{K}$-linear secret sharing scheme $\Sigma = (S_x)_{x\in Q}$ on P. The access structure Γ' of Σ will be in general different from Γ but $B_I \in \Gamma'$ if and only if $B_I \in \Gamma$. Since the entropic polymatroid (Q, h) determined by Σ is $\mathbb{K}$-linearly entropic, it satisfies all rank inequalities by Proposition 3.7. Moreover, (P, h) is a multiple of $\mathcal{Z}_{r-1} = (P, f)$. In fact, $h(X) = \log|\mathbb{K}| f(X)$ for every $X \subseteq P$. Moreover, $h(A_I) = \log|\mathbb{K}| f(A_I)$ for every $I \subseteq [r]$. Indeed, $h(B_I) = \log|\mathbb{K}| f(B_I)$ because $B_I \subseteq P$ and $h(B_I p_o) = \log|\mathbb{K}| f(B_I p_o)$ because $B_I \in \Gamma$ if and only if $B_I \in \Gamma'$. Therefore,

$$\sum_{I\subseteq[r]} \alpha_I f(A_I) = \frac{1}{\log|\mathbb{K}|} \sum_{I\subseteq[r]} \alpha_I h(A_I) \geq 0$$

for every rank inequality $(\alpha_I)_{I\in\mathcal{P}([r])}$ on r variables. This proves our affirmation.

We proceed now to construct a set $T \subseteq M(P, r-1)$ with the required properties. Consider the family of sets $\Lambda \subseteq \mathcal{P}([r])$ formed by the maximal sets $J \subseteq [r]$ with $B_J \notin \Gamma$. Observe that $\emptyset \notin \Lambda$ because there exists $i \in [r]$ with $B_i \notin \Gamma$. Given $J \in \Lambda$, take a set $Y(J) \subseteq P$ with $|Y(J)| \leq r-1$ that contains, for every $i \in [r] \setminus J$, an element $x_i \in B_i \setminus B_J$. Such an element exists because $B_J \notin \Gamma$ and $B_{Ji} = B_J \cup B_i \in \Gamma$. Take $T = \{Y(J) : J \in \Lambda\} \subseteq M(P, r-1)$. Observe that $T = \{\emptyset\}$ if $\Lambda = \{[r]\}$. Finally, we prove that $B_I \in \Gamma$ if and only if $T \subseteq M_{B_I}(P, r-1)$. Suppose that $B_I \in \Gamma$. If $J \in \Lambda$, then $I \setminus J \neq \emptyset$ and $B_i \cap Y(J) \neq \emptyset$ for every $i \in I \setminus J$. Therefore $Y(J) \in M_{B_I}(P, r-1)$ for every $J \in \Lambda$, and hence $T \subseteq M_{B_I}(P, r-1)$. If $B_I \notin \Gamma$, then $I \subseteq J$ for some $J \in \Lambda$, and hence $Y(J) \notin M_{B_I}(P, r-1)$ and $T \not\subseteq M_{B_I}(P, r-1)$. □

Theorem 6.2. *For an access structure Γ on n participants, the best lower bound on $\lambda(\Gamma)$ that can be obtained by using rank inequalities on r variables is at most*

$$\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{r-2}$$

and hence $O(n^{r-2})$. As an immediate consequence, the same applies to the lower bounds on the optimal information ratio $\sigma(\Gamma)$ that are obtained by using information inequalities on r variables.

Proof. By Proposition 6.1, the polymatroid $\mathcal{Z}_{r-1}(\Gamma) = (Q, f)$ gives a feasible solution to any linear program that is obtained from rank inequalities on r variables. Therefore, every lower bound on $\lambda(\Gamma)$ derived from such a linear program is at most $\max_{x \in P} f(x) = \delta_1$, the first component of the increment vector of $\mathcal{Z}(P, r-1)$. □

The rank inequalities on 3 variables are Shannon inequalities and, moreover, they span all Shannon inequalities. Therefore, the case $r = 3$ in Theorem 6.2 corresponds to the negative result by Csirmaz [12].

The results in this work, together with the previously known limitations [6, 12], clearly indicate that new techniques are needed to find relevant advances in the search of a proof for Conjecture 1.1. Nevertheless, it could be the case that the conjecture is false and those results show the way to refute it. For instance, one could think that, for some integer r, the feasible solutions introduced here to prove Theorem 6.2 are linearly representable, and hence they provide secret sharing schemes with polynomial information ratio for all access structures. This is not possible because of the super-polynomial lower bounds on the information ratio of linear secret sharing schemes presented in [3].

7 Common Information

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, it is not possible to find a random variable conveying the common information of two given random variables [20]. 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 7.1. Consider a polymatroid (E, f) and two sets $A, B \subseteq E$. Then every subset $X_0 \subseteq E$ such that

- $f(X_0|A) = f(X_0|B) = 0$ and
- $f(X_0) = \Delta_f(A{:}B) = f(A) + f(B) - f(AB)$.

is called a *common information for the pair* (A, B). By an abuse of language, if $X_0 = \{x_0\}$, then the element x_0 is also called a common information for the pair (A, B).

Proposition 7.2. *Let (E, f) be a polymatroid, $A, B \subseteq E$, and $X_0 \subseteq E$ a common information for (A, B). Consider a subset $Y \subseteq E$ such that $f(Y|A) = f(Y|B) = 0$. Then $f(Y|X_0) = 0$.*

Proof. We prove first that $f(Y) \leq f(X_0)$ if $f(Y|A) = f(Y|B) = 0$. Indeed,

$$\begin{aligned} 0 \leq \Delta_f(A{:}B|Y) &= f(AY) + f(BY) - f(ABY) - f(Y) \\ &= f(A) + f(B) - f(AB) - f(Y) \\ &= f(X_0) - f(Y), \end{aligned}$$

where the second equality holds because $f(Y|A) = f(Y|B) = 0$. Therefore, $f(YX_0) \leq f(X_0)$ because $f(YX_0|A) = f(YX_0|B) = 0$. This concludes the proof. □

Let $(V_x)_{x\in E}$ be a collection of vector subspaces representing a $\mathbb{K}$-linear polymatroid $\mathcal{S} = (E, f)$, and consider two subsets $A, B \subseteq E$. By taking $V_{x_0} = V_A \cap V_B$, an extension of $\mathcal{S}$ to Ex_0 is obtained in which x_0 is a common information for (A, B). Obviously, this new polymatroid is $\mathbb{K}$-linear as well. In particular, if $\mathcal{S} = (E, f)$ is a Boolean polymatroid defined by a family $(M_x)_{x\in E}$ of sets, then the extension of $\mathcal{S}$ to Ex_0 given by $M_{x_0} = M_A \cap M_B$ is a Boolean polymatroid in which x_0 is a common information for (A, B).

Definition 7.3. Let k be a positive integer. A polymatroid (E, f) satisfies the *k-common information property* if, for every k pairs $(A_{i0}, A_{i1})_{i\in[k]}$ of subsets of E, there exists an extension $(\widehat{E}, f)$ of $\mathcal{S}$ such that, for every $i \in [k]$, there exists a common information $Y_i \subseteq \widehat{E}$ for the pair (A_{i0}, A_{i1})

Clearly, every linear polymatroid satisfies the k-common information property for all k. Every rank inequality on four variables is a combination of the Shannon inequalities and the Ingleton inequality [22]. If a polymatroid satisfies the 1-common information property, then it satisfies the Ingleton inequality [15], and hence it satisfies all information inequalities on 4 variables. Moreover, there exist 24 rank inequalities on five variables that, together with the Ingleton and Shannon inequalities, generate all rank inequalities on five variables [15]. All these inequalities are satisfied by every polymatroid with the 2-common information property [15], and hence such polymatroids satisfy all information inequalities on 5 variables. Moreover, according to [15], all known sharp rank inequalities are derived from the 2-common information property.

8 On Rank Inequalities Derived from Common Informations

Our second main result, Theorem 8.6, is proved in this section and the next one. Similarly to Theorem 6.2, we present feasible solutions to the corresponding linear programming problems that are obtained from the family of uniform Boolean polymatroids presented in Section 5. We are going to need the following technical result on Boolean polymatroids.

Lemma 8.1. *Let $(M_x)_{x\in E}$ be a Boolean representation of a polymatroid (E, f) and X, Y, Z subsets of E. Then $\Delta_f(Y{:}Z|X) = 0$ if and only if $M_Y \cap M_Z \subseteq M_X$.*

Proof. Observe that $M_Y \cap M_Z \subseteq M_X$ if and only if $M_X \cap M_Z = M_{XY} \cap M_Z$. In addition, $\Delta_f(Y{:}Z|X) = |M_{XY} \cap M_Z| - |M_X \cap M_Z|$. □

Let Γ be an access structure on a set P. Consider the uniform Boolean polymatroid $\mathcal{Z} = \mathcal{Z}(P, 4) = (P, f)$ and the polymatroid $\mathcal{Z}(\Gamma)$, the only extension of $\mathcal{Z}$ to $Q = Pp_o$ that is a normalized Γ-polymatroid. Take $M = M(P, 4)$ and $M_x = M_x(P, 4)$ for every $x \in P$. Then $(M_x)_{x\in P}$ is a Boolean representation of $\mathcal{Z}$. Consider a collection $(B_{i0}, B_{i1})_{i\in[k]}$ of pairs of subsets of P. Consider the Boolean extension $\mathcal{S} = (Py_1 \dots y_k, f)$ of $\mathcal{Z}$ that is given by the sets $M_{y_i} = M_{B_{i0}} \cap M_{B_{i1}}$ for $i \in [k]$. Then y_i is a common information for (B_{i0}, B_{i1}) in $\mathcal{S}$.

Consider the extension of Γ to $Py_1 \dots y_k$ such that, for every $X \subseteq P$ and $\{i_1, \dots, i_s\} \subseteq [k]$, the set $Xy_{i_1} \dots y_{i_s}$ is qualified if and only if $XB_{i_1 j_1} \dots B_{i_s j_s} \in \Gamma$ for every $(j_1, \dots, j_s) \in \{0,1\}^s$. We also use Γ to denote this extended access structure.

Lemma 8.2. *The polymatroid $\mathcal{S}$ and the access structure Γ on $Py_1 \dots y_k$ are compatible.*

Proof. By combining Proposition 4.10, Remark 4.11, and Lemma 8.1, we only have to prove that $M_y \cap M_z \not\subseteq M_X$ for every $X \subseteq Py_1 \dots y_k$ and $y, z \in Py_1 \dots y_k$ such that $Xy, Xz \in \Gamma$ and $X \notin \Gamma$. Without loss of generality, we can assume that $X = Yy_1 \dots y_s$ for some $Y \subseteq P$ and $0 \leq s \leq k$, and that $YB_{10} \dots B_{s0} \notin \Gamma$. If $y, z \in P$, then $y, z \notin YB_{10} \dots B_{s0}$, and hence $\{y, z\} \in (M_y \cap M_z) \smallsetminus M_X$. If $y \notin P$ and $z \in P$, we can assume that $y = y_k$. Then there exist $u_j \in B_{kj} \smallsetminus YB_{10} \dots B_{s0}$ for $j = 0, 1$ and $\{u_0, u_1, z\} \in (M_y \cap M_z) \smallsetminus M_X$. If $y, z \notin P$, we can assume that $y = y_k$ and $z = y_\ell$ for some $\ell > s$. Then $\{u_0, u_1, v_0, v_1\} \in (M_y \cap M_z) \smallsetminus M_X$ if $u_j \in B_{kj} \smallsetminus YB_{10} \dots B_{s0}$ and $v_j \in B_{\ell j} \smallsetminus YB_{10} \dots B_{s0}$. □

Proposition 8.3. *Let Γ be an access structure on P and $(B_{i0}, B_{i1})_{i \in [k]}$ a collection of pairs of subsets of P. Take $\mathcal{Z} = \mathcal{Z}(P, 4)$. Then there exists a polymatroid $(Qy_1 \dots y_k, f)$, extension of $\mathcal{Z}(\Gamma)$, such that y_i is a common information for (B_{i0}, B_{i1}) for every $i \in [k]$.*

Proof. The polymatroid $\mathcal{S}(\Gamma)$ satisfies the required properties. □

Observe that Proposition 8.3 does not imply that $\mathcal{Z}(\Gamma)$ satisfies the k-common information property, because the existence of common informations is guaranteed only for pairs of subsets of P but not for pairs of subsets of Q. Some additional difficulties appear when dealing with pairs of subsets involving the element p_o. We discuss this issue in the following.

Lemma 8.4. *Consider a pair (B_0, B_1) of subsets of P. Let (Q, g) be a Γ-polymatroid and let (Qy, g) be an extension such that y is a common information for (B_0, B_1).*

1. *If both B_0 and B_1 are qualified, then y is a common information for the pairs $(B_0 p_o, B_1)$, $(B_0, B_1 p_o)$, and $(B_0 p_o, B_1 p_o)$.*
2. *If $B_0 \in \Gamma$ and $B_1 \notin \Gamma$, then y is a common information for $(B_0 p_o, B_1)$ and yp_o is a common information for both $(B_0, B_1 p_o)$ and $(B_0 p_o, B_1 p_o)$.*
3. *If $B_0 B_1 \notin \Gamma$, then y is a common information for both $(B_0 p_o, B_1)$ and $(B_0, B_1 p_o)$, while yp_o is a common information for $(B_0 p_o, B_1 p_o)$.*

Proof. If $B_0, B_1 \in \Gamma$, then $g(yp_o|B_0) = g(yp_o|B_1) = 0$, and hence $g(yp_o) = g(y)$ by Proposition 7.2. If $B_1 \notin \Gamma$, then $g(yp_o) - g(y) = g(p_o|y) \geq g(p_o|B_1) = 1$ and $g(yp_o) = g(y) + 1$. Observe that $g(yp_o|B_i p_o) = 0$ for $i = 0, 1$. In addition, $g(yp_o|B_i) = 0$ if and only if $B_i \in \Gamma$. By taking these facts into account, one can easily check all statements. □

One situation is missing in Lemma 8.4, namely $B_0, B_1 \notin \Gamma$ and $B_0 B_1 \in \Gamma$. In this case, neither y nor yp_o provides common informations for the pairs $(B_0 p_o, B_1)$ and $(B_0 p_o, B_1 p_o)$. A method to find those common informations is given in the proof of Proposition 8.5. Take $\mathcal{Z}' = (P, g) = (P, 3f)$, a multiple of the polymatroid $\mathcal{Z}(P, 4) = (P, f)$. Obviously, $\mathcal{Z}'$ is compatible with all access structures on P.

Proposition 8.5. *For every access structure Γ on P, the polymatroid $\mathcal{Z}'(\Gamma)$ satisfies the 2-common information property.*

Before giving the proof of this proposition, we present the main result of this section. It is a consequence of Proposition 8.5 and the value of $\max_{x \in P} g(x)$, where g is the rank function of $\mathcal{Z}'(\Gamma)$.

Theorem 8.6. *For an access structure Γ on n participants, the best lower bound on $\lambda(\Gamma)$ that can be obtained by using rank inequalities that can be derived from the 2-common information property is at most*

$$3\left(1+(n-1)+\binom{n-1}{2}+\binom{n-1}{3}\right)$$

and hence $O(n^3)$.

9 A Complicated Proof

This section is devoted to the proof of Proposition 8.5, which is quite involved and tedious. The proof is divided into several partial results.

Consider two pairs $(A_{i0}, A_{i1})_{i\in[2]}$ of subsets of Q and take $B_{ij} = A_{ij} \smallsetminus \{p_o\}$. For the pairs $(B_{i0}, B_{i1})_{i\in[2]}$, consider the extension $\mathcal{S} = (Py_1y_2, f)$ of $\mathcal{Z}(P, 4) = (P, f)$ and the extension of Γ to Py_1y_2 as defined at the beginning of Section 8. Recall that y_i is a common information of (B_{i0}, B_{i1}) for $i = 1, 2$ and that the polymatroid $\mathcal{S}$ is compatible with the access structure Γ. Obviously, these properties hold as well for the polymatroid $\mathcal{T} = (Py_1y_2, g) = (Py_1y_2, 3f)$. Observe that the polymatroid $\mathcal{T}(\Gamma) = (Qy_1y_2, g)$ is an extension of $\mathcal{Z}'(\Gamma)$.

Assume that there is no common information in $\mathcal{T}(\Gamma)$ for the pair (A_{10}, A_{11}). Then, by Lemma 8.4, we can suppose that $p_o \in A_{10}$ and $B_{10}, B_{11} \notin \Gamma$ while $B_{10} \cup B_{11} \in \Gamma$. We construct next an extension of $\mathcal{T}(\Gamma)$ in which there is a common information for that pair. Extend $\mathcal{Z}'$ to $Py_1y_2z_1$ by taking, for every $X \subseteq Py_1y_2$,

- $g(Xz_1) = g(Xy_1)$ if $XB_{10} \in \Gamma$, and
- $g(Xz_1) = g(Xy_1) + 1$ otherwise.

In addition, consider the extension of Γ to $Py_1y_2z_1$ such that, for every $X \subseteq Py_1y_2$, the set Xz_1 is qualified if and only if $XB_{11} \in \Gamma$. Observe that $g(y_1|z_1) = 0$ and that $Xz_1 \in \Gamma$ if $Xy_1 \in \Gamma$.

Lemma 9.1. *$(Py_1y_2z_1, g)$ is a polymatroid, and it is compatible with the access structure Γ. Moreover, in the extension $(Qy_1y_2z_1, g)$ of $\mathcal{T}(\Gamma)$, The sets z_1 and z_1p_o are common informations for the pairs (A_{10}, B_{11}) and $(A_{10}, B_{11}p_o)$, respectively.*

Proof. By combining Propositions 3.3 and 4.10, it is enough to prove that

$$\Delta_g(y{:}z|X) \geq \max\{0, \Delta_\Gamma(y{:}z|X)\}$$

for every $X \subseteq Py_1y_2z_1$ and $y, z \in Py_1y_2z_1 \smallsetminus X$. We distinguish three cases.

Case 1 *$X \subseteq Py_1y_2$ and $y = z = z_1$.* Then $\Delta_g(z_1{:}z_1|X) = g(Xz_1) - g(X) \geq 0$. If this quantity is equal to 0 and $\Delta_\Gamma(z_1{:}z_1|X) = 1$, then $X \notin \Gamma$, $Xz_1 \in \Gamma$, and $g(Xz_1) = g(Xy_1)$. Therefore, both sets XB_{10}, XB_{11} are qualified, and hence $Xy_1 \in \Gamma$ and $g(Xy_1) - g(X) \geq 1$, a contradiction.

Case 2 *$Xy \subseteq Py_1y_2$ and $z = z_1$.* Then $\Delta_g(y{:}z_1|X) = \Delta_g(y{:}y_1|X) + \varepsilon$, where

$$\varepsilon = g(Xz_1) - g(Xy_1) - (g(Xyz_1) - g(Xyy_1)) \geq 0.$$

Suppose that $\varepsilon = 0$ and $\Delta_\Gamma(y{:}z_1|X) = 1$. Then $X \notin \Gamma$ while $Xy \in \Gamma$ and $Xz_1 \in \Gamma$, and hence $XB_{10} \in \Gamma$ because $g(Xz_1) - g(Xy_1) = g(Xyz_1) - g(Xyy_1) = 0$. This implies that $Xy_1 \in \Gamma$, and hence $\Delta_g(y{:}y_1|X) \geq \Delta_\Gamma(y{:}y_1|X) \geq 1$.

Case 3 $X = Yz_1$ *with* $Yyz \subseteq Py_1y_2$. Take $\varepsilon = \Delta_g(y{:}z|Yz_1) - \Delta_g(y{:}z|Yy_1)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_0$, where $\varepsilon_0 = g(Yz_1) - g(Yy_1)$, $\varepsilon_1 = g(Yyz_1) - g(Yyy_1)$, $\varepsilon_2 = g(Yzz_1) - g(Yzy_1)$, and $\varepsilon_3 = g(Yyzz_1) - g(Yyzy_1)$. Since $0 \leq \varepsilon_3 \leq \varepsilon_1, \varepsilon_2 \leq \varepsilon_0 \leq 1$, we have that $\varepsilon \geq -1$. In addition,

$$\Delta_g(y{:}z|Yz_1) = \Delta_g(y{:}z|Yy_1) + \varepsilon = 3\Delta_f(y{:}z|Yy_1) + \varepsilon \tag{1}$$

If $\varepsilon = -1$, then $\varepsilon_0 = 1$ and $\varepsilon_1 = \varepsilon_2 = 0$, and hence $YB_{10} \notin \Gamma$ while $YyB_{10}, YzB_{10} \in \Gamma$. This implies that $M_y \cap M_z \not\subseteq M_{YB_{10}}$, and hence $M_y \cap M_z \not\subseteq M_{Yy_1}$ and $\Delta_f(y{:}z|Yy_1) \geq 1$. If $\Delta_\Gamma(y{:}z|Yz_1) = 1$, then $YB_{11} \notin \Gamma$ and $YyB_{11}, YzB_{11} \in \Gamma$. As before, $\Delta_f(y{:}z|Yy_1) \geq 1$.

Finally, we prove that z_1 is a common information for (A_{10}, B_{11}). Indeed, $g(A_{10}z_1) = g(B_{10}z_1) = g(B_{10}y_1) + 1 = g(B_{10}) + 1 = g(A_{10})$ and $g(B_{11}z_1) = g(B_{11}y_1) = g(B_{11})$. Moreover, $g(\{z_1\}) = g(\{y_1\}) + 1 = \Delta_g(B_{10}{:}B_{11}) + 1 = \Delta_g(A_{10}{:}B_{11})$. It is clear that z_1p_o is a common information for $(A_{10}, B_{11}p_o)$. □

Remark 9.2. From Equation (1), $\Delta_g(y{:}z|Yz_1) \geq 2$ if $\Delta_f(y{:}z|Yy_1) \neq 0$.

Assume now that there is no common information in $\mathcal{T}(\Gamma)$ for any of the pairs $(A_{i0}, A_{i1})_{i\in[2]}$. Then we can suppose that $p_o \in A_{i0}$ and $B_{i0}, B_{i1} \notin \Gamma$ while $B_{i0} \cup B_{i1} \in \Gamma$ for $i = 1, 2$. WE proved before that one can find, for $i = 1, 2$, an extension $(Qy_1y_2z_i, g)$ of $\mathcal{Z}'(\Gamma)$ such that z_i is a common information for (A_{i0}, B_{i1}). At this point, we have to extend $\mathcal{Z}'$ and Γ to $Py_1y_2z_1z_2$ in some way that is compatible with the previous extensions. This is done as follows.

First, we extend Γ to $Py_1y_2z_1z_2$ by setting that, for every $X \subseteq Py_1y_2$, the set Xz_1z_2 is qualified if and only if $XB_{11}B_{21} \in \Gamma$ and at least one of the sets $XB_{10}B_{20}$, $XB_{10}B_{21}$, $XB_{11}B_{20}$ is qualified. Observe that $Xz_1z_2 \in \Gamma$ if $Xz_1y_2 \in \Gamma$ or $Xy_1z_2 \in \Gamma$. Second, we extend the polymatroid $\mathcal{Z}'$ by giving the value of $g(Xz_1z_2)$ for every $X \subseteq Py_1y_2$.

1. If both $XB_{10}y_2$ and Xy_1B_{20} are qualified sets, then $g(Xz_1y_2) = g(Xy_1z_2) = g(Xy_1y_2)$, and hence we must take $g(Xz_1z_2) = g(Xy_1y_2)$.

2. If $XB_{10}y_2 \in \Gamma$ and $Xy_1B_{20} \notin \Gamma$, then $g(Xy_1y_2) = g(Xz_1y_2) = g(Xy_1z_2) - 1$. Therefore, $g(Xz_1z_2) = g(Xz_1y_2) + 1 = g(Xy_1z_2) = g(Xy_1y_2) + 1$ is the only possible option. Symmetrically, $g(Xz_1z_2) = g(Xz_1y_2) = g(Xy_1z_2) + 1 = g(Xy_1y_2) + 1$ if $XB_{10}y_2 \notin \Gamma$ and $Xy_1B_{20} \in \Gamma$.

3. Assume now that neither $XB_{10}y_2$ nor Xy_1B_{20} is a qualified subset. Then $g(Xz_1y_2) = g(Xy_1z_2) = g(Xy_1y_2) + 1$. If $Xz_1y_2 \in \Gamma$ and $Xy_1z_2 \in \Gamma$, then $g(Xz_1z_2) = g(Xz_1y_2) = g(Xy_1z_2)$. If at least one of the sets Xz_1y_2, Xy_1z_2 is unqualified and $Xz_1z_2 \in \Gamma$, then $g(Xz_1z_2) = g(Xz_1y_2) + 1 = g(Xy_1z_2) + 1$. If $Xz_1z_2 \notin \Gamma$ and both sets $XB_{10}B_{21}$ and $XB_{11}B_{20}$ are qualified, then $g(Xz_1z_2) = g(Xz_1y_2) = g(Xy_1z_2)$. Finally, if $Xz_1z_2 \notin \Gamma$ and one of the sets $XB_{10}B_{21}$ or $XB_{11}B_{20}$ is unqualified, then $g(Xz_1z_2) = g(Xz_1y_2) + 1 = g(Xy_1z_2) + 1$.

Lemma 9.3. *Consider two sets* X, Y *with* $X = Yz_1$ *with* $Y \subseteq X \subseteq Py_1y_2$ *and take* $\varepsilon_1 = g(Yz_1z_2) - g(Yz_1y_2)$ *and* $\varepsilon_2 = g(Xz_1z_2) - g(Xz_1y_2)$. *Then* $\varepsilon_1 \geq \varepsilon_2$.

Proof. Suppose that, on the contrary, $\varepsilon_1 = 0$ and $\varepsilon_2 = 1$. Then $Xy_1B_{20} \notin \Gamma$ because $\varepsilon_2 = 1$. Moreover, since $\varepsilon_1 = 0$, we have that $YB_{10}y_2 \notin \Gamma$ and both sets Yz_1y_2 and Yy_1z_2 are qualified, and hence $XB_{10}B_{20} \notin \Gamma$ and $XB_{10}y_2 \notin \Gamma$, a contradiction with $\varepsilon_2 = 1$. □

The proof of Proposition 8.5 is concluded with the following lemma.

Lemma 9.4. $(Py_1y_2z_1z_2, g)$ *is a polymatroid, and it is compatible with the access structure* Γ.

Proof. As in Lemma 9.1, we have to prove that $\Delta_g(y{:}z|X) \geq \max\{0, \Delta_\Gamma(y{:}z|X)\}$ for every $X \subseteq Py_1y_2z_1z_2$ and $y, z \in Py_1y_2z_1z_2 \smallsetminus X$. At this point, it is enough to consider the cases in which both z_1 and z_2 are involved.

Case 1 *$X \subseteq Py_1y_2$, and $y = z_1$ and $z = z_2$.* Then $\Delta_g(z_1{:}z_2|X) = \Delta_g(z_1{:}y_2|X) + \varepsilon_1 - \varepsilon_2$, where $\varepsilon_1 = g(Xz_2) - g(Xy_2)$ and $\varepsilon_2 = g(Xz_1z_2) - g(Xz_1y_2)$. Clearly, $\varepsilon_2 = 0$ if $\varepsilon_1 = 0$, and hence $\Delta_g(z_1{:}z_2|X) \geq 0$ by Lemma 9.1. Suppose that $\Delta_g(z_1{:}z_2|X) = 0$ and $\Delta_\Gamma(z_1{:}z_2|X) = 1$. Then $Xz_1, Xz_2 \in \Gamma$ and $\Delta_g(z_1{:}y_2|X) = \varepsilon_1 - \varepsilon_2 = 0$, which implies that $\Delta_\Gamma(z_1{:}y_2|X) = 0$ and $Xy_2 \notin \Gamma$. Then $\varepsilon_1 = 1$ by Lemma 9.1, and hence $\varepsilon_2 = g(Xz_1z_2) - g(Xz_1y_2) = 1$. By symmetry, $g(Xz_1z_2) - g(Xy_1z_2) = 1$. Therefore, at least one of the sets Xz_1y_2, Xy_1z_2 is unqualified, a contradiction.

Case 2 *$X = Yz_1$ with $Y \subseteq Py_1y_2$, and $y = z = z_2$.* Then $\Delta_g(z_2{:}z_2|Yz_1) = g(Yz_1z_2) - g(Yz_1) \geq 0$. Suppose that $\Delta_g(z_2{:}z_2|Yz_1) = 0$ and $\Delta_\Gamma(z_2{:}z_2|Yz_1) = 1$. Then $Yz_1 \notin \Gamma$ but $Yz_1z_2 \in \Gamma$. In addition $g(Yz_1z_2) = g(Yz_1y_2) = g(Yz_1)$, and hence $Yz_1y_2 \notin \Gamma$ by Lemma 9.1. Since $Yz_1z_2 \in \Gamma$, this implies that $YB_{11}B_{20} \notin \Gamma$, and hence $Yy_1B_{20} \notin \Gamma$, which leads to $g(Yz_1z_2) = g(Yz_1y_2) + 1$, a contradiction.

Case 3 *$X = Yz_1$ with $Yy \subseteq Py_1y_2$, and $z = z_2$.* In this case, $\Delta_g(y{:}z_2|Yz_1) = \Delta_g(y{:}y_2|Yz_1) + \varepsilon_1 - \varepsilon_2$, where $\varepsilon_1 = g(Yz_1z_2) - g(Yz_1y_2)$ and $\varepsilon_2 = g(Yyz_1z_2) - g(Yyz_1y_2)$. Then $\Delta_g(y{:}z_2|Yz_1) \geq 0$ because $\varepsilon_1 \geq \varepsilon_2$ by Lemma 9.3. Suppose now that $\Delta_g(y{:}z_2|Yz_1) = 0$ and $\Delta_\Gamma(y{:}z_2|Yz_1) = 1$. In particular, this implies that $\varepsilon_1 = \varepsilon_2$ and $\Delta_g(y{:}y_2|Yz_1) = \Delta_\Gamma(y{:}y_2|Yz_1) = 0$. Then $Yz_1y_2 \notin \Gamma$ and, since $Yz_1z_2 \in \Gamma$, we have that $YB_{11}B_{20} \notin \Gamma$ and $Yy_1B_{20} \notin \Gamma$. Therefore, $\varepsilon_1 = \varepsilon_2 = 1$, and hence $Yyy_1B_{20} \notin \Gamma$. Since $Yyz_1 \in \Gamma$, this implies that $YyB_{10}B_{20} \notin \Gamma$. So $YyB_{10}y_2 \notin \Gamma$ and $Yyy_1z_2 \notin \Gamma$. Therefore, none of the sets $YB_{10}B_{20}$, $YB_{10}B_{21}$, $YB_{11}B_{20}$ is qualified, a contradiction with $Yz_1z_2 \in \Gamma$.

Case 4 *$X = Yz_1z_2$, where $Yyz \subseteq Py_1y_2$.* Take $\varepsilon_0^1 = g(Yz_1z_2) - g(Yz_1y_2)$, $\varepsilon_1^1 = g(Yyz_1z_2) - g(Yyz_1y_2)$, $\varepsilon_2^1 = g(Yzz_1z_2) - g(Yzz_1y_2)$ and $\varepsilon_3^1 = g(Yyzz_1z_2) - g(Yyzz_1y_2)$. Consider also $\varepsilon_0^2 = g(Yz_1z_2) - g(Yy_1z_2)$, $\varepsilon_1^2 = g(Yyz_1z_2) - g(Yyy_1z_2)$, $\varepsilon_2^2 = g(Yzz_1z_2) - g(Yzy_1z_2)$ and $\varepsilon_3^2 = g(Yyzz_1z_2) - g(Yyzy_1z_2)$. Then

$$\Delta_g(y{:}z|Yz_1z_2) = \Delta_g(y{:}z|Yz_1y_2) + \varepsilon^1 = \Delta_g(y{:}z|Yy_1z_2) + \varepsilon^2,$$

where $\varepsilon^i = \varepsilon_1^i + \varepsilon_2^i - \varepsilon_3^i - \varepsilon_0^i$ for $i = 1, 2$. The result is obvious if $\{y, z\} \cap \{y_1, y_2\} \neq \emptyset$, so we can assume that $y, z \in P$. Observe that, by Lemma 9.3, $0 \leq \varepsilon_3^i \leq \varepsilon_1^i, \varepsilon_2^i \leq \varepsilon_0^i \leq 1$, and hence $\varepsilon^i \geq -1$. By Remark 9.2, $\Delta_g(y{:}z|Yz_1y_2) \geq 2$ If $\Delta_f(y{:}z|Yy_1y_2) \neq 0$. Suppose that $\Delta_f(y{:}z|Yy_1y_2) = 0$, that is, $M_y \cap M_z \subseteq M_{Yy_1y_2}$. Without loss of generality, we can assume that $y \in B_{10} \cap B_{11}$ or $y \in B_{10}$ and $z \in B_{11}$.

Suppose that $y \in B_{10} \cap B_{11}$ (observe that this covers the case $y = z$). Then $\varepsilon_1^1 = \varepsilon_0^1$ and $\varepsilon_3^1 = \varepsilon_2^1$, and hence $\varepsilon^1 = 0$. Moreover, $\Delta_\Gamma(y{:}z|Yz_1z_2) \leq 0$ because $Yz_1z_2y \notin \Gamma$ if $Yz_1z_2 \notin \Gamma$.

Suppose now that $y \in B_{10}$ and $z \in B_{11}$. We prove first that $\varepsilon^1 \geq 0$ or $\varepsilon^2 \geq 0$. Suppose that, otherwise, $\varepsilon_0^i = 1$ and $\varepsilon_1^i = \varepsilon_2^i = 0$ for $i = 1, 2$. Then both sets $YB_{10}y_2$ are Yy_1B_{20} are unqualified and one of the sets Yz_1y_2 and Yy_1z_2 is unqualified. Then $YyB_{10}y_2 \notin \Gamma$ and, since $\varepsilon_1^2 = 0$, this implies that $Yyy_1B_{20} \notin \Gamma$ and that either both sets Yyz_1y_2 and Yyy_1z_2 are qualified or $Yyz_1z_2 \notin \Gamma$ and both sets $YyB_{10}B_{21}$ and $YyB_{11}B_{20}$ are qualified. In both cases, $YyB_{10}B_{21} \in \Gamma$, and hence $YB_{10}B_{21} \in \Gamma$. We affirm that $Yzz_1y_2 \notin \Gamma$. Indeed, since $z \in B_{11}$, this is obvious if $Yz_1y_2 \notin \Gamma$. Otherwise, $Yy_1z_2 \notin \Gamma$, and hence $YB_{11}B_{21} \notin \Gamma$, which implies that $YzB_{11}B_{21} \notin \Gamma$ and $Yzz_1y_2 \notin \Gamma$. Our affirmation is now proved. Since $\varepsilon_2^i = 0$ for

$i = 1, 2$ either both sets $YzB_{10}y_2$ and Yzy_1B_{20} are qualified or both of them are unqualified and $Yzz_1z_2 \notin \Gamma$ while $YzB_{10}B_{21} \in \Gamma$ and $YzB_{11}B_{20} \in \Gamma$. In both cases, $YzB_{11}B_{20} \in \Gamma$, and hence $YB_{11}B_{20} \in \Gamma$, which implies that $YB_{11}B_{21} \notin \Gamma$ because $Yz_1y_2 \notin \Gamma$. Therefore, $Yz_1z_2 \notin \Gamma$, and hence $YB_{10}B_{21} \notin \Gamma$ because $\varepsilon_0^i = 1$ for $i = 1, 2$. We have reached a contradiction proving that $\varepsilon^1 \geq 0$ or $\varepsilon^2 \geq 0$. Next, we prove that $\Delta_\Gamma(y{:}z|Yz_1z_2) \leq 0$ if $\varepsilon^1 = \varepsilon^2 = 0$. Suppose that $\Delta_\Gamma(y{:}z|Yz_1z_2) = 1$. Then $YzB_{11}B_{21} \in \Gamma$, and hence $YB_{11}B_{21} \in \Gamma$. Since $Yz_1z_2 \notin \Gamma$, the sets $YB_{10}B_{20}$, $YB_{10}B_{21}$ and $YB_{11}B_{20}$ are unqualified. Then $\varepsilon_0^i = 1$ for $i = 1, 2$. In addition, $YyB_{11}B_{20} \in \Gamma$ because $Yyz_1z_2 \in \Gamma$, which implies that $Yyz_1y_2 \in \Gamma$. On the other hand, the sets $YyB_{10}y_2$, Yyy_1B_{20} and Yyy_1z_2 are unqualified, and hence $\varepsilon_2^i = 1$ for $i = 1, 2$. Clearly, Yzy_1B_{20} and Yzz_1y_2 are unqualified sets and, since $Yzz_1z_2 \in \Gamma$, we get that $\varepsilon_2^1 = 1$. Moreover, at least one of the sets $YzB_{10}B_{20}$, $YzB_{10}B_{21}$ is qualified. If $YzB_{10}B_{20}$, then $Yyzy_1B_{20} \in \Gamma$ and $\varepsilon_3^1 = 0$. If $YzB_{10}B_{20} \notin \Gamma$, and $YzB_{10}B_{21} \in \Gamma$, then $\varepsilon_3^1 = 0$ because both sets $Yyzz_1y_2$ and $Yyzy_1z_2$ are qualified. In any case, $\varepsilon^1 = 1$. □

10 Conclusion

Even though other methods have been used for linear secret sharing schemes [1, 4, 21], the only known general technique to find lower bounds on the length of the shares in secret sharing is the one formalized by Csirmaz [12]. By this method, the lower bounds are derived from linear programs that involve information inequalities.

In the same line as the works by Csirmaz [12] and Beimel and Orlov [6], we present some limitations on the power of that method. First, the lower bounds that are obtained by using all rank inequalities (and hence all information inequalities) on a bounded number of variables are polynomial on the number of participants (Theorem 6.2). And second, the rank inequalities that are implied by the existence of *two* common informations can provide only lower bounds that are at most cubic on the number of participants (Theorem 8.6). Both results are proved by similar techniques. Namely, by finding feasible solutions to the corresponding linear programs. Specifically, we present families of polymatroids such that the values of their rank functions are polynomial on the number of participants and satisfy all constraints given by the corresponding rank inequalities.

Theorem 8.6 refers to the *common informations*, which provide the only known method to find rank inequalities. Extending this result from two to a larger number of common informations does not seem easy, at least by using the ideas and techniques in this work. Finally, we think that the extension of this result to the known methods of finding information inequalities is worth considering. These methods have been recently analyzed by Kaced [26].

Acknowledgements

We especially thank Laszlo Csirmaz for providing an approach to the proof of Theorem 6.2 that is much more intuitive and elegant than the one in previous versions of this work. We thank Amos Beimel and Ilan Orlov for useful discussions about the contents of this paper. We are grateful to the anonymous referees for their careful revision of our work and their valuable ideas and suggestions that greatly improved its presentation.

The first and second authors' work was supported by the Spanish Government through the projects MTM2009-07694 and MTM2013-41426-R. The second and third authors' work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

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., Ben-Efraim, A., Padró, C., Tyomkin, I.: Multi-linear Secret-Sharing Schemes. In: Theory of Cryptography, TCC 2014. LNCS, vol. 8349, 394–418 (2014)

[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. In: Goldwasser, S (ed.) Advances in Cryptology—CRYPTO'88. LNCS, vol. 403, pp. 27–35. Springer, Heidelberg (1990)

[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] 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)

[11] Chan, T.: Recent Progresses in Characterizing Information Inequalities. Entropy 13, 379–401 (2011)

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

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

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

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

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

[17] 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)

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

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

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

[21] Gál, A.: A characterization of span program size and improved lower bounds for monotone span programs. Comput. Complexity 10, 277–296 (2001)

[22] 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)

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

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

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

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

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

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

[29] Matúš, F., Csirmaz, L.: Entropy region and convolution. Available at arXiv.org, arXiv:1310.5957 (2013)

[30] 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)

[31] 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)

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

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

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

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

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

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