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

February 17, 2013

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 negative result about the power of information inequalities in the search for lower bounds in secret sharing. Namely, we prove that all information inequalities on a bounded number of variables only can provide lower bounds that are polynomial on the number of participants.

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

1 Introduction

Secret sharing schemes, which were independently introduced by Shamir [27] 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 [20], 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.

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 [9], 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, 17]. 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.

Similarly to the works by Csirmaz [9] 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. This is the case of the bounds in [7, 8, 9, 21] and many other papers. Even though it was implicitly used before, the method was formalized by Csirmaz [9]. 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 the fact that certain linear combinations of the values of the joint entropies of the random variables defining a secret sharing scheme must be nonnegative. These constraints can be divided into two classes.

1. The first class is formed by the constraints that are derived from the access structure. Namely, from the fact that the qualified subsets can recover the secret while the unqualified ones have no information about it.

2. The second class is formed by constraints derived from *information inequalities* that hold for every collection of random variables.

In the second class, the constraints derived from the so-called *Shannon inequalities* are always considered. These basic information inequalities are equivalent to the conditional mutual information being nonnegative, and equivalent as well to the fact that the joint entropies of a collection of random variables define a polymatroid [15, 16].

Csirmaz [9] proved that, by taking only the Shannon inequalities in the second class, one obtains lower bounds that are at most linear on the number of participants. This was proved by showing that every such linear program admits a small solution.

One may expect that better lower bounds should be obtained by adding to the second class new constraints derived from the *non-Shannon information inequalities*, which are the ones that cannot be derived from the basic Shannon inequalities. The existence of such inequalities was unknown when Csirmaz [9] formalized that method. The first one was presented by Zhang and Yeung [30] and many others have been found subsequently [11, 13, 23, 29]. When dealing with 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 [19]. Other rank inequalities have been presented afterwards [12, 22]. Indeed, better lower bounds on the information ratio have been found for some families of access structures by using non-Shannon information and rank inequalities [4, 10, 24, 25].

Nevertheless, Beimel and Orlov [5] presented a negative result about the power of non-Shannon information inequalities to provide better general lower bounds on the size of the shares. Specifically, they proved that the best lower bound that can be obtained by using all information inequalities on four and five variables, together with all inequalities on more than five variables that are known to date, is at most linear on the number of participants. Specifically, they proved that every linear program that is obtained by using these inequalities

admits a small solution that is related to the solution used by Csirmaz [9] to prove his negative result. They used 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 [12, 18]. 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 [29]. 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 negative result about the power of information inequalities to provide general lower bounds on the size of the shares in secret sharing schemes. Namely, we prove 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, 9], 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, 9].

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.

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 [26, 28]. For a finite set Q, we notate $\mathcal{P}(Q)$ for the power set of Q, that is, the set of all subsets of Q.

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

A polymatroid is called *integer* if its rank function is integer-valued.

The following characterization of rank functions of polymatroids is a straightforward consequence of [26, Theorem 44.1].

Proposition 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 the following properties are satisfied.*

- $f(\emptyset) = 0$.
- *If $X \subseteq Q$ and $y \in Q$, then $f(X) \leq f(X \cup \{y\})$.*
- *If $X \subseteq Q$ and $y, z \in Q$, then $f(X \cup \{y, z\}) + f(X) \leq f(X \cup \{y\}) + f(X \cup \{z\})$.*

If $\mathcal{S} = (Q, f)$ is a polymatroid and α is a positive real number, then $\alpha\mathcal{S} = (Q, \alpha f)$ is a polymatroid as well, which is called a *multiple* of $\mathcal{S}$. A polymatroid $\mathcal{S}' = (Q', g)$ is called an *extension* of a polymatroid $\mathcal{S} = (Q, f)$ if $Q \subseteq Q'$ 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.

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* or $\mathbb{K}$-*representable*, and the tuple $(V_x)_{x\in Q}$ is called a $\mathbb{K}$-*linear representation* of $\mathcal{S}$. A $\mathbb{K}$-*poly-linear polymatroid* is the multiple of a $\mathbb{K}$-linear polymatroid.

For a finite set Q, consider a family of random variables $(S_x)_{x\in Q}$, where S_x is defined on a finite set E_x. For every $X \subseteq Q$, we use S_X to denote the random variable $(S_x)_{x\in X}$ on the set $\prod_{x\in X} E_x$, and $H(S_X)$ will denote its Shannon entropy. Fujishige [15, 16] found out the following connection between Shannon entropy and polymatroids.

Theorem 2.3. *Let $(S_x)_{x\in Q}$ be a family of random variables. Consider the mapping $h\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(X) = H(S_X)$ if $\emptyset \neq A \subseteq Q$. Then h is the rank function of a polymatroid with ground set Q.*

A polymatroid $\mathcal{S} = (Q, h)$ is said to be *entropic* if there exists a family $(S_x)_{x\in Q}$ of discrete random variables such that $h(X) = H(S_X)$ for every $X \subseteq Q$. A *poly-entropic polymatroid* is a multiple of an entropic polymatroid. It is well known that, if $\mathbb{K}$ is a finite field, then every $\mathbb{K}$-poly-linear polymatroid is poly-entropic. Indeed, given a $\mathbb{K}$-vector space E, let E^* be its *dual space*, which is formed by all linear forms $\alpha : E \to \mathbb{K}$, and S the random variable given by the uniform probability distribution on E^*. For every subspace $V \subseteq E$, consider the random variable $S|_V$ on V^*, the restriction of S to V. Clearly, $H(S|_V) = \log|\mathbb{K}| \dim V$. Therefore, the $\mathbb{K}$-linear polymatroid given by a collection $(V_x)_{x\in Q}$ of subspaces of E is a multiple of the entropic polymatroid defined by $(S_x)_{x\in Q}$, where $S_x = S|_{V_x}$. The collections of random variables that can be defined in this way are said to be $\mathbb{K}$-*linear*.

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. Clearly, $(\mathbf{e}^w)_{w\in M}$ is a basis of $\mathbb{K}^M$. For every $x \in Q$, consider the vector subspace $V_x = \langle \mathbf{e}^w : w \in M_x \rangle$. Obviously, 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 2.2, 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 [14].

For a positive integer r, we notate $[r] = \{1, \ldots, r\}$. Given 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 poly-entropic, respectively poly-linear, polymatroid (Q, f) and for every collection $(A_i)_{i\in[r]}$ of r subsets of Q.

Obviously, every information inequality is also a rank inequality. By Theorem 2.3, the polymatroid axioms are information inequalities, which are called *Shannon inequalities*. The Ingleton inequality [19] was the first known example of a rank inequality that cannot be derived from Shannon-type inequalities. Zhang and Yeung [30] presented the first information inequality that cannot be derived from the Shannon inequalities. Subsequently, many other rank and information inequalities have been found in [11, 12, 13, 22, 23, 29] and other works. We need the following technical result, which is a consequence of [5, Lemma 4.3].

Lemma 2.4. *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*, $p_0 \notin P$ a special participant, usually called *dealer*, and $Q = P \cup \{p_0\}$. 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. For a polymatroid $\mathcal{S} = (Q, f)$ and an element $p_0 \in Q$ with $f(\{p_0\}) > 0$, we define the access structure $\Gamma_{p_0}(\mathcal{S})$ on $P = Q \setminus \{p_0\}$ by

$$\Gamma_{p_0}(\mathcal{S}) = \{X \subseteq P \,:\, f(X \cup \{p_0\}) = f(X)\}.$$

We need as well the parameter

$$\sigma_{p_0}(\mathcal{S}) = \frac{\max_{x\in P} f(\{x\})}{f(\{p_0\})}.$$

If $\Gamma = \Gamma_{p_0}(\mathcal{S})$ and, in addition, $f(X \cup \{p_0\}) = f(X) + 1$ for every unqualified set $X \subseteq P$, then $\mathcal{S}$ is said to be a Γ-*polymatroid*.

A *secret sharing scheme* Σ on P with access structure Γ is a family $(S_x)_{x\in Q}$ of random variables such that

1. $H(S_{X\cup\{p_0\}}) = H(S_X)$ if $X \in \Gamma$ and
2. $H(S_{X\cup\{p_0\}}) = H(S_X) + H(S_{p_0})$ otherwise.

The random variables S_{p_0} 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 collection of random variables. The *information ratio* $\sigma(\Sigma)$ of the secret sharing scheme Σ is the ratio between the maximum length of the shares and the length of the secret. Namely,

$$\sigma(\Sigma) = \frac{\max_{x\in P} H(S_x)}{H(S_{p_0})}.$$

The entropic polymatroid $\mathcal{S}$ defined by the collection $(S_x)_{x\in Q}$ is such that $\Gamma = \Gamma_{p_0}(\mathcal{S})$ and, in addition, $\sigma(\Sigma) = \sigma_{p_0}(\mathcal{S})$.

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,

$$\sigma(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a poly-entropic } \Gamma\text{-polymatroid}\}.$$

Therefore, the parameters

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}$$

and

$$\lambda(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a poly-linear } \Gamma\text{-polymatroid}\}$$

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 [25]. Most of the known lower bounds on the information ratio, as the ones from [7, 8, 9, 21], 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, 10, 24, 25].

A polymatroid $\mathcal{S} = (P, f)$ and an access structure Γ on a set P are said to be *compatible* if $\mathcal{S}$ can be extended to a Γ-polymatroid $\mathcal{S}(\Gamma) = (Q, f)$.

Proposition 3.1. *An access structure Γ on P is compatible with a polymatroid $\mathcal{S} = (P, f)$ if and only if the following conditions are satisfied.*

1. *If $X \subseteq P$ and $y \in P$ are such that $X \notin \Gamma$ and $X \cup \{y\} \in \Gamma$, then $f(X) \leq f(X \cup \{y\}) - 1$.*
2. *If $X \subseteq P$ and $y, z \in P$ are such that $X \notin \Gamma$ while both $X \cup \{y\}$ and $X \cup \{z\}$ are qualified, then $f(X \cup \{y, z\}) + f(X) \leq f(X \cup \{y\}) + f(X \cup \{z\}) - 1$.*

Proof. Suppose that $\mathcal{S}$ can be extended to a Γ-polymatroid $\mathcal{S}(\Gamma) = (Q, f)$. If $X \notin \Gamma$ and $X \cup \{y\} \in \Gamma$, then $f(X \cup \{y\}) = f(X \cup \{y, p_0\}) \geq f(X \cup \{p_0\}) = f(X) + 1$. If $X \notin \Gamma$ and $X\cup\{y\}$ and $X\cup\{z\}$ are qualified, then $f(X\cup\{y\})+f(X\cup\{z\}) = f(X\cup\{y, p_0\})+f(X\cup\{z, p_0\}) \geq f(X \cup \{y, z, p_0\}) + f(X \cup \{p_0\}) = f(X \cup \{y, z\}) + f(X) + 1$.

We prove now the converse. Assume that $\mathcal{S} = (P, f)$ satisfies the conditions in the statement and consider the extension of f to $\mathcal{P}(Q)$ determined by $f(X \cup \{p_0\}) = f(X)$ if $X \in \Gamma$ and $f(X \cup \{p_0\}) = f(X) + 1$ otherwise. We have to prove that (Q, f) is a polymatroid. Clearly,

$f(X) \leq f(X \cup \{p_0\})$ and $f(X \cup \{p_0\}) \leq f(X \cup \{p_0, y\})$ for every $X \subseteq P$ and $y \in P$. Therefore, the first condition in Proposition 2.2 is satisfied. Moreover, it is not difficult to prove that the second condition holds as well by checking that $f(X \cup \{y, p_0\}) + f(X) \leq f(X \cup \{y\}) + f(X \cup \{p_0\})$ and $f(X \cup \{p_0, y, z\}) + f(X \cup \{p_0\}) \leq f(X \cup \{p_0, y\}) + f(X \cup \{p_0, z\})$ for every $X \subseteq P$ and $y, z \in P$. □

The following result was presented by Csirmaz [9].

Proposition 3.2. *An access structure Γ on P is compatible with a polymatroid $\mathcal{S} = (P, f)$ if and only if the following conditions are satisfied.*

1. *If $X \subseteq Y \subseteq P$ are such that $X \notin \Gamma$ and $Y \in \Gamma$, then $f(X) \leq f(Y) - 1$.*
2. *If $X, Y \in \Gamma$ and $X \cap Y \notin \Gamma$, then $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y) - 1$.*

Proof. Necessity can be proved in a similar way as in Proposition 3.1. Sufficiency is obvious from Proposition 3.1. □

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 structure 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 the following conditions are satisfied.*

1. *If $X \subseteq P$ and $z \in P \setminus X$, then $f(X) \leq f(X \cup \{z\}) - 1$.*
2. *If $X \subseteq P$ and $y, z \in P \setminus X$, then $f(X \cup \{y, z\}) + f(X) \leq f(X \cup \{y\}) + f(X \cup \{z\}) - 1$.*

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 from 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 $B(P, r)$ 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 $M(P, r) \setminus M_X(P, r)$ are the ones involving only elements in $P \setminus X$. That is, $M(P, r) \setminus M_X(P, r) = M(P \setminus X, r)$, and hence

$$f(X) = |M_X(P, r)| = |M(P, r)| - |M(P \setminus X, r)| = \binom{|P| + r - 1}{r} - \binom{|P| - |X| + r - 1}{r}.$$

Therefore, if $|P| = n$, the increment vector $(\delta_1, \ldots, \delta_n)$ 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 $i = 1, \ldots, n$. 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 [9]. 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 Main Result

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

Proposition 5.1. *Let P be a set of n participants, Γ an access structure on P, $r \geq 3$ an integer, and $\mathcal{Z}_{r-1} = \mathcal{Z}(P, r-1)$. Then the Γ-polymatroid $\mathcal{Z}_{r-1}(\Gamma)$ that is an extension of $\mathcal{Z}_{r-1}$ to $Q = P \cup \{p_0\}$ 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 $B_i = A_i \smallsetminus \{p_0\}$. 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

$$\sum_{I \subseteq [r]} \alpha_I f(A_I) = \sum_{I \subseteq [r]} \alpha_I f(B_I) + \sum_{I \,:\, p_0 \in A_I} \alpha_I \geq 0$$

by Lemma 2.4. 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 $I \subseteq [r]$. The polymatroid $\mathcal{S}$ is Boolean, and hence it is linearly representable over every field. 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 $\mathcal{S}$. We describe next a linear representation of $\mathcal{S}$. Let $\mathbb{K}$ be a field. Given the basis $(\mathbf{e}^w)_{w \in M}$ of $\mathbb{K}^M$, 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 access structure Λ on $[r]$ formed by the sets $I \subseteq [r]$ such that $B_I \in \Gamma$. Consider as well 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 $J \neq \emptyset, [r]$. In addition, $B_I \notin \Gamma$ and $B_I \cup B_j \in \Gamma$ for every $j \in J$. 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 $\mathcal{S}' = ([r] \cup \{0\}, g)$ of $\mathcal{S}$ is obtained.

We prove next that $\mathcal{S}'$ 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 $g(I \cup \{0\}) = g(I) + 1$.

Since $\mathcal{S}' = ([r] \cup \{0\}, g)$ is a Λ-polymatroid, $f(A_I) = g(I \cup \{0\})$ if $p_0 \in A_I$. Finally,

$$\begin{aligned}\sum_{I \subseteq [r]} \alpha_I f(A_I) &= \sum_{I\,:\,p_0 \notin A_I} \alpha_I f(B_I) + \sum_{I\,:\,p_0 \in A_I} \alpha_I f(A_I) \\ &= \sum_{I\,:\,p_0 \notin A_I} \alpha_I g(I) + \sum_{I\,:\,p_0 \in A_I} \alpha_I g(I \cup \{0\}) \geq 0\end{aligned}$$

because $\mathcal{S}'$ is linearly representable. □

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*

$$\binom{n+r-3}{r-2},$$

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 $\sigma_{p_0}(\mathcal{Z}_{r-1}(\Gamma)) = \delta_1$, where δ_1 is the first component of the increment vector of $\mathcal{Z}(P, r-1)$. □

Acknowledgements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] C. Padró, L. Vázquez, A. Yang. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. To appear in *Discrete Applied Mathematics* (2013).

[26] A. Schrijver. *Combinatorial optimization. Polyhedra and efficiency*. Springer-Verlag, Berlin, 2003.

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

[28] D. J. A. Welsh. *Matroid Theory*. Academic Press, London, 1976.

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

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