Secret Sharing, Rank Inequalities and Information Inequalities*

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

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

October 29, 2014

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 [31] and Blakley [6], 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 [22], 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*.

Nevertheless, not many results supporting this conjecture have been proved. 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 [10], who presented a family of access structures on an arbitrary number n of participants that require shares of size $\Omega(n/\log n)$ times the size of the secret.

In contrast, superpolynomial lower bounds on the size of the shares have been obtained for linear secret sharing schemes [1, 3, 19]. 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 [10] and by Beimel and Orlov [5], 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 [7, 8, 10, 23] and many other papers. Even though it was implicitly used before, the method was formalized by Csirmaz [10]. 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, and hence 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, from the fact that the joint entropies of a collection of random variables define a polymatroid [16, 17].

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 [10] 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 small solution. Notice that he 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 [34], and many others have been found subsequently [12, 14, 26, 33]. 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 [4, 28, 29].

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 [21]. Other rank inequalities have been presented afterwards [13, 25]. 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 [4, 11, 29].

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 [13, 24], and it seems that many of them remain unknown. And second, except for a few cases, no spanning sets are known for the rank inequalities on a given number of variables. Besides, even for four variables, there are infinitely many independent information inequalities [26].

Moreover, the aforementioned negative result by Csirmaz [10] was generalized by Beimel and Orlov [5], 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 small solution that is related to the solution used by Csirmaz [10] 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 [13, 20]. 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 [33]. This sequence contains inequalities on arbitrarily many variables and generalizes the infinite sequences from previous works.

In particular, the results in [5] 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 5.2 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 superpolynomial lower bounds by using the method described above. The proof is extremely simple and concise. Similarly to the proofs in [5, 10], it is based on finding small 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 [5, 10]. In some sense, our result is weaker than the one in [5], because for $r = 4$ and $r = 5$, our solutions to the linear programs 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 [9, 13, 24, 27]. In particular, non-Shannon rank inequalities have been found by using *common informations* [13, 20]. Specifically, all known sharp rank inequalities are derived from the existence of *two* common informations [13]. We prove in Theorem 7.5 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 5.2.

2 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 [30, 32]. 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 $X \smallsetminus \{x\}$. For a function $f : \mathcal{P}(Q) \to \mathbb{R}$ and subsets $X, Y, Z \subseteq Q$, 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 $\{1, \dots, r\}$.

Definition 2.1. A *polymatroid* is a pair $\mathcal{S} = (Q, f)$ formed by a finite set Q, the *ground set*, and a *rank function* $f\colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

- $f(\emptyset) = 0$.
- f is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $f(X) \le f(Y)$.
- 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 $\mathcal{S}$.

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

Remark 2.2. A map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if $f(\emptyset) = 0$ and $\Delta_f(Y{:}Z|X) \ge 0$ for every $X, Y, Z \subseteq Q$.

The following characterization of rank functions of polymatroids is a straightforward consequence of [30, Theorem 44.1].

Proposition 2.3. *A map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if $f(\emptyset) = 0$ and $\Delta_f(y{:}z|X) \ge 0$ for every $X \subseteq Q$ and $y, z \in Q \smallsetminus X$.*

In the following, four important classes of polymatroids are discussed. Namely, the entropic, the linear, the Boolean, and the uniform polymatroids. The notation S_X, where X is a set, will be used for random variables, vector subspaces and subsets with different meanings. Nevertheless, the context in which this notation is used should avoid any confusion.

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 $(S_i)_{i \in [3]}$, 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 result by Fujishige [16, 17].

Theorem 2.4. *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.*

Proof. Observe that $\Delta_h(Y{:}Z|X) = I(S_Y{:}S_Z|S_X) \geq 0$ for every $X, Y, Z \subseteq Q$ and apply Remark 2.2. □

Because of the connection between Shannon entropy and polymatroids given by Theorem 2.4, and by analogy to the conditional entropy, we write $f(X|Y) = f(XY) - f(Y)$ if (Q, f) is a polymatroid and $X, Y \subseteq Q$.

A polymatroid $\mathcal{S} = (Q, h)$ is called *entropic* if there exists a random vector $(S_x)_{x \in Q}$ such that $h(X) = H(S_X)$ for every $X \subseteq Q$. Let V be a vector space over a field $\mathbb{K}$ and $(V_x)_{x \in Q}$ a tuple of vector subspaces of V. For $X \subseteq Q$, we notate $V_X = \sum_{x \in X} V_x$. Then the map $f\colon \mathcal{P}(Q) \to \mathbb{Z}$ defined by $f(X) = \dim V_X$ for every $X \subseteq Q$ is the rank function of an integer polymatroid $\mathcal{S}$ with ground set Q. Integer polymatroids that can be defined in this way are 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 [20]. 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 $(S_x)_{x \in Q}$ is called $\mathbb{K}$-*linear* if $S_x = S|_{V_x}$ for some collection $(V_x)_{x \in Q}$ 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.

Proposition 2.5. *For a finite field $\mathbb{K}$, every $\mathbb{K}$-linearly entropic polymatroid is a multiple of a $\mathbb{K}$-linear polymatroid.*

Consider a finite set M and a family $(M_x)_{x \in Q}$ of subsets of M. For every $X \subseteq Q$, take $M_X = \bigcup_{x \in X} M_x$. Then the map defined by $f(X) = |M_X|$ for every $X \subseteq Q$ is the rank function of an integer polymatroid $\mathcal{S}$ with ground set Q. The family $(M_x)_{x \in Q}$ is called a *Boolean representation* of $\mathcal{S}$. *Boolean polymatroids* are those admitting a Boolean representation. Boolean polymatroids are $\mathbb{K}$-linear 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 $\mathbf{e}^w(w') = 1$ if $w' = w$ and $\mathbf{e}^w(w') = 0$ otherwise. Obviously, $(\mathbf{e}^w)_{w \in M}$ is a basis of $\mathbb{K}^M$. For every $x \in Q$, 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 $\mathcal{S}$.

We say that a polymatroid $\mathcal{S}$ with ground set Q is *uniform* if every permutation on Q is an automorphism of $\mathcal{S}$. In this situation, the rank $f(X)$ of a set $X \subseteq Q$ depends only on its cardinality, that is, there exist values $0 = f_0 \leq f_1 \leq \cdots \leq f_n$, where $n = |Q|$, such that

$f(X) = f_i$ for every $X \subseteq Q$ with $|X| = i$. By Proposition 2.3, 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 $i = 1, \dots, n-1$. Clearly, a uniform polymatroid is univocally determined by its *increment vector* $\delta = (\delta_1, \dots, \delta_n)$, 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 [15].

Given a positive integer r, a collection $(A_i)_{i\in[r]}$ of subsets of a set Q, 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 (Q, f) and for every collection $(A_i)_{i\in[r]}$ of r subsets of Q.

By Proposition 2.5, 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 2.4. The Ingleton inequality [21] 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 [34]. Subsequently, many other rank and information inequalities have been found in [12, 13, 14, 25, 26, 33] and other works. We need the following technical result, which is a consequence of [5, Lemma 4.3].

Lemma 2.6. *Let $(\alpha_I)_{I\in\mathcal{P}([r])}$ be a rank inequality. Then $\sum_{I\,:\,I\cap J\neq\emptyset} \alpha_I \geq 0$ for every $J \subseteq [r]$.*

Proof. Take $J \subseteq [r]$, a set M with $|M| = 1$, and the family $(M_i)_{i\in[r]}$ of subsets of M given by $M_i = M$ if $i \in J$ and $M_i = \emptyset$ otherwise. Let $([r], f)$ be the Boolean polymatroid defined by this family. Then $\sum_{I\,:\,I\cap J\neq\emptyset} \alpha_I = \sum_{I\subseteq[r]} \alpha_I f(I) \geq 0$ because Boolean polymatroids are linearly representable. □

3 Polymatroids and Secret Sharing

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

For an access structure Γ on P, a Γ-*polymatroid* is a polymatroid $\mathcal{S} = (Q, f)$ such that

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

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

A *secret sharing scheme* Σ on P with access structure Γ is a random vector $(S_x)_{x\in Q}$ such that the entropic polymatroid $\mathcal{S} = (Q, h)$ determined by Σ is a Γ-polymatroid. 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. If $X \notin \Gamma$, then $I(S_{p_o}{:}S_X) = 0$, that is, the random variables S_{p_o} and S_X are independent. On the other hand, $H(S_{p_o}|S_X) = 0$ if $X \in \Gamma$, that is, S_{p_o} is a function of S_X. A secret sharing scheme is $\mathbb{K}$-*linear* if it is a $\mathbb{K}$-linear random vector.

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

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

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

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

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 uniformly distributed secret value, the same access structure, and shares of the same length [2]. Therefore, lower bounds on the information ratio $\sigma(\Sigma)$ provide lower bounds on the length of the shares.

For a polymatroid $\mathcal{S} = (Q, f)$, we define

$$\sigma_{p_o}(\mathcal{S}) = \frac{\max_{x \in P} f(\{x\})}{f(\{p_o\})}.$$

Observe that $\sigma(\Sigma) = \sigma_{p_o}(\mathcal{S})$ if $\mathcal{S}$ is the entropic polymatroid defined by Σ. 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. Clearly,

$$\sigma(\Gamma) = \inf\{\sigma_{p_o}(\mathcal{S}) \,:\, \mathcal{S} \text{ is an entropic } \Gamma\text{-polymatroid}\}.$$

Therefore, the parameters

$$\kappa(\Gamma) = \inf\{\sigma_{p_o}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}$$

and

$$\lambda(\Gamma) = \inf\{\sigma_{p_o}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a linear } \Gamma\text{-polymatroid}\}$$

are, respectively, a lower and an upper bound for $\sigma(\Gamma)$. Observe that $\lambda(\Gamma)$ is the infimum of the information ratios of the linear secret sharing schemes for Γ. The value $\kappa(\Gamma)$ is the solution of a linear programming problem, and hence the infimum is a minimum and $\kappa(\Gamma)$ is a rational number [29]. Most of the known lower bounds on the information ratio, as the ones from [7, 8, 10, 23], 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.

Information inequalities and rank inequalities can be added to the linear program computing $\kappa(\Gamma)$ to find better lower bounds on $\sigma(\Gamma)$ and $\lambda(\Gamma)$, respectively. This has been done for several families of access structures [4, 11, 28, 29].

A polymatroid $\widehat{\mathcal{S}} = (\widehat{Q}, g)$ is called an *extension* of a polymatroid $\mathcal{S} = (Q, f)$ if $Q \subseteq \widehat{Q}$ and $g(X) = f(X)$ for every $X \subseteq Q$. In general, we will use the same symbol for the rank function of a polymatroid and the rank function of an extension of it. 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 $\mathcal{S}(\Gamma) = (Q, f)$. The following characterization of compatibility between access structures and polymatroids is a variant of a result by Csirmaz [10, Proposition 2.3].

Proposition 3.1. *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 2.3, (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 3.2. 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 $X \notin \Gamma$.

4 A Family of Uniform Boolean Polymatroids

We present a family of polymatroids that are uniform and Boolean. In addition, every member of this family is compatible to all access structures on its ground set. The following results are straightforward consequences of Proposition 3.1.

Proposition 4.1. *A polymatroid $\mathcal{S} = (P, f)$ 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 $y, z \in P \smallsetminus X$.*

Proposition 4.2. *Let P be a set with $|P| = n$ and let $\mathcal{S}$ be a uniform polymatroid on P. Then $\mathcal{S}$ 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 $\delta_n \geq 1$.*

Given a set P and an integer $r \geq 2$, let $M(P, r)$ be the set of all multisets of size r of the set P. For example, if $P = \{a, b, c\}$, then

$$M(P, 3) = \{aaa, aab, aac, abb, abc, acc, bbb, bbc, bcc, ccc\}.$$

Observe that $|M(P, r)| = \binom{n+r-1}{r}$ if $|P| = n$. For every $x \in P$, let $M_x(P, r)$ be the set of the multisets in $M(P, r)$ that contain x. In the previous example,

$$M_a(P, 3) = \{aaa, aab, aac, abb, abc, acc\}.$$

Finally, we define $\mathcal{Z}(P, r) = (P, f)$ as the Boolean polymatroid on P defined by the family $(M_x(P, r))_{x \in P}$ of subsets of $M(P, r)$. As usual, we notate $M_X(P, r) = \bigcup_{x \in X} M_x(P, r)$ for every $X \subseteq Q$.

Clearly, every permutation on P is an automorphism of $\mathcal{Z}(P, r)$, and hence this polymatroid is uniform. For every $X \subseteq P$, the multisets in $M(P, r) \smallsetminus M_X(P, r)$ are the ones involving only elements in $P \smallsetminus X$. That is, $M(P, r) \smallsetminus M_X(P, r) = M(P \smallsetminus X, r)$, and hence

$$\begin{aligned} f(X) &= |M_X(P, r)| = |M(P, r)| - |M(P \smallsetminus X, r)| \\ &= \binom{|P| + r - 1}{r} - \binom{|P| - |X| + r - 1}{r}. \end{aligned}$$

Therefore, if $|P| = n$, the increment vector $(\delta_1, \dots, \delta_n)$ of $\mathcal{Z}(P, r)$ is given by

$$\delta_i = \binom{n-i+r}{r} - \binom{n-i+r-1}{r} = \binom{n-i+r-1}{r-1}$$

for every $i = 1, \dots, n$. Observe that $\delta_1 > \cdots > \delta_n > 0$, and hence $\mathcal{Z}(P, r)$ is compatible with all access structures on P. In particular, $\delta_i = n - i + 1$ if $r = 2$, and hence $\kappa(\Gamma) \leq n$ for every access structure Γ on n participants [10]. The *Csirmaz function* introduced in [5, 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 [5, Lemma 3.11]. Finally, observe that [5, Lemma 6.2] is a straightforward consequence of the fact that $\mathcal{Z}(P, 2)$ is a Boolean polymatroid.

5 On Rank Inequalities on a Bounded Number of Variables

This section is devoted to prove our first main result, Theorem 5.2.

Proposition 5.1. *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 Γ-polymatroid $\mathcal{Z}_{r-1}(\Gamma)$, an extension of $\mathcal{Z}_{r-1}$ to $Q = P \cup \{p_o\}$. Then $\mathcal{Z}_{r-1}(\Gamma)$ satisfies all rank inequalities on r variables.*

Proof. Let f be the rank function of $\mathcal{Z}_{r-1}(\Gamma)$ and $(\alpha_I)_{I \in \mathcal{P}([r])}$ a rank inequality on r variables. We have to prove that $\sum_{I \subseteq [r]} \alpha_I f(A_I) \geq 0$ for every r subsets $(A_i)_{i \in [r]}$ of Q. Take $B_i = A_i \smallsetminus \{p_o\}$. If $B_i \in \Gamma$ for every $i \in [r]$, then $\sum_{I \subseteq [r]} \alpha_I f(A_I) = \sum_{I \subseteq [r]} \alpha_I f(B_I) \geq 0$ because $\mathcal{Z}_{r-1}$ is Boolean. If $B_{[r]} \notin \Gamma$, then

$$\sum_{I \subseteq [r]} \alpha_I f(A_I) = \sum_{I \subseteq [r]} \alpha_I f(B_I) + \sum_{I \,:\, p_o \in A_I} \alpha_I \geq 0$$

by Lemma 2.6 with $J = \{i \in [r] \,:\, p_o \in A_i\}$. From now on, we assume that $B_{[r]} \in \Gamma$ and that $B_i \notin \Gamma$ for some $i \in [r]$.

Consider the polymatroid $\mathcal{S} = ([r], g)$ determined by $g(I) = f(B_I)$ for every $I \subseteq [r]$. In addition, consider the access structure Λ on $[r]$ formed by the sets $I \subseteq [r]$ such that $B_I \in \Gamma$. We prove next that $\mathcal{S}$ can be extended to a linearly representable Λ-polymatroid $\mathcal{S}(\Lambda) = ([r] \cup \{0\}, g)$. This concludes the proof. Indeed, since $\mathcal{S}(\Lambda)$ is a Λ-polymatroid, $f(A_I) = g(I \cup \{0\})$ if $p_o \in A_I$, and hence

$$\begin{aligned} \sum_{I \subseteq [r]} \alpha_I f(A_I) &= \sum_{I \,:\, p_o \notin A_I} \alpha_I f(B_I) + \sum_{I \,:\, p_o \in A_I} \alpha_I f(A_I) \\ &= \sum_{I \,:\, p_o \notin A_I} \alpha_I g(I) + \sum_{I \,:\, p_o \in A_I} \alpha_I g(I \cup \{0\}). \end{aligned}$$

Consider the family $(C_i)_{i \in [r]}$ of subsets of $[r] \cup \{0\}$ given by $C_i = \{i, 0\}$ if $p_o \in A_i$ and $C_i = \{i\}$ otherwise. Then

$$\sum_{I \,:\, p_o \notin A_I} \alpha_I g(I) + \sum_{I \,:\, p_o \in A_I} \alpha_I g(I \cup \{0\}) = \sum_{I \subseteq [r]} \alpha_I g(C_I) \geq 0$$

because $\mathcal{S}(\Lambda)$ is linearly representable.

The polymatroid $\mathcal{S}$ is Boolean. Indeed, take $M = M(P, r-1)$ and $M_X = M_X(P, r-1)$ for every $X \subseteq P$. Then $(M_{B_i})_{i \in [r]}$ is a Boolean representation of $\mathcal{S}$. Therefore, this polymatroid is linearly representable over every field, as proved in Section 2. For a field $\mathbb{K}$, take a basis

$(\mathbf{e}^w)_{w\in M}$ of $\mathbb{K}^M$. Then the subspaces $(V_i)_{i\in[r]}$ with $V_i = \langle \mathbf{e}^w : w \in M_{B_i}\rangle$ form a $\mathbb{K}$-linear representation of $\mathcal{S}$.

Consider the dual access structure $\Lambda^* = \{J \subseteq [r] : [r] \smallsetminus J \notin \Lambda\}$. Take $J \in \min \Lambda^*$ and $I = [r] \smallsetminus J$. Observe that $B_I \notin \Gamma$ and $B_I \cup B_j \in \Gamma$ for every $j \in J$. In particular, this implies that $J \neq \emptyset, [r]$. Therefore, we can take an element $x_j \in B_j \smallsetminus B_I$ for every $j \in J$. Consider a multiset $w_J \in M(P, r-1)$ containing exactly the elements in $\{x_j : j \in J\}$, repeating some of them if necessary. Take the vector

$$\mathbf{v}_0 = \sum_{J\in\min\Lambda^*} \mathbf{e}^{w_J} \in \mathbb{K}^M$$

and the subspace $V_0 = \langle \mathbf{v}_0 \rangle$. By adding this subspace to the collection $(V_i)_{i\in[r]}$, an extension $\mathcal{S}(\Lambda) = ([r] \cup \{0\}, g)$ of $\mathcal{S}$ is obtained. Obviously, $\mathcal{S}(\Lambda)$ is $\mathbb{K}$-linearly representable.

Finally, we prove that $\mathcal{S}(\Lambda)$ is a Λ-polymatroid. Clearly, $I \in \Lambda$ if and only if $I \cap J \neq \emptyset$ for every $J \in \min \Lambda^*$. If $I \in \Lambda$, then $w_J \in M_{B_I}(P, r-1)$ for every $J \in \min \Lambda^*$. Indeed, if $j \in I \cap J$, the element x_j in the multiset w_J is also in B_I. Therefore, $\mathbf{e}^{w_J} \in V_I$ for every $J \in \min \Lambda^*$, and hence $\mathbf{v}_0 \in V_I$ and $g(I \cup \{0\}) = g(I)$. Suppose now that $I \notin \Lambda$ and take $J \in \min \Lambda^*$ with $I \cap J = \emptyset$. Then $w_J \notin M_{B_I}(P, r-1)$ because $x_j \notin B_I$ for every $j \in J$. Therefore, $\mathbf{v}_0 \notin V_I$ and $g(I \cup \{0\}) = g(I) + 1$. □

Theorem 5.2. *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*

$$\binom{n+r-3}{r-2} \tag{1}$$

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 5.1, the polymatroid $\mathcal{Z}_{r-1}(\Gamma)$ is 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 $\sigma_{p_o}(\mathcal{Z}_{r-1}(\Gamma)) = \delta_1$, where δ_1 is the first component of the increment vector of $\mathcal{Z}(P, r-1)$. □

A smaller value for the bound (1) can be proved for the case $r \leq n$ by using in the same way the uniform Boolean polymatroid defined by the set M of all subsets (instead of multisets) of P with at most $r-1$ participants and the subsets $(M_x)_{x\in P}$, where M_x consists of the subsets in M that contain x. Nevertheless, the asymptotic result is not improved.

6 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 [18]. 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 6.1. Consider a polymatroid $\mathcal{S} = (Q, f)$ and two sets $A, B \subseteq Q$. Then every subset $X_0 \subseteq Q$ 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 6.2. *Let $\mathcal{S} = (Q, f)$ be a polymatroid, $A, B \subseteq Q$, and $X_0 \subseteq Q$ a common information for (A, B). Consider a subset $Y \subseteq Q$ such that $f(Y|A) = f(Y|B) = 0$. Then $f(Y|X_0) = 0$.*

Proof. Observe that

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

The second equality holds because $f(Y|A) = f(Y|B) = 0$. Finally, $f(YX_0) \leq f(X_0)$ because $f(YX_0|A) = f(YX_0|B) = 0$, and hence $f(Y|X_0) = 0$. □

Let $(V_x)_{x \in Q}$ be a collection of vector subspaces representing a $\mathbb{K}$-linear polymatroid $\mathcal{S} = (Q, f)$, and consider two subsets $A, B \subseteq Q$. By taking $V_{x_0} = V_A \cap V_B$, an extension of $\mathcal{S}$ to Qx_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 $\mathcal{S} = (Q, f)$ is a Boolean polymatroid defined by a family $(M_x)_{x \in Q}$ of sets, then the extension of $\mathcal{S}$ to Qx_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 6.3. Let k be a positive integer. A polymatroid $\mathcal{S} = (Q, f)$ satisfies the *k-common information property* if, for every k pairs $(A_{i0}, A_{i1})_{i \in [k]}$ of subsets of Q, there exists an extension $\widehat{\mathcal{S}} = (\widehat{Q}, f)$ of $\mathcal{S}$ such that, for every $i \in [k]$, there exists a common information $Y_i \subseteq \widehat{Q}$ 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 [20]. If a polymatroid satisfies the 1-common information property, then it satisfies the Ingleton inequality [13], 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 [13]. All these inequalities are satisfied by every polymatroid with the 2-common information property [13], and hence such polymatroids satisfy all information inequalities on 5 variables. Moreover, according to [13], all known sharp rank inequalities are derived from the 2-common information property.

7 On Rank Inequalities Derived from Common Informations

Let P be a set of n participants, Γ an access structure on P, and $\mathcal{Z} = \mathcal{Z}(P, 4)$. Consider the Γ-polymatroid $\mathcal{Z}(\Gamma)$ that is an extension of $\mathcal{Z}$ to $Q = Pp_o$. 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 $\mathcal{Z} = \mathcal{Z}(P, 4) = (P, f)$. 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 7.1. *Let $(M_x)_{x\in P}$ be a Boolean representation of a polymatroid (P,f) and X,Y,Z subsets of P. 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, $\Delta_f(Y{:}Z|X)=|M_{XY}\cap M_Z|-|M_X\cap M_Z|$. □

Lemma 7.2. *The polymatroid $\mathcal{S}$ and the access structure Γ on $Py_1\dots y_k$ are compatible.*

Proof. By combining Proposition 3.1, Remark 3.2, and Lemma 7.1, 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 $0\le s\le k$, 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 $yyzz\in(M_y\cap M_z)\smallsetminus M_X$. 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 $u_0u_1zz\in(M_y\cap M_z)\smallsetminus M_X$. If $y,z\notin P$, we can assume that $y=y_k$ and $z=y_\ell$ for some $\ell>s$. Then $u_0u_1v_0v_1\in(M_y\cap M_z)\smallsetminus M_X$ 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 7.3. *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 7.3 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 7.4. *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_0p_o,B_1), (B_0,B_1p_o), and (B_0p_o,B_1p_o).*
2. *If $B_0\in\Gamma$ and $B_1\notin\Gamma$, then y is a common information for (B_0p_o,B_1) and yp_o is a common information for both (B_0,B_1p_o) and (B_0p_o,B_1p_o).*
3. *If $B_0\cup B_1\notin\Gamma$, then y is a common information for both (B_0p_o,B_1) and (B_0,B_1p_o), while yp_o is a common information for (B_0p_o,B_1p_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 6.2. If $B_1\notin\Gamma$, then $g(yp_o)-g(y)=g(p_o|y)\ge g(p_o|B_1)=1$ and $g(yp_o)=g(y)+1$. Observe that $g(yp_o|A_i)=0$ 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 7.4, namely $B_0,B_1\notin\Gamma$ and $B_0\cup B_1\in\Gamma$. In this case, neither y nor yp_o provides common informations for the pairs (B_0p_o,B_1) and (B_0p_o,B_1p_o). A method to find those common informations is given in the proof of Proposition 7.5. 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 7.5. *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 7.5 and the value of $\sigma_{p_o}(\mathcal{Z}'(\Gamma))$.

Theorem 7.6. *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*

$$3 \cdot \binom{n+2}{3}$$

and hence $O(n^3)$.

The remaining of this section is devoted to the proof of Proposition 7.5, which 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 this section. 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 7.4, we can suppose that $p_o \in A_{10}$ and $B_{10}, B_{11} \notin \Gamma$ while $B_{10} \cup B_{11} \in \Gamma$. 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 7.7. *$(Py_1y_2z_1, g)$ is a polymatroid, and it is compatible with the access structure Γ.*

The proof of Lemma 7.7 will be presented later. Assuming this result, it is not difficult to check 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, $g(\{z_1\}) = g(\{y_1\}) + 1 = \Delta_g(B_{10}{:}B_{11}) + 1 = \Delta_g(A_{10}{:}B_{11})$ and our affirmation is proved. In addition, it is clear that z_1p_o is a common information for (A_{10}, A_{11}) if $p_o \in A_{11}$.

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 $i = 1, 2$. As before, 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. For each set $X \subseteq Py_1y_2$, let $N(X)$ be the number of pairs $(j,k) \in \{0,1\}^2$ such that $XB_{1j}B_{2k} \in \Gamma$. The following requirements define extensions of $\mathcal{Z}'$ and Γ to $Py_1y_2z_1z_2$.

- If $N(X) = 0, 1$, then $g(Xz_1z_2) = g(Xy_1y_2) + 2$ and $Xz_1z_2 \notin \Gamma$.
- If $N(X) = 2$ and $XB_{11}B_{21} \notin \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2) + 1$ and $Xz_1z_2 \notin \Gamma$.
- If $N(X) = 2$ and $XB_{11}B_{21} \in \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2) + 2$ and $Xz_1z_2 \in \Gamma$.
- If $N(X) = 3$ and $XB_{11}B_{21} \notin \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2)$ and $Xz_1z_2 \notin \Gamma$.
- If $N(X) = 3$ and $XB_{11}B_{21} \in \Gamma$, then $g(Xz_1z_2) = g(Xy_1y_2) + 1$ and $Xz_1z_2 \in \Gamma$.

- If $N(X) = 4$, then $g(Xz_1z_2) = g(Xy_1y_2)$ and $Xz_1z_2 \in \Gamma$.

Lemma 7.8. *$(Py_1y_2z_1z_2, g)$ is a polymatroid, and it is compatible with the access structure Γ.*

Assuming that Lemma 7.8 is true, we have that, for $i = 1, 2$, either z_i or z_ip_o is a common information for (A_{i0}, A_{i1}) in the polymatroid $(Qy_1y_2z_1z_2, g)$. Therefore, the proof of Proposition 7.5 is concluded with the proofs of Lemmas 7.7 and 7.8. By combining Propositions 2.3 and 3.1, it is enough to prove the following result.

Lemma 7.9. *$\Delta_g(y{:}z|X) \geq \max\{0, \Delta_\Gamma(y{:}z|X)\}$ for every $X \subseteq Py_1y_2z_1z_2$ and $y, z \in Py_1y_2z_1z_2 \smallsetminus X$.*

Proof. Since $\mathcal{T} = (Py_1y_2, g)$ is a polymatroid that is compatible with Γ, the result holds if $Xyz \subseteq Py_1y_2$. For a subset $X \subseteq Py_1y_2z_1z_2$, we notate $\widehat{X}$ for the subset of Py_1y_2 that is obtained by substituting z_i by y_i for $i = 1, 2$. For $X \subseteq Py_1y_2z_1z_2$ and $y, z \in Py_1y_2z_1z_2 \smallsetminus X$, consider

- $\delta = \max\{0, \Delta_\Gamma(y{:}z|X)\}$ and
- $\varepsilon = \Delta_g(y{:}z|X) - \Delta_g(\widehat{y}{:}\widehat{z}|\widehat{X})$.

Then $\Delta_g(y{:}z|X) = \Delta_g(\widehat{y}{:}\widehat{z}|\widehat{X}) + \varepsilon = 3\Delta_f(\widehat{y}{:}\widehat{z}|\widehat{X}) + \varepsilon$. Since $\Delta_f(\widehat{y}{:}\widehat{z}|\widehat{X}) \geq 0$ and $\delta \leq 1$, the lemma is proved by checking that $\varepsilon \geq -2$ and that $\varepsilon \geq \delta$ if $\Delta_f(\widehat{y}{:}\widehat{z}|\widehat{X}) = 0$. Recall that, by Lemma 7.1, $\Delta_f(\widehat{y}{:}\widehat{z}|\widehat{X}) = 0$ if and only if $M_{\widehat{y}} \cap M_{\widehat{z}} \subseteq M_{\widehat{X}}$. We distinguish several cases. The first three involve z_1 but not z_2, while the remaining ones involve both z_1 and z_2.

Case 1. *$X \subseteq Py_1y_2$ and $y = z = z_1$.* Then $\varepsilon = g(Xz_1) - g(Xy_1) \geq 0$. If $\delta = 1$ and $\varepsilon = 0$, then $X \notin \Gamma$ and $Xy_1 \in \Gamma$, and hence $\Delta_f(y_1{:}y_1|X) \geq \Delta_\Gamma(y_1{:}y_1|X) \geq 1$.

Case 2. *$Xy \subseteq Py_1y_2$ and $z = z_1$.* Then $\varepsilon = g(Xz_1) - g(Xy_1) - (g(Xyz_1) - g(Xyy_1)) \geq 0$ and $\varepsilon = 0$ if and only if $XyB_{10} \notin \Gamma$ or $XB_{10} \in \Gamma$. If $\delta = 1$ and $\varepsilon = 0$, then $X \notin \Gamma$ while $Xy \in \Gamma$ and $Xy_1 \in \Gamma$, which implies that $\Delta_f(y{:}y_1|X) \geq \Delta_\Gamma(y{:}y_1|X) \geq 1$.

Case 3. *$X = Yz_1$ with $Yyz \subseteq Py_1y_2$.* Take $\varepsilon_0 = g(Yz_1) - g(Yy_1)$, $\varepsilon_1 = g(Yyz_1) - g(Yyy_1)$, $\varepsilon_2 = g(Yzz_1) - g(Yzy_1)$, and $\varepsilon_3 = g(Yyzz_1) - g(Yyzy_1)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_0$, and hence $\varepsilon \geq -1$ because $0 \leq \varepsilon_3 \leq \varepsilon_1, \varepsilon_2 \leq \varepsilon_0 \leq 1$. Suppose that $M_y \cap M_z \subseteq M_{Yy_1}$. Then we can assume that $y \in B_{10}$ and $\{y, z\} \cap B_{11} \neq \emptyset$, which implies that $\varepsilon_1 = \varepsilon_0$ and $\delta = 0$.

Case 4. *$X \subseteq Py_1y_2$, and $y = z_1$ and $z = z_2$.* For $i = 1, 2$, take $\varepsilon_i = g(Xz_i) - g(Xy_i)$, and also $\varepsilon_3 = g(Xz_1z_2) - g(Xy_1y_2)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3$. If $\varepsilon_3 = 2$, then $\varepsilon_1 = \varepsilon_2 = 1$. In addition, $\varepsilon_3 = 0$ if $\varepsilon_1 = \varepsilon_2 = 0$. Therefore, $\varepsilon \geq 0$. Suppose now that $\delta = 1$ and $\varepsilon = 0$. In this case $\varepsilon_3 \leq 1$ because $XB_{11}, XB_{21} \in \Gamma$. If $\varepsilon_3 = 1$, then $XB_{10}B_{20} \notin \Gamma$, and hence $\varepsilon_1 = \varepsilon_2 = 1$, a contradiction. If $\varepsilon_1 = \varepsilon_2 = 0$, then $XB_{10}, XB_{20} \in \Gamma$, and hence $Xy_1, Xy_2 \in \Gamma$. Since $X \notin \Gamma$, this implies that $\Delta_f(y_1{:}y_2|X) \geq 1$.

Case 5. *$X = Yz_1$ with $Y \subseteq Py_1y_2$, and $y = z = z_2$.* In this case, $\varepsilon = \varepsilon_1 - \varepsilon_0$, where $\varepsilon_0 = g(Yz_1) - g(Yy_1)$ and $\varepsilon_1 = g(Yz_1z_2) - g(Yy_1y_2)$, and hence $\varepsilon \geq -1$. Suppose that $\Delta_f(y_2{:}y_2|Yy_1) = 0$, which is equivalent to $M_{y_2} \subseteq M_{Yy_1}$. In particular, $M_{y_2} \subseteq M_{YB_{1j}}$ for $j = 1, 2$. If $\varepsilon_0 = 1$, then $YB_{10} \notin \Gamma$, and hence $YB_{10}\,y_2 \notin \Gamma$, which implies that $\varepsilon_1 \geq 1$. Therefore, $\varepsilon \geq 0$. Assume that $\delta = 1$ and $\varepsilon = 0$. Then $Yz_1z_2 \in \Gamma$ while $Yz_1 \notin \Gamma$. In particular, $YB_{11} \notin \Gamma$, and hence $YB_{11}\,y_2 \notin \Gamma$. This implies that $N(Y) = 3$, $\varepsilon_1 = 1$, and $YB_{11}B_{21} \in \Gamma$, and hence $YB_{11}B_{20} \notin \Gamma$. Then $\varepsilon_0 = 1$ and $YB_{10} \notin \Gamma$, and hence $YB_{10}\,y_2 \notin \Gamma$, a contradiction.

Case 6. *$X = Yz_1$ with $Yy \subseteq Py_1y_2$, and $z = z_2$.* Take $\varepsilon_0 = g(Yz_1) - g(Yy_1)$, $\varepsilon_1 = g(Yyz_1) - g(Yyy_1)$, $\varepsilon_2 = g(Yz_1z_2) - g(Yy_1y_2)$ and $\varepsilon_3 = g(Yyz_1z_2) - g(Yyy_1y_2)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_0$. Then $0 \leq \varepsilon_1 \leq \varepsilon_0 \leq 1$ and $0 \leq \varepsilon_3 \leq \varepsilon_2 \leq 2$, and hence $\varepsilon \geq -1$. Suppose that $\varepsilon = -1$, that is, $\varepsilon_0 = 1$, $\varepsilon_1 = 0$, and $\varepsilon_2 = \varepsilon_3$. In particular, $YB_{10} \notin \Gamma$ and $YB_{10}\,y \in \Gamma$, and hence $\varepsilon_3 \leq 1$. If $\varepsilon_2 = \varepsilon_3 = 1$, then $YyB_{11}B_{20} \notin \Gamma$, and hence $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$. Since $YB_{10} \notin \Gamma$ and $YB_{10}\,y, YB_{10}\,y_2 \in \Gamma$, we have that $\Delta_f(y{:}y_2|Yy_1) \geq 1$. Similarly, $\Delta_f(y{:}y_2|Yy_1) \geq 1$ if $\varepsilon_2 = \varepsilon_3 = 0$. Suppose now that $\varepsilon = 0$ and $\delta = 1$. Then $YB_{11} \notin \Gamma$ while $YyB_{11} \in \Gamma$ and $Yz_1z_2 \in \Gamma$. If $\varepsilon_1 = 0$, then $Yyy_1 \in \Gamma$, and hence $\varepsilon_3 = 0$. If, in addition, $\varepsilon_0 = 1$, we have that $\varepsilon_2 = 1$ and, since $Yz_1z_2 \in \Gamma$, we have that $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$ or $YB_{11}B_{2k} \in \Gamma$ for $k = 0, 1$. Therefore, $\Delta_f(y{:}y_2|Yy_1) \geq 1$. If $\varepsilon_1 = \varepsilon_0 = 0$, Then $Yy_1y_2 \in \Gamma$. This implies that $\Delta_f(y{:}y_2|Yy_1) \geq 1$ because $YB_{11} \notin \Gamma$ while $YyB_{11} \in \Gamma$ and $YB_{11}B_{2k} \in \Gamma$ for $k = 0, 1$.

Case 7. *$X = Yz_1z_2$, where $Yyz \subseteq Py_1y_2$.* Take $\varepsilon_0 = g(Yz_1z_2) - g(Yy_1y_2)$, $\varepsilon_1 = g(Yz_1z_2y) - g(Yy_1y_2y)$, $\varepsilon_2 = g(Yz_1z_2z) - g(Yy_1y_2z)$ and $\varepsilon_3 = g(Yz_1z_2yz) - g(Yy_1y_2yz)$. Then $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_0$. Observe that $0 \leq \varepsilon_3 \leq \varepsilon_1, \varepsilon_2 \leq \varepsilon_0 \leq 2$, and hence $\varepsilon \geq -2$. 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 $\varepsilon_1 = \varepsilon_0$ and $\varepsilon_3 = \varepsilon_2$, and hence $\varepsilon = 0$. Moreover, $\delta = 0$ because $Yy_1y_2y \notin \Gamma$ if $Yy_1y_2 \notin \Gamma$. Suppose now that $y \in B_{10}$ and $z \in B_{11}$. We prove first that $\varepsilon \geq 0$. Three cases are considered.

1. If $\varepsilon_1 = 0$, then $YyB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, and hence $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, which implies that $\varepsilon_0 \leq 1$. If $\varepsilon_1 = 0$ and $\varepsilon_0 = 1$, then $YB_{11}B_{20} \notin \Gamma$ and $YzB_{11}B_{20} \notin \Gamma$, which implies that $\varepsilon_2 = 1$. Therefore, $\varepsilon = 0$ if $\varepsilon_1 = 0$.

2. Suppose now that $\varepsilon_1 = 1$ and $\varepsilon_2 = 0$. Then $YzB_{11}B_{20} \in \Gamma$, and hence $YB_{11}B_{20} \in \Gamma$. If $\varepsilon < 0$, then $\varepsilon_0 = 2$, and hence $YB_{10}B_{2k} \notin \Gamma$ for $k = 0, 1$, a contradiction with $\varepsilon_1 = 1$.

3. Consider now the case $\varepsilon_1 = \varepsilon_2 = 1$, and suppose that $\varepsilon < 0$. Then $\varepsilon_0 = 2$ and $\varepsilon_3 = 1$. Since $\varepsilon_1 = 1$, exactly one of the sets $YB_{10}B_{20}$, $YB_{10}B_{21}$ is in Γ. Moreover, $YB_{11}B_{20} \notin \Gamma$ while $YyB_{11}B_{20} \in \Gamma$. and $YzB_{10}B_{21} \in \Gamma$. This implies that $\varepsilon_3 = 0$, a contradiction.

Now, we have to prove that $\varepsilon \geq 1$ if $\delta = 1$. Suppose that, on the contrary, $\varepsilon = 0$ and $\delta = 1$. As before, we distinguish three cases.

1. If $\varepsilon_1 = 0$, then $YB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, and hence $Yz_1z_2 \in \Gamma$, a contradiction. Therefore, we assume from now on that $\varepsilon_1 \geq 1$, and hence $\varepsilon_0 \geq 1$.

2. If $\varepsilon_0 = 1$, then $N(Y) = 2$ and $YB_{11}B_{21} \notin \Gamma$ because $Yz_1z_2 \notin \Gamma$. This implies that $Yzz_1z_2 \notin \Gamma$, a contradiction.

3. If $\varepsilon_0 = 2$, then $N(Y) = 1$ and $YB_{11}B_{21} \in \Gamma$ because $Yzz_1z_2 \in \Gamma$. Therefore, $YyB_{10}B_{2k} \notin \Gamma$ for $k = 0, 1$, and hence $\varepsilon_1 = 2$. Moreover, $N(Yz) \geq 2$ and $YzB_{11}B_{20} \notin \Gamma$. If $YzB_{10}B_{20} \notin \Gamma$ or $YzB_{10}B_{21} \notin \Gamma$, then $\varepsilon_2 = 2$, and hence $\varepsilon_3 = 2$. This implies that $YyB_{11}B_{20} \notin \Gamma$, and hence $Yyz_1z_2 \notin \Gamma$, a contradiction. If $YzB_{10}B_{2k} \in \Gamma$ for $k = 0, 1$, then $\varepsilon_2 = 1$, and hence $\varepsilon_3 = 1$. Again, this implies that $Yyz_1z_2 \notin \Gamma$, a contradiction.

□

8 Conclusion

Even though other methods have been used for linear secret sharing schemes [1, 3, 19], the only known general technique to find lower bounds on the length of the shares in secret sharing is the one formalized by Csirmaz [10]. By this method, the lower bounds are derived from linear programs that involve information inequalities.

In the same line as the works by Csirmaz [10] and Beimel and Orlov [5], we present some limitations on 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 5.2). 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 7.6). Both results are proved by similar techniques. Namely, by finding 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 7.6 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 [24].

Acknowledgements

We thank Amos Beimel and Ilan Orlov for useful discussions about the contents of this paper. The first author's work was partially supported by the Spanish Government through the project MTM2009-07694. 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., Gál, A., Paterson, M.: Lower bounds for monotone span programs. Comput. Complexity 6, 29–45 (1997)

[4] 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.

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

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

[7] 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)

[8] 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)

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

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

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

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

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

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

[15] 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)

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

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

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

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

[20] 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)

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

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

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

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

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

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

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

[28] 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)

[29] 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)

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

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

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

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

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