On the theory of linear rank inequalities

Carolina Mejía Moreno

Universidad Nacional de Colombia

Facultad de Ciencias, Departamento de Matemáticas

Bogotá, Colombia

2016

On the theory of linear rank inequalities

Carolina Mejía Moreno

Dissertation submitted to the Department of Mathematics in partial fulfilment of the requirements for the degrees of

Doctor of Philosophy in Mathematics

Advisor:

Dr. Humberto Sarria Zapata

Research Topic: Information Theory

Research Group: Teoría de Matrices

Universidad Nacional de Colombia

Facultad de Ciencias, Departamento de Matemáticas

Bogotá, Colombia

2016

Approved by

_____

Professor Lazlo Cirmaz

_____

Professor Diana Bueno Carreño

_____

Professor Jorge Eduardo Ortiz

Dedication

This thesis is dedicated to my wonderful family. To my parents who for making me be who I am. To my sons, Sebastián and Federico, they make me very very very happy. And finally, to Andrés for supporting me all the way.

Acknowledgement

I wish to express my gratitude to Professor Humberto Sarria who proposed the topics of this research. Thanks for providing me an opportunity to work in his group.

I sincerely thank Professor Lazlo Csirmaz for his valuable suggestions and timely comments.

Finally I want to thank COLCIENCIAS for their financial support. Without this had not been possible to complete this dissertation.

Resumen

En este trabajo estudiamos los polimatroides lineales y las desigualdades rango lineales. Nos enfocamos en el problema de determinar si el Método de la Información Común puede generar todas las desigualdades rango lineales, que son las desigualdades satisfechas por todos los polimatroides lineales. Se sabe que existen conexiones profundas entre la Teoría de desigualdades rango lineales y el Problema de Repartición Lineal de Secretos. En este texto estudiamos estas conexiones. Primero, estudiamos el problema de estimar las ratas de información que pueden ser alcanzadas por soluciones lineales al Problema de Repartición de Secretos. Luego, llegamos a la nueva noción de Repartición Abeliana de Secretos. Probamos que si las soluciones abelianas al Problema de Repartición de Secretos superan a las soluciones lineales, entonces el Método de la Información Común es incompleto. Por lo tanto, nos enfocamos en el problema de comparar las representaciones de esquemas abelianos y lineales. Nosotros probamos que este último problema está relacionado con la Teoría de Representación de Matroides.

Palabras clave: Polimatroides lineales, desigualdades rango lineales, Repartición de Secretos, esquemas lineales, polimatroides abelianos, matroides.

Clasificación por temas según AMS: 94A15, 94A60, 62B10, 94A17

Abstract

In this work, we study linear polymatroids and linear rank inequalities. We focus on the problem of determining if the Common Information Method can generate all the linear inequalities satisfied by all linear polymatroids. It is well known that there exist deep connections between the Theory of Linear Rank Inequalities and Linear Secret Sharing. We study those connections. First, we study the problem of estimating the information rates that can be achieved by Linear Secret Sharing. Then, we arrive to the novel notion of Abelian Secret Sharing. We prove that if Abelian Secret Sharing outperforms Linear Secret Sharing, then the Common Information Method is incomplete. Therefore, we focus on the problem of comparing the performances of abelian and linear schemes. We show that the last problem is related to the Representation Theory of Matroids.

Keywords: Linear polymatroids, linear rank inequalities, Secret Sharing, linear schemes, abelian polymatroids, matroids.

Mathematics subject classification: 94A15, 94A60, 62B10, 94A17

Publications related to this thesis

- C. Mejia. Linear secret sharing and the automatic search of linear rank inequalities. *Applied Mathematical Science*, 9 (2015), 5305 - 5324

- A. Gomez, C. Mejia, and J.A. Montoya. Linear network coding and the model theory of linear rank inequalities. *IEEE International Symposium on Network Coding* (NetCod) (Aalborg, Denmark), (2014), 1 - 6.

- A. Gomez, C. Mejia, and J.A. Montoya. Network coding and the model theory of linear information inequalities. *IEEE International Symposium on Network Coding* (NetCod) (Aalborg, Denmark), (2014), 1 - 6.

Contents

Chapter 1

Introduction

In this dissertation we study linear rank functions, we also study linear rank inequalities, which are the linear inequalities satisfied by those submodular functions. Linear rank functions are interesting because of their relation with Linear Network Coding and Linear Secret Sharing (the interested reader can see [6]). We show, in this work, that they can be used to compute information rates for general access structures, see Theorem 55. It is important to remark that such an application depends on a fine understanding of the linear regions, which are the convex cones constituted by those functions. Thus, we have tried to unveil the geometrical and logical structure of those regions and we could say that we have partially succeed.

The low dimensional linear regions are well understood. It is known that for one, two and three variables, those regions are equal to the convex cones of polymatroidal functions defined by the so called *Shannon inequalities*. It is also known that the linear region of order four is defined by the Shannon inequalities plus the Ingleton inequalities. The structure of the linear region of order five was unveiled few years ago thanks to the work of Dougherty, Freiling and Zeger [13]. To this end, they introduced the common information method, which is an heuristics that can be used to search for linear rank inequalities. They used this method to compute the several thousands of linear inequalities defining the linear region of order five. They tried to make the same work for the linear region of

order six, but the combinatorial explosion was an obstacle that they could not overcome.

In despite of the important applications of linear rank functions, there are few published works related to this class of polymatroidal functions. Perhaps, the most important work on this subject is the aforementioned paper of Dougherty, Freiling and Zeger [13]. At the very end of this paper, the authors asked two important questions:

- Are the linear regions polyhedral cones?
- Is the common information method a complete method?

We would like to shed some light on the first problem, but we have little to say on this subject. We have focused on the second question. Thus, we have tried to prove, in this dissertation, that the common information method is not complete. It means that there exist linear rank inequalitites which cannot be obtained via this method. To begin with, we present the method as a rigorous algorithm which can be analyzed with the available tools of the theory of computation. It allowed us to reformulate the question of Dougherty, Freiling and Zeger [13] in the following way: Can any linear rank inequality be obtained as an output of the CI algorithm, (see algorithm 40), presented in this work? It is the problem that we attack in this dissertation. We think that such a problem is a hard piece of work, given that, among other things, we do not have a characterization of the linear rank inequalitites. Such a characterization could be used as a standard to measure the completeness of our algorithm. Thus, we had to try some indirect strategies. Actually, the core of this dissertation is constituted by the study of two strategies intended to prove that the CI algorithm is not complete. We will call those strategies *the asymptotic and the abelian attacks*.

It is known that there exist access structures, in Secret Sharing, whose optimal information rates are superpolynomial, [2] and [21]. Then, a complete set of linear rank inequalities must allow one to establish superpolynomial lower bounds on the share complexity of general access structures. Thus, the core idea of the asymptotic attack, which

arose in the classical work of Csirmaz, [11], consists in proving that the set of linear rank inequalities, that can be obtained via the CI algorithm, cannot yield the superpolynomial lower bounds predicted by the theory. We got some partial results in this direction (see Theorems 59 and 60). We could prove that, if we restrict our attention to a special subset of the output set of our algorithm, then we will get lower bounds on the share complexity which are of cubic order. It means that such a special subset cannot be equal to the whole set of linear rank inequalities.

Linear polymatroids are the entropic polymatroids that are related to the arrays of linear random variables, and those variables are the random variables that are naturally defined by vector subspaces and linear maps. Linear random variables have common information, see Definition 32, and it is a consequence of the algebraic nature of those variables. The common information method is based on this fact. Thus, it is natural to ask if there does exist a larger class of algebraic variables having common information. Notice that all the linear rank inequalities that can be obtained via the common information method must hold for all the entropic polymatroids determined by such more general type of random variables. Thus, if one can construct such a larger class of algebraic random variables, and he is able to prove that there exists a polymatroid determined by a tuple of those variables, which is not a linear polymatroid, he will get as a corollary that the CI algorithm is not complete. It is the core idea of our abelian attack. We prove that abelian variables (see Section 6.1) have common information. It allows us to reduce our problem to the problem of constructing an abelian polymatroid which cannot be approximated by a sequence of linear polymatroids. In order to attack the last problem, we use a connection between Secret Sharing and Matroid Theory, which we will explain in the next paragraph.

It is not easy to search for an access structure whose abelian rate is strictly smaller than its linear rate. Suppose that we have an access structure, say M, which is a good candidate to be the separator we are looking for. How can we prove that the abelian

rate of M is strictly smaller than its linear rate? Take into account that it is not known if the problem of computing optimal rates can be algorithmically solved. One can try to establish a lower bound α for the linear rate of M, together with an upper bound β for its abelian rate, and such that $\beta < \alpha$. How can one establish such bounds? Using the right linear rank inequalities. Notice that the above claim implies that he must know a linear rank inequality which holds for all the linear polymatroids, but which does not hold for some abelian polymatroids. Then, in some sense, he must know in advance the solution of the problem. How can we overcome the aforementioned difficulties? We restricted our search to a class of access structures coming from matroids, and we ask if there does exist one of those structures, which admits an ideal abelian secret sharing scheme, but which does not admit ideal linear secret sharing (see definition 69). In order to attack this last problem, we characterize the matroids that admit ideal secret sharing, see Lemma 83. We could not find an analogous characterization for abelian ideal secret sharing, but the aforementioned positive result allowed us to reduce our motivating problem (the completeness of the common information method) to a very concrete combinatorial problem about matroids of small size, see Section 6.6.

Part I

Basics

Chapter 2

Mathematical background

2.1 Polymatroids

We begin by introducing the fundamental notion of polymatroid. Polymatroidal functions, also called submodular functions, have played an important role in discrete optimization, see [15].

Definition 1 (Polymatroid) *We say that a function* $h : (\wp([n]) \setminus \{\emptyset\}) \to \mathbb{R}^+$*, where* $[n] = \{1, 2, ..., n\}$*, is a polymatroid of order* n*, if and only if,* h *satisfies the following two properties:*

1. ***MONOTONE*** *Given* $I, J \in (\wp([n]) \setminus \{\emptyset\})$*, if* $I \subseteq J$ *then* $h(I) \leq h(J)$*.*
2. ***SUBMODULAR*** *For all* $I, J \in (\wp([n]) \setminus \{\emptyset\})$*, we have that* $h(I \cup J) + h(I \cap J) \leq h(I) + h(J)$*.*

We fix the convention that $h(\emptyset) = 0$, hence if $I \cap J = \emptyset$ the submodularity condition corresponds to the inequality $h(I \cup J) \leq h(I) + h(J)$.

Notice that one can think of a polymatroid of order n as it were an element of $\mathbb{R}^{2^n-1}$. To this end, he can fix a bijection from $[2^n - 1]$ to $\wp([n]) \setminus \{\emptyset\}$, and use the bijection to

define a labeling of the canonical vectors of $\mathbb{R}^{2^n-1}$ (using as labels the nonempty subsets of $[n]$). Suppose that, for $n \geq 1$, we have already fixed such a labeling and that h is a polymatroid of order n, then we can express h as

$$h = \sum_{I \in (\wp([n]) \setminus \{\emptyset\})} h(I)\, e_I$$

We will use the symbol Γ_n to denote the set of all the polymatroids of order n. Notice that $\Gamma_n \subseteq \mathbb{R}^{2^n-1}$ is a closed convex cone, which is defined by a finite list of linear inequalities, ensuring that polymatroids are monotone and submodular (see definition 1). Thus, we have that Γ_n is a *polyhedral cone*. The polymatroidal inequalities defining Γ_n are also called *Shannon inequalities*.

Example 2 *Consider the case $n = 2$. The set Γ_2 is the convex cone of all the polymatroids of order 2. Let $h \in \Gamma_2$, function h is defined over the set $\wp([2]) \setminus \{\emptyset\}$, which is equal to $\{\{1\}, \{2\}, \{1,2\}\}$, to $\mathbb{R}^+$. Furthermore, h must satisfies the conditions imposed in the definition 1, that is:*

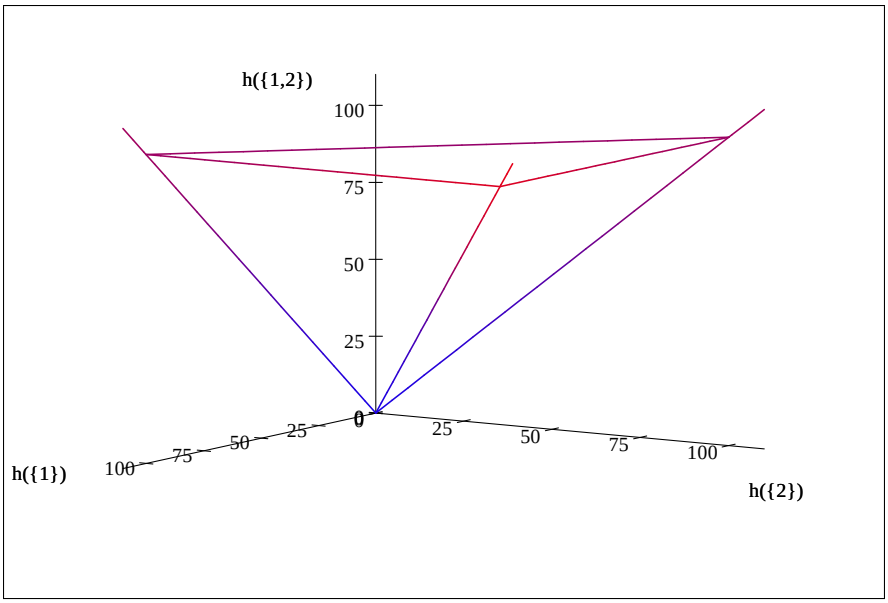
1. *Function h is monotone. Then, we have*

$$\begin{aligned} h(\{1\}) &\leq h(\{1,2\}) \\ h(\{2\}) &\leq h(\{1,2\}) \end{aligned}$$

2. *Function h is submodular, then we have that*

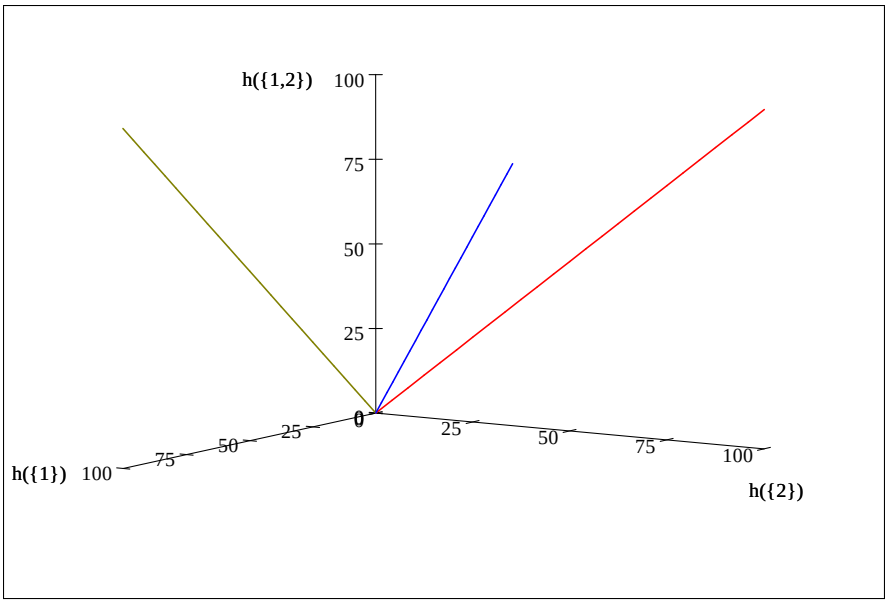
$$h(\{1,2\}) \leq h(\{1\}) + h(\{2\})$$

The above three inequalities, and the positivity condition imposed on the rank of h, are the linear inequalities defining the polyhedral cone Γ_2. We include, below, a graphic representing a truncated version of Γ_2.



Definition 3 (Extremal rays) *Given a closed convex cone $\Delta \subseteq \mathbb{R}^n$, and given $v \in \Delta$, we say that v belongs to an extremal ray of Δ, if and only if, for all $u, w \in \Delta$ and for all $\alpha, \beta \in \mathbb{R}$, if the equality $v = \alpha u + \beta w$ holds, then u and w are scalar multiples of v.*

Example 4 *Now, we can compute, as an example, the extremal rays of the convex cone Γ_2. The extremal rays are the intersection lines of the planes (faces), defining Γ_2 in the above example. We can plot those rays*



which are equal to the lines defined by:

$$\begin{aligned} L_1 &\rightarrow (h(\{1\}), h(\{2\}), h(\{1,2\})) = (1,1,1)\, t \\ L_2 &\rightarrow (h(\{1\}), h(\{2\}), h(\{1,2\})) = (1,0,1)\, t \\ L_3 &\rightarrow (h(\{1\}), h(\{2\}), h(\{1,2\})) = (0,1,1)\, t \end{aligned}$$

Definition 5 (Conic closure) *Given $A \subseteq \mathbb{R}^n$, the conic closure of A, denoted with the symbol $cc(A)$, is the set*

$$cc(A) = \left\{ u \in \mathbb{R}^n : (\exists m \in \mathbb{N})(\exists \alpha_1, ..., \alpha_m \geq 0)(\exists v_1, ..., v_m \in A)\left(u = \sum_{i=1}^{m} \alpha_i v_i \right) \right\}$$

A convex cone $\Delta \subseteq \mathbb{R}^n$ is a polyhedral cone, if and only if, it has a finite number of extremal rays. Moreover, if Δ is polyhedral, it is completely determined by the finite set of its extremal rays: Δ is the conic closure of its extremal rays.

The notion of polymatroid is related to the mathematical notion of dimension. It becomes clear if we consider the different classes of polymatroids that one can find in the

literature. A first example is the class of boolean polymatroids, which are related to the set-theoretical notion of cardinality. Let $A = (A_1, ..., A_n)$ be a tuple of finite sets, this tuple determines a boolean polymatroid of order n, which we denote with the symbol h_A and which is defined by:

$$\text{given } I \subseteq [n]\,,\ I \neq \emptyset, \text{ we have that } h_A(I) = \left|\bigcup_{i \in I} A_i\right|$$

2.2 Entropic functions

A second important example of polymatroid is the class of *entropic polymatroid.* Entropic polymatroids are related to the notion of statistical dimension. Given a tuple of finite random variables $X = (X_1, ..., X_n)$, this tuple determines an entropic polymatroid of order n, which is denoted with the symbol h_X, and which we define by:

$$\text{given } I \subseteq [n]\,,\ I \neq \emptyset, \text{ we have that } h_X(I) = H(X_I)$$

where X_I denotes the tuple $(X_i)_{i \in I}$, and $H(X_I)$ denotes its *Shannon entropy.* First, some definitions.

Definition 6 (Entropy) *Let X be a discrete random variable with alphabet $\mathcal{X}$ and probability mass function*

$$p(x) = \Pr\{X = x\}$$

where $x \in \mathcal{X}$. The Shannon entropy of X, or just entropy, is defined by

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x)$$

The interested reader can check, for example [10].

A second important notion is the notion of Conditional Entropy.

Definition 7 (Conditional Entropy) *Given X and Y two random variables, the conditional entropy of X given Y, which we denote with the symbol $H(X \mid Y)$ is equal to*

$$H(X,Y) - H(Y)$$

The symbol $H(X,Y)$ denotes the join entropy of X and Y, which is equal to the entropy of the join random variable (X,Y).

The next definition allow us measure the amount of information that is shared by two random variables.

Definition 8 (Mutual Information) *Let X, Y be two random variables. The mutual information $I(X;Y)$ can be defined as*

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$

2.2.1 Almost entropic polymatroids and the entropic regions

Given $X = (X_1, ..., X_n)$, a n-tuple of random variables, and $I \subset [n]$, $I \neq \emptyset$, we have that the equality

$$\langle h_X, e_I \rangle = H_X(I)$$

holds. Here, the symbol $\langle\rangle$ denote the canonical inner product of $\mathbb{R}^{2^n-1}$. The vector $(H_X(I))_{I \in \wp([n]) \setminus \{\emptyset\}}$ is the *entropic vector* associated to the tuple X.

Definition 9 *The set of entropic vectors of order n is the set*

$$\Gamma_n^* = \left\{ v \in \mathbb{R}^{2^n-1} : v \text{ is an entropic vector} \right\}$$

We use the term *entropic region of order* n to denote the set $\overline{\Gamma_n^*}$, the topological closure of Γ_n^*. Thus, for all $n \geq 1$ we have an entropic region, *the entropic region of order* n, which is a subset of $\mathbb{R}^{2^n-1}$. The elements of $\overline{\Gamma_n^*}$ will be called *almost-entropic vectors*. It is known that for all $n \geq 1$ the set $\overline{\Gamma_n^*}$ is a closed convex cone [33]. Let $n \geq 1$, is the convex cone $\overline{\Gamma_n^*}$ a polyhedral cone?

Definition 10 (Linear Information Inequalities) *An information inequality of order* n *is a vector* $a \in \mathbb{R}^{2^n-1}$*, such that for all* $v \in \overline{\Gamma_n^*}$*, we have that* $\langle a, v \rangle \geq 0$.

The set of linear information inequalities in n random variables is a subset of $\mathbb{R}^{2^n-1}$, we use the symbol $\left(\overline{\Gamma_n^*}\right)^\circ$ to denote this set.

Definition 11 *Given* $A \subset \mathbb{R}^n$*, the polar set of* A*, denoted by the symbol* A°*, is the set*

$$\{v \in \mathbb{R}^n : (\forall w \in A)\,(\langle v, w \rangle \geq 0)\}$$

Notice that $\left(\overline{\Gamma_n^*}\right)^\circ$ is the *polar cone* of $\overline{\Gamma_n^*}$, and as a consequence it is also a closed convex cone (the interested reader can consult [18]).

Definition 12 *Given* $A \subset \left(\overline{\Gamma_n^*}\right)^\circ$*, and* $v \in \left(\overline{\Gamma_n^*}\right)^\circ$*, we say that* A *entails* v*, if and only if, there exist* $m \geq 1$*,* $v_1, ..., v_m \in A$ *and* $\alpha_1, ..., \alpha_m \in \mathbb{R}^+$*, such that*

$$v = \alpha_1 v_1 + ... + \alpha_m v_m$$

Notice that $\left(\overline{\Gamma_n^*}\right)^\circ$ is a polyhedral cone, if and only if, there exists a finite subset of $\left(\overline{\Gamma_n^*}\right)^\circ$, say B, such that B entails all the linear inequalities included in $\left(\overline{\Gamma_n^*}\right)^\circ$. It was conjectured for long time that for all $n \geq 1$, the cone $\overline{\Gamma_n^*}$ is polyhedral and that the equality $\overline{\Gamma_n^*} = \Gamma_n$ holds. We know, nowadays, that:

1. For all $n \leq 3$, the equality $\overline{\Gamma_n^*} = \Gamma_n$ holds [33].

2. For all $n \geq 4$, the cone $\overline{\Gamma_n^*}$ is not polyhedral [25], and then the equality $\overline{\Gamma_n^*} = \Gamma_n$ does not hold. The theorem ensuring that $\overline{\Gamma^*}$ is not polyhedral (provided $n \geq 4$) is the so called Matúš Theorem. Moreover, it seems that, for all $n \geq 4$, the cone $\overline{\Gamma_n^*}$ is not semialgebraic [16], and as a consequence we have that those cones cannot be defined by algebraic inequalities.

2.3 Linear polymatroids, cc-linear polymatroids and the linear regions

A third important example of polymatroids is related to the notion of linear dimension, it is the class of linear polymatroids which we study in this dissertation.

Definition 13 (Linear polymatroid) *A linear polymatroid of order n is a polymatroid $h : (\wp([n]) \setminus \{\emptyset\}) \to \mathbb{R}^+$, for which there exists a tuple $(V, V_1, ..., V_n)$, where V is a finite vector space; $V_1, ..., V_n$ are subspaces of V, and such that*

$$h(I) = \log\left(\left|\frac{V}{\bigcap\limits_{i\in I} V_i}\right|\right) \text{, for all } I \in (\wp([n]) \setminus \{\emptyset\})$$

Although linear polymatroids are mentioned few times in the literature, they are essentially the same as the well known linear rank functions.

Definition 14 (Linear rank function) *A linear rank function of order n is a function $r : (\wp([n]) \setminus \{\emptyset\}) \to \mathbb{R}^+$, which is determined by a tuple $(V, V_1, ..., V_n)$, where V is a finite*

vector space, $V_1, ..., V_n$ *are subspaces of* V*, and for which it happens that:*

$$r(I) = \dim\left(\left\langle \bigcup_{i\in I} V_i \right\rangle\right), \text{ for all } I \in (\wp([n]) \setminus \{\emptyset\})$$

In Chapter 3 we prove that the definitions of linear rank functions and linear polymatroids are essentially equivalent.

Notation 1 *From now on, and for the ease of notation, we write* $h(i)$ *instead of* $h(\{i\})$*, whenever* h *is a polymatroid and* i *is an element of its domain.*

Matúš theorem [25] implies that there exist polymatroids which are not almost entropic. However, it is easy to prove that any linear polymatroid is entropic.

Proposition 15 *All the linear polymatroids are entropic.*

Proof. Let h be a linear polymatroid of order n, and suppose that $\mathcal{V} = (V, V_1, ..., V_n)$ is a subspace arrangement, such that, for all $I \subseteq [n]$, $I \neq \emptyset$, the equality

$$h(I) = \log\left|\frac{V}{\bigcap_{i\in I} V_i}\right|$$

holds. Now, suppose that X is a random variable that is uniformly distributed over V. Given $I \subseteq [n]$, $I \neq \emptyset$, we use the symbol X_I to denote the random variable that is induced by X over the quotient $\frac{V}{\bigcap_{i\in I} V_i}$. Variable X_I is defined in the following way:

$$\text{If } X = a, \text{ then } X_I = [a]_I$$

where $[a]_I$ is the equivalence class of a in the quotient $\frac{V}{\bigcap_{i\in I} V_i}$. Let $X = (X_1, ..., X_n)$. Notice that for all $I \subseteq [n]$, $I \neq \emptyset$, the equalities

$$h_X(I) = H(X_I) = \log \left| \frac{V}{\bigcap_{i\in I} V_i} \right| = h(I)$$

hold. Then, we have that h is equal to h_X, which is an entropic polymatroid. ■

Definition 16 (Linear random variables) *Let $(V, V_1, ..., V_n)$ be a tuple such that V is a finite vector space and such that $V_1, ..., V_n$ are subspaces of V. Let X be a random variable that is uniformly distributed over V, and let $(X_1, ..., X_n)$ be the tuple of random variables that are induced by X over the quotients $\frac{V}{V_1}, \frac{V}{V_2}, ..., \frac{V}{V_n}$. We say that the tuple $(X_1, ..., X_n)$ is a tuple of linear random variables, and any tuple of random variables having such a representation is said to be a tuple of linear random variables.*

Definition 17 *Given h a polymatroid of order n, we say that h is weakly linear, if and only if, h is a scalar multiple of a linear polymatroid. We say that h is cc-linear, if and only if, it is a positive linear combination of linear polymatroids. We say that h is almost linear, if and only if, h belongs to the topological closure of the set of cc-linear polymatroids.*

From now on, we will use the symbol L_n to denote the set of all the linear polymatroids of order n and we use the symbol $\mathcal{L}_n$ to denote the topological closure of the set $cc(L_n)$, which is constituted by the almost linear polymatroids.. The set $\mathcal{L}_n$ is known as the *linear region of order n*. It is worth to remark that $\mathcal{L}_n$ is a closed convex cone. Moreover, we have that:

Claim 18 *For all $n \geq 1$, the containment $\mathcal{L}_n \subseteq \overline{\Gamma_n^*}$ holds.*

2.4 Matroids

Matroids are combinatorial structures [29], which were introduced to capture the abstract notion of independence, and which have found their way into cryptology [24], coding theory and information theory[14].

Definition 19 (Matroid) *Given $n \geq 1$, a matroid of order n is a set $M \subseteq \wp([n])$, such that:*

1. $\emptyset \in M$.
2. *Given $A \subseteq B \subseteq [n]$, if $B \in M$ then $A \in M$.*
3. *Given $A, B \in M$, if $|A| < |B|$ there exists $b \in B$, such that, $A \cup \{b\} \in M$.*

Given a matroid M of order n, the elements of M are the *independent subsets of* $[n]$. Moreover, the matroid M encodes a notion of dimension, which is given by its *rank function*, that we denote with the symbol rk_M, and which is defined as follows.

Definition 20 (Rank function) *Let M be a matroid of order n and let $I \subseteq [n]$*

$$rk_M(I) = \max\{|J| : J \in M \text{ and } J \subseteq I\}$$

The rank function of M characterizes the matroid, notice that

$$M = \{I \subseteq [n] : rk_M(I) = |I|\}$$

Notice also that rk_M is a polymatroid of order n.

2.4.1 Representability of matroids

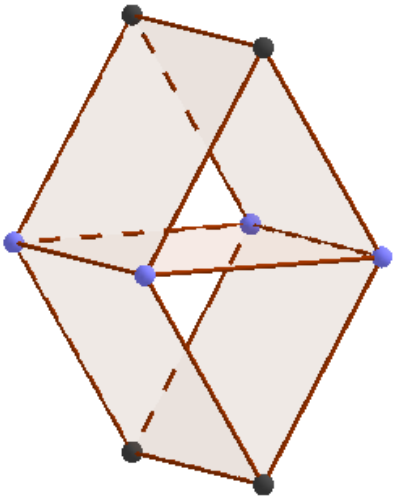
Natural examples of matroids can be defined using the notion of linear independence. We say that M is a representable or linear matroid, if and only if, there exists a subspace arrangement $(V, V_1, ..., V_n)$ such that:

1. For all $i \leq n$, we have that $\dim(V_i) = 1$.
2. Given $I \subseteq [n]$, we have that $rk_M(I) = \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right)$.
3. $V = \left\langle \bigcup_{i \in [n]} V_i \right\rangle$.

Let M be a matroid of order n. It is known (see [29]) that M is linear, if and only if, there exist a subspace arrangement $(V, V_1, ..., V_n)$ such that, V is a finite vector space and for all $I \subseteq [n]$, the equality $rk_M(I) = \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right)$ holds. Therefore, we will focus our attention on subspace arrangements defined over finite vector spaces. Notice that M is representable, if and only if, rk_M is a linear rank function. Notice that M is weakly linear, if and only if, rk_M is a linear rank function.

2.4.2 Non-linear matroids: The Vamos Matroid

It is natural to ask whether the abstract notion of dimension, as encoded by the concept of matroid, is equivalent to the notion of linear dimension. That is, it is natural to ask if any matroid has a linear representation. Linear representability of matroids is one of the most studied topics in Matroid Theory, and we know many things about that. We know, for instance, that the famous Vamos Matroid (defined below) cannot be linearly represented (for a proof see [29]).



Definition 21 (Vamos Matroid) *The Vamos matroid can be easily defined by means of the below graphic.*

The ground set of this matroid is a set of size 8*, which can be represented by the nodes of the graphic. The independent sets are all the sets with three or fewer elements plus all the subsets of size four that are not included on the same face.*

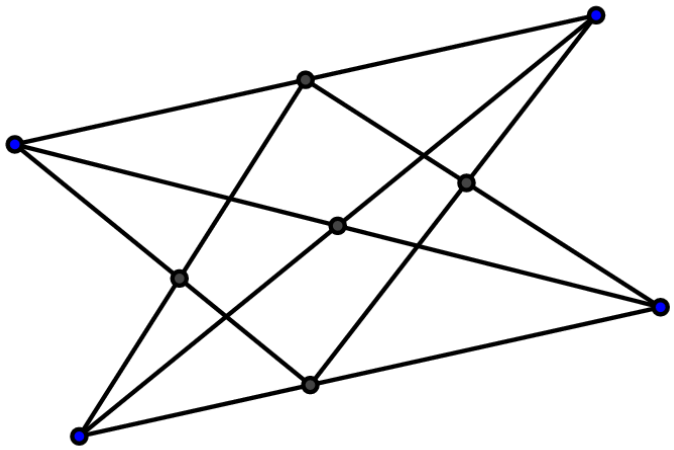
2.4.3 Weakly linear matroids: The non-Pappus Matroid

Let M be a linear matroid and let $\mathcal{V} = (V, V_1, ..., V_n)$ be a linear representation of M. Suppose that the ground field of V is the finite field $\mathbb{F}$. Notice that $\frac{1}{\log(|\mathbb{F}|)} rk_M$ is a linear polymatroid. Thus, if a given matroid M is linear, we have that a scalar multiple of its rank function is a linear polymatroid. It is natural to ask if the converse holds true. We show that it is not the case.

Definition 22 *Let M be a matroid, we say that M is weakly linear, if and only if, there exist $\lambda > 0$ such that, $\lambda \cdot rk_M$ is a linear rank function.*

Is any weakly linear matroid a linear one? It can be proved that it is not the case. One important example is the famous non-Pappus Matroid (defined below).

Definition 23 (Non-Pappus Matroid) *The non-Pappus matroid can be easily defined by means of the below graphic.*



The ground set of this matroid is a set of size 9*, which can be represented by the nodes of the graphic. The independent sets are all the sets with two or fewer elements, plus all the subsets of size three that are not included on the same line.*

It can be proved that the non-Pappus matroid is non-linear, for a proof see [29]. The following matrix of order 6×18, gives us a weakly linear representation of this matroid over the field $(\mathbb{F}_3)^2$, see [32].

$$\begin{bmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}$$

Part II

Studies on the common information method

Chapter 3

Linear polymatroids

In this chapter we will review, in more depth than in the previous chapter, the theory of linear polymatroids together with the theory of linear rank inequalities. Let us begin recalling the definitions of linear polymatroid and linear rank function.

Definition 24 (Linear polymatroid) *A linear polymatroid of order n is a polymatroid $h : (\wp([n]) \setminus \{\emptyset\}) \to \mathbb{R}^+$, for which there exist a tuple $(V, V_1, ..., V_n)$, where V is a finite vector space and $V_1, ..., V_n$ are subspaces of V, and such that*

$$h(I) = \log\left(\left|\frac{V}{\bigcap\limits_{i\in I} V_i}\right|\right), \text{ for all } I \in (\wp([n]) \setminus \{\emptyset\})$$

Now, the well known linear rank functions.

Definition 25 (Linear rank function) *A linear rank function of order n is a function $r : (\wp([n]) \setminus \{\emptyset\}) \to \mathbb{R}^+$, which is determined by a tuple $(V, V_1, ..., V_n)$, where V is a finite vector space and $V_1, ..., V_n$ are subspaces of V, and for which it happens that:*

$$r(I) = \dim\left(\left\langle \bigcup_{i\in I} V_i \right\rangle\right), \text{ for all } I \in (\wp([n]) \setminus \{\emptyset\})$$

Given W, a subspace of V, we set

$$W^{\perp} = \{v \in V : (\forall w \in W)\,(\langle v, w\rangle = 0)\}$$

where given $v = (v_1, ..., v_k)$ and $w = (w_1, ..., w_k)$, the *scalar product* $\langle v, w\rangle$ is defined as

$$v_1 w_1 + v_2 w_2 + ... + v_k w_k$$

with the arithmetical operations computed on $\mathbb{F}$. By an abuse of language, we will use the term *orthogonal complement of* W to denote the subspace $W^{\perp}$. Next proposition partially justifies the use of this term.

Proposition 26 *Let V be a finite vector space. Given W a subspace of V, we have that* $\dim(V) = \dim\left(W^{\perp}\right) + \dim(W)$.

Proof. Let $w_1, ..., w_k$ be a basis of W and let $T : V \to V$ be the linear map defined by

$$T(v) = \left(\langle v, w_1\rangle, ..., \langle v, w_k\rangle\right)^{\top}$$

It is easy to check that $\ker(T) = W^{\perp}$. On the other hand, we notice that $T(v)$ is given by right-multiplying v by the matrix $\begin{pmatrix} w_1 & \cdots & w_k \end{pmatrix}$. By definition, this matrix has column span of dimension k. The Rank Nullity Theorem, which holds true for any vector space, asserts that

$$\dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T))$$

then

$$\begin{aligned} \dim(V) &= \dim\left(W^{\perp}\right) + k \\ &= \dim\left(W^{\perp}\right) + \dim(W) \end{aligned}$$

■

Proposition 27 *For all W, subspace of V, we have that, $\left(W^{\perp}\right)^{\perp} = W$.*

Proof. Let $w \in W$. We have that, for all $u \in W^{\perp}$, the equality $\langle w, u\rangle = 0$ holds. Then, we have that $w \in \left(W^{\perp}\right)^{\perp}$. Thus, we have that $W \subseteq \left(W^{\perp}\right)^{\perp}$. On the other hand, the above proposition implies that $\dim(W) = \dim\left(\left(W^{\perp}\right)^{\perp}\right)$. Those two facts imply that $W = \left(W^{\perp}\right)^{\perp}$. ■

Proposition 28 *Let V be a finite vector space, and let $\{V_i : i \in I\}$ be a family of subspaces of V, we have that*

$$\dim\left(\frac{V}{\bigcap_{i\in I} V_i}\right) = \dim\left(\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle\right)$$

Proof. We have from definition that

$$\dim\left(\frac{V}{\bigcap_{i\in I} V_i}\right) = \dim(V) - \dim\left(\bigcap_{i\in I} V_i\right)$$

then,

$$\dim\left(\frac{V}{\bigcap_{i\in I} V_i}\right) = \dim\left(\left(\bigcap_{i\in I} V_i\right)^{\perp}\right)$$

then, it is sufficient to prove that $\left(\bigcap_{i\in I} V_i\right)^{\perp}$ is equal to $\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle$. To this end, we prove that

$$\bigcap_{i\in I} V_i = \left(\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle\right)^{\perp}$$

First, we suppose that $v \in \bigcap_{i\in I} V_i$. Given $w \in \left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle$, the vector w can be expressed as $\sum_{i\in I} \alpha_i v_i$, where, for all $i \in I$, we have that $v_i \in (V_i)^{\perp}$ and α_i is a scalar. Notice that

$$\langle v, w\rangle = \sum_{i\in I} \alpha_i \langle v, v_i\rangle = 0$$

Then, $v \in \left(\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle\right)^{\perp}$ and $\bigcap_{i\in I} V_i \subseteq \left(\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle\right)^{\perp}$.

Now, we suppose that $v \in \left(\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle\right)^{\perp}$. Given $i \in I$, and given $w \in (V_i)^{\perp}$ we have that, $\langle v, w\rangle = 0$. It means that, for all $i \in I$, the vector v belongs to $\left((V_i)^{\perp}\right)^{\perp}$. Thus, we have that $v \in \left(\bigcap_{i\in I} \left((V_i)^{\perp}\right)^{\perp}\right) = \bigcap_{i\in I} V_i$ and $\left(\left\langle \bigcup_{i\in I} (V_i)^{\perp} \right\rangle\right)^{\perp} \subseteq \bigcap_{i\in I} V_i$. ■

Now, we are ready to prove that linear rank functions and linear polymatroids are one and the same thing.

Proposition 29 *For all linear polymatroid h there exists a linear rank function r and there exists $c > 0$, such that, $h = cr$. On the other hand, for all linear rank function r there exist a linear polymatroid h and a constant $d > 0$ such that $r = dh$.*

Proof. Let h be a linear polymatroid determined by a tuple $(V, V_1, ..., V_n)$, where V is a vector space over a finite field $\mathbb{F}$. Given I, a non empty subset of $[n]$, we have that

$$\begin{aligned} h(I) &= \log\left(\left|\frac{V}{\bigcap_{i\in I} V_i}\right|\right) = \frac{1}{\log_{|\mathbb{F}|}(2)} \log_{|\mathbb{F}|}\left(\left|\frac{V}{\bigcap_{i\in I} V_i}\right|\right) \\ &= \frac{1}{\log_{|\mathbb{F}|}(2)} \dim\left(\frac{V}{\bigcap_{i\in I} V_i}\right) = \frac{1}{\log_{|\mathbb{F}|}(2)} \dim\left(\left\langle \bigcup_{i\in I} V_i^{\perp} \right\rangle\right) \end{aligned}$$

where $V_i^{\perp}$ denotes the orthogonal complement of V_i. Let $c = \frac{1}{\log_{|\mathbb{F}|}(2)}$, let $R = \left(V, V_1^{\perp}, ..., V_n^{\perp}\right)$ and let r be equal to the linear rank function determined by the tuple R. Then we have

that $h = cr$. The proof of the other claim is similar. ■

3.1 Linear rank inequalities

Recall that we use the symbol $\mathcal{L}_n$ to denote the set $\overline{cc\,(L_n)}$, which is the closed convex cone constituted by all the limits of sequences of *cc*-linear polymatroids of order n, and recall that the set $\mathcal{L}_n$ is called the *linear region* of order n.

Definition 30 (Linear rank inequalities) *A linear rank inequality of order n is a vector $v \in \mathbb{R}^{2^n-1}$, such that, for $h \in \mathcal{L}_n$, it happens that the inequality $\langle h, v\rangle \geq 0$ holds.*

Thus, linear rank inequalities are dual to linear polymatroids. Fix $n \geq 1$, linear rank inequalities on n variables, are dual to linear polymatroids of order n. Therefore, all those inequalities are elements of $\mathbb{R}^{2^n-1}$, and any one of those inequalities can be expressed as a linear combination $\sum_{I \in (\wp([n]) \setminus \{\emptyset\})} a_I e_I$.

We know that, given $A \subseteq \mathbb{R}^n$, its polar is a closed convex cone. Notice that the closed convex cone of linear rank inequalities of order n is the polar of the set of linear polymatroids of order n. We use the symbol $(\mathcal{L}_n)^\circ$ to denote this cone. Then, given n, the set of all linear rank inequalities of order n is a convex cone.

If $A \subseteq \mathbb{R}^n$ is a closed convex cone, then the equality $A = (A^\circ)^\circ$ holds. It implies that given $A, B \subseteq \mathbb{R}^n$, two closed convex cones, we have that $A = B$, if and only if, $A^\circ = B^\circ$.

Now, it is natural to ask: Which is the polar cone of $(\mathcal{L}_n)^\circ$?

3.2 The linear regions

Proposition 31 *The polar of* $(\mathcal{L}_n)^\circ$ *is equal to* $\mathcal{L}_n$.

Proof. Let $h \in \mathcal{L}_n$, there exists a sequence $\{h_j\}_{j\geq 1}$ such that $h_j \to h$ and for all j, we have that h_j is a positive linear combination of linear polymatroids. Let $v \in \mathcal{L}_n^\circ$ and suppose that $h_j = \sum_{i=1}^{k_j} c_i^j f_i^j$, where for all $i = 1, ..., k_j$, we have that $c_i^j \in \mathbb{R}^+$ and f_i^j is a linear polymatroid, then

$$\langle h_j, v\rangle = \left\langle \left(\sum_{i=1}^{k_j} c_i^j f_i^j \right), v \right\rangle = \sum_{i=1}^{k_j} c_i^j \left\langle f_i^j, v \right\rangle \geq 0$$

and

$$\langle h, v\rangle = \left\langle \left(\lim_{j\to\infty} h_j \right), v \right\rangle = \lim_{j\to\infty} \left(\langle h_j, v\rangle \right) \geq 0$$

Thus, we have that h belongs to the polar of $\mathcal{L}_n^\circ$, and then $\mathcal{L}_n$ is contained in the polar of $\mathcal{L}_n^\circ$.

On the other hand, we know that the subset of $\mathbb{R}^{2^n-1}$ constituted by all the vectors that satisfy the linear inequalities contained in $\mathcal{L}_n^\circ$, is equal to the conic closure of the set of linear polymatroids of order n. The later set is equal to $\mathcal{L}_n$, given that $\mathcal{L}_n$ is the conic closure of those linear polymatroids. Then, we have that the polar of $\mathcal{L}_n^\circ$ is contained in $\mathcal{L}_n$ and then the proposition is proved. ■

The low dimensional linear regions are well understood. It is easy to prove that for all $n \leq 3$, the equality $\mathcal{L}_n = \Gamma_n$ holds [17]. The case $n = 4$ is different.

3.2.1 Four variables and the Ingleton Inequality

We will see, at the end of this section, that $\mathcal{L}_4 \neq \overline{\Gamma_4^*}$. To this end, we will exhibit a linear rank inequality, which does not hold for all the entropic polymatroids. This inequality is the famous Ingleton inequality, [19]. First, some definitions.

Definition 32 *Given random variables $X_1, ..., X_n$ and given two sets $I, J \subseteq [n]$, a common information for X_I and X_J is a random variable Y such that:*

- $H(Y \mid X_I) = H(Y \mid X_J) = 0$ *and*
- $H(Y) = I(X_I; X_J) = H(X_I) + H(X_J) - H(X_I, X_J)$.

Theorem 33 *Let $(X, X_1, ..., X_n)$ be a tuple of linear random variables, and let $I, J \subseteq [n]$. The two variables X_I and X_J have a common information.*

Proof. Suppose that $(X, X_1, ..., X_n)$ is determined by the subspace arrangement $(V, V_1, ..., V_n)$. Set $W = \langle V_I \cup V_J \rangle$, and let Y be equal to the random variable that is induced by X over the quotient $\frac{V}{W}$. It is easy to check that Y is the common information of X_I and X_J.

First, notice that $V_I, V_J \subseteq W$. It implies that given a equivalence class in $\frac{V}{V_I}$ $\left(\text{or } \frac{V}{V_J}\right)$, it is contained in a equivalence class of W. Thus, if one knows the value of X_I (or X_J), he knows to which equivalence class of $\frac{V}{W}$ belongs the vector $v \in V$ such that $X = v$.

Therefore we have that

$$H(Y \mid X_I) = H(Y \mid X_J) = 0$$

We check the second condition, that is, we check that the equality

$$H(Y) = H(X_I) + H(X_J) - H(X_I, X_J)$$

holds.

We notice that

$$H(Y) = \log\left(\frac{|V|}{|\langle V_I \cup V_J \rangle|}\right)$$

Claim 34 *Given $I, J \subseteq [n]$, the equality $H(X_I, X_J) = \log\left(\frac{|V|}{|V_I \cap V_J|}\right)$ holds.*

Proof of the claim:

We suppose that $I = \{i\}$ and $J = \{j\}$, the proof of the general case is similar. We have that $H(X_i) = \log\left(\left|\frac{V}{V_i}\right|\right)$ and $H(X_j) = \log\left(\left|\frac{V}{V_j}\right|\right)$. Recall that X_i and X_j corresponds to the variables that are induced by X over the quotient $\frac{V}{V_i}$ and $\frac{V}{V_j}$ (respectively).

Suppose that $X = v$, knowing the join variable (X_i, X_j) corresponds to know the equivalent classes $[v]_i \in \frac{V}{V_i}$ and $[v]_j \in \frac{V}{V_j}$, and hence $H(X_i, X_j)$ corresponds to the minimal amount of information that is necessary to determine the classes $[v]_i$ and $[v]_j$. Now, we notice that determining the classes $[v]_i$ and $[v]_j$ is the same as determining the class $[v]_{ij} \in \frac{V}{V_i \cap V_j}$.

Therefore, the entropy of (X_i, X_j) is equal to the entropy of a random variable that is uniformly distributed over $\frac{V}{V_i \cap V_j}$ and hence

$$H(X_i, X_j) = \log\left(\frac{|V|}{|V_i \cap V_j|}\right)$$

Now, that we have proven the claim, we can continue with the proof of the theorem. It is enough to check that the equality

$$\log\left(\frac{|V|}{|\langle V_I \cup V_J\rangle|}\right) = \log\left(\frac{|V|}{|V_I|}\right) + \log\left(\frac{|V|}{|V_J|}\right) - \log\left(\frac{|V|}{|V_I \cap V_J|}\right)$$

holds. Notice that

$$\begin{aligned}
& \log\left(\frac{|V|}{|V_I|}\right) + \log\left(\frac{|V|}{|V_J|}\right) - \log\left(\frac{|V|}{|V_I \cap V_J|}\right) \\
= \; & \log\left(\frac{|V|^2}{|V_I|\,|V_J|}\frac{|V_I \cap V_J|}{|V|}\right) \\
= \; & \log\left(\frac{|V|}{\frac{|V_I||V_J|}{|V_I \cap V_J|}}\right) \\
= \; & \log\left(\frac{|V|}{|\langle V_I \cup V_J\rangle|}\right)
\end{aligned}$$

The last equality holds, given that

$$|\langle V_I \cup V_J \rangle| = \frac{|V_I|\,|V_J|}{|V_I \cap V_J|} \tag{3.1}$$

To finish with the proof, we check the soundness of the equation 3.1. Let $f : V_I \times V_J \rightarrow \langle V_I \cup V_J \rangle$ be the function

$$f(v, w) = v + w$$

Function f is a surjective homomorphism from the abelian group $(V_I \times V_J, +)$ onto the abelian group $(\langle V_I \cup V_J \rangle, +)$. Thus, we have that

$$|V_I|\,|V_J| = |V_I \times V_J| = |\langle V_I \cup V_J \rangle|\,|Ker(f)|$$

Notice that $Ker(f) = \{(v, -v) : v \in V_I \cap V_J\}$, and hence

$$|Ker(f)| = |V_I \cap V_J|$$

■

Definition 35 (Ingleton Inequality) *The Ingleton inequality is the linear inequality given by the linear expression*

$$\mathcal{I} = -\left(e_1 + e_2 + e_{\{1,2,3\}} + e_{\{1,2,4\}} + e_{\{3,4\}}\right) + e_{\{1,3\}} + e_{\{1,4\}} + e_{\{2,3\}} + e_{\{2,4\}} + e_{\{1,2\}}$$

Theorem 36 *Ingleton inequality is a linear rank inequality.*

Proof. Let α be equal to the linear expression

$$-\left(e_{\{1,2,3\}} + e_{\{1,2,4\}} + e_{\{3,4\}} + 2e_1 + 2e_2 + e_5\right) + e_{\{1,3\}} + e_{\{1,4\}} + e_{\{2,3\}} + e_{\{2,4\}} + 2e_{\{1,5\}} + 2e_{\{2,5\}}$$

It can be checked that α encodes a polymatroidal inequality, which holds for all the entropic polymatroids of order 5. Let $\mathcal{V} = (V, V_1, .., V_4)$ be a subspace arrangement and let $(X, X_1, ..., X_4)$ be the associated tuple of linear random variables. Notice that, given $I \subseteq [4]$, the equality $h_{\mathcal{V}}(I) = H(X_I)$ holds. Now, we suppose that X_5 is a common information of X_1 and X_2. We have that

$$\begin{aligned} &-(H(X_{1,2,3}) + H(X_{1,2,4}) + H(X_{3,4}) + 2H(X_1) + 2H(X_2) + H(X_5)) \\ &+H(X_{1,3}) + H(X_{1,4}) + H(X_{2,3}) + H(X_{2,4}) + 2H(X_{1,5}) + 2H(X_{2,5}) \quad \geq \quad 0 \end{aligned}$$

Given that X_5 is the common information of X_1 and X_2, we get

$$\begin{aligned} \langle h_{\mathcal{V}}, \mathcal{I} \rangle = &-(H(X_1) + H(X_2) + H(X_{1,2,3}) + H(X_{1,2,4}) + H(X_{3,4})) + \\ &H(X_{1,3}) + H(X_{1,4}) + H(X_{2,3}) + H(X_{2,4}) + H(X_{1,2}) \quad \geq \quad 0 \end{aligned}$$

and then the theorem is proved. ■

The above proof entails a method for the generation of linear rank inequalities. This method is called *The common information method* (CI-method, for short). We will study in depth the CI-method along this dissertation, but first it is important to remark that the Ingleton inequality is not an information inequality, see [17], it means that there exists a tuple of random variables, say $X = (X_1, ..., X_4)$, such that, $\langle h_X, \mathcal{I} \rangle < 0$.

3.3 The CI-method

Let h be a linear polymatroid, let $(V, V_1, ..., V_n)$ be a subspace arrangement representing h, and let $(X, X_1, ..., X_n)$ be the tuple of linear random variables determined by it. Recall that, given $I, J \subseteq [n]$, the random variables X_I and X_J have a common information. This fact is the basis of the method, which is a kind of projection method that has been used as a heuristic, but which can be completely automatized (see below).

Given $n \geq 1$ and $L, K \subseteq [n]$, we define a set $\Delta_{L,K}^{n+1}$ of linear rank inequalities on $n+1$ variables, such that, if $v = \sum_{I \subseteq [n+1]} a_I e_I$ is a linear rank inequality, we have that $v \in \Delta_{L,K}^{n+1}$, if and only if, the following condition is satisfied:

Given $R \subseteq [n+1]$, if $a_R \neq 0$ and $n+1 \in R$ then we have that either $L \subseteq R$, or $K \subseteq R$, or, $R = \{n+1\}$.

Given $v \in \Delta_{L,K}^{n+1}$, we define $T_{L,K}^{n+1}(v) = \sum_{I \subseteq [n]} a_I^* e_I$, where

$$a_I^* = \begin{cases} a_L + a_{L \cup \{n+1\}} + a_{n+1}, & \text{if } I = L \\ a_K + a_{K \cup \{n+1\}} + a_{n+1}, & \text{if } I = K \\ a_{L \cup K} + a_{L \cup K \cup \{n+1\}} - a_{n+1}, & \text{if } I = L \cup K \\ a_{I \cup \{n+1\}} + a_I, & \text{if } (K \subseteq I \text{ or } L \subseteq I) \text{ and } I \neq L, K, L \cup K \\ a_I, & \text{otherwise} \end{cases}$$

Notice that $T_{L,K}^{n+1}$ is a linear map. Those maps are the projections employed in the common information method. Next theorem asserts that if one picks a linear rank inequality on $n+1$ variables within the set $\Delta_{L,K}^{n+1}$, then he can apply $T_{L,K}^{n+1}$ to the chosen inequality to get a linear rank inequality on n variables. It is mathematical core of the method.

Theorem 37 *If $v \in \Delta_{L,K}^{n+1}$, then $T_{L,K}^{n+1}(v) \in (\mathcal{L}_n)^\circ$.*

Proof. Let $v \in \Delta_{L,K}^{n+1}$ and suppose that $T_{L,K}^{n+1}(v) \notin \mathcal{L}_n^\circ$, then there exists a tuple of linear random variables $X = (X_1, ..., X_n)$, such that h_X, the linear polymatroid determined by X, satisfies the inequality $\left\langle h_X, T_{L,K}^{n+1}(v) \right\rangle < 0$. Let $Y = (X_1, ..., X_n, X_{n+1})$ where X_{n+1} is the common information of X_L and X_K. We will prove that the equality

$$\langle v, h_Y \rangle = \left\langle h_X, T_{L,K}^{n+1}(v) \right\rangle \tag{3.2}$$

holds. Notice that we have arrived to a contradiction because v is, for definition, a linear rank function. It remains to be proved that the equality 3.2 actually holds. Suppose that

$$v = \left(\sum_{I \subseteq [n]} a_I e_I \right) + \left(\sum_{K \subseteq I \text{ or } L \subseteq I} a_{I \cup \{n+1\}} e_{I \cup \{n+1\}} \right) + (a_{n+1} e_{n+1})$$

we have

$$\begin{aligned}
\langle v, h_Y \rangle &= \sum_{I \subseteq [n]} a_I h(I) + \sum_{K \subseteq I \text{ or } L \subseteq I} a_{I \cup \{n+1\}} h(I \cup \{n+1\}) + a_{n+1} h(n+1) \\
&= \sum_{I \subseteq [n]} a_I h(I) + \sum_{K \subseteq I \text{ or } L \subseteq I} a_{I \cup \{n+1\}} h(I \cup \{n+1\}) + a_{n+1} h(n+1) \\
&= \sum_{I \subseteq [n]} a_I h(I) + \sum_{K \subseteq I \text{ or } L \subseteq I} \left(a_{I \cup \{n+1\}} \right) h(I) + a_{n+1} \left(h(K) + h(L) - h(L \cup K) \right) \\
&= \sum_{\substack{I \subseteq [n] \\ L, K \nsubseteq I}} a_I h(I) + \sum_{\substack{K \subseteq I \text{ or } L \subseteq I \\ I \neq L, K, L \cup K}} \left(a_{I \cup \{n+1\}} + a_I \right) h(I) + \\
&\quad \left(a_L + a_{L \cup \{n+1\}} + a_{\{n+1\}} \right) h(L) + \left(a_K + a_{K \cup \{n+1\}} + a_{\{n+1\}} \right) h(K) + \\
&\quad \left(a_{L \cup K} + a_{L \cup K \cup \{n+1\}} - a_{\{n+1\}} \right) h(L \cup K) + \\
&= \sum_{\substack{I \subseteq [n] \\ L, K \nsubseteq I}} a^*_I h(I) + \sum_{\substack{K \subseteq I \text{ or } L \subseteq I \\ I \neq L, K, L \cup K}} a^*_I h(I) + a^*_L h(L) + a^*_K h(K) + a^*_{L \cup K} h(L \cup K) \\
&= \left\langle h_X, T^{n+1}_{L,K}(v) \right\rangle
\end{aligned}$$

It implies that $\langle v, h \rangle < 0$, which is clearly a contradiction. ■

Example 38 (Ingleton inequality) *Let α be equal to*

$$-\left(e_{\{1,2,3\}} + e_{\{1,2,4\}} + + e_{\{3,4\}} + 2e_1 + 2e_2 + e_5 \right) + e_{\{1,3\}} + e_{\{1,4\}} + e_{\{2,3\}} + e_{\{2,4\}} + 2e_{\{1,5\}} + 2e_{\{2,5\}}$$

It can be checked that $\alpha \in \Delta^5_{\{1\},\{2\}}$ and that

$$T^5_{\{1\},\{2\}}(\alpha) = -\left(e_1 + e_2 + e_{\{1,2,3\}} + e_{\{1,2,4\}} + e_{\{3,4\}} \right) + e_{\{1,3\}} + e_{\{1,4\}} + e_{\{2,3\}} + e_{\{2,4\}} + e_{\{1,2\}}$$

According to theorem 37, the vector $T^5_{\{1\},\{2\}}(\alpha)$ is a linear rank inequality. Notice that it is the aforementioned Ingleton inequality [19], which was the first ever discovered non-Shannon inequality that holds for all linear polymatroids.

One can use the method employed above, in the derivation of Ingleton's inequality, as a general method for the searching of new linear rank inequalities. It is the common information method, which we will proceed to define in the next few paragraphs. First some definitions

Given $n, k \geq 1$ and $L, K \subseteq [n + (k-1)]$, we use the symbol $\Omega^{n+k}_{L,K}$ to denote the subset of $\mathbb{R}^{2^{n+k}-1}$ determined by the condition:

$$\text{If } L, K \nsubseteq I,\ I \neq \{n+1\} \text{ and } n+1 \in I, \text{ then } \left\langle x, e_{I \cup \{n+k\}} \right\rangle = 0.$$

Remark 39 *Given Δ_{n+k} a polyhedral cone contained in $\mathbb{R}^{2^{n+k}-1}$, we have that $\Delta_{n+k} \cap \Omega^{n+k}_{L,K}$ is a polyhedral cone contained in $(\mathcal{L}_{n+k})^\circ$.*

Algorithm 40 (The CI Algorithm) *We define the CI algorithm in the following way:*

Input: *(n, k, Δ), where $n, k \geq 1$ and Δ is a polyhedral cone included in $(\mathcal{L}_{n+k})^\circ$, (we suppose that the cone Δ is presented as the finite list of its extremal rays).*

1. *Set $X = \Delta$.*
2. *For $i = k-1$ to 0 do:*
   - *2.1 For all $I, J \subseteq [n+i]$, compute the set $X_{I,J}$ which is equal to the set of extremal rays of $X \cap \Omega^{n+i+1}_{I,J}$.*
     - *2.1.1 Compute $T^{n+i+1}_{I,J}(X_{I,J})$.*

2.2 Compute $Z_i = \bigcup_{I,J \subseteq [n+i]} T_{I,J}^{n+i+1}(X_{I,J})$.

2.3 Compute W_i*, which is equal to the set of extremal rays of the convex cone determined by the finite set* Z_i.

2.4 Set $X = W_i$.

The above algorithm is a *galactic* one, which cannot be effectively used on most inputs because of its prohibitive running time and work space requirements. Dougherty, Freiling and Zeger [13] used it on input $(5, 2, \Gamma_7)$, obtaining in this way a set of linear rank inequalities that generate the cone $(\mathcal{L}_5)^\circ$. Dougherty [12] ran the same algorithm, on input $(6, 2, \Gamma_8)$, and he reported on the discovering of more than one billion of new linear rank inequalities, which are pairwise independent and which do not constitute a generating set for $(\mathcal{L}_6)^\circ$. It is important to stress that such a generating set for $(\mathcal{L}_6)^\circ$ is not known.

Definition 41 *Given* $n, k \geq 1$*, we use the symbol* $CI[n,k]$ *to denote the output of algorithm CI on input* (n, k, Γ_n)*. Given* $k \geq 1$*, we use the symbol* $CI[n]$ *to denote the set* $\bigcup_{k \geq 1} CI[n,k]$*. Finally, we use the symbol* ***CI*** *to denote the set* $\bigcup_{n \geq 1} \left(\bigcup_{k \geq 1} CI[n,k] \right)$.

3.4 The DFZ questions

Are the linear regions polyhedral? Perhaps, we could address this question, if we would have an algorithmic method for the recognition and generation of all the linear rank inequalities. It is unknown if such a method actually exists. It could be argued that the CI-method is the most powerful method for the generation of linear rank inequalities that has been designed up to the date, but it is unknown if such method is complete (i.e. it is unknown if the CI-method can be used to generate all the linear rank inequalities).

$\mathcal{L}_4$ is a polyhedral cone determined by the Shannon inequalitites plus the six Ingleton inequalitites, [17] (there are six independent Ingleton inequalities, which can be obtained from the Ingleton inequality discussed above by permuting the variables). Dougherty et al [13] have used the *common information method* for the searching of new linear rank inequalities. They have used the method for investigating the structure of the linear regions of order five. They were able of determining a complete set of linear rank inequalities for $\mathcal{L}_5$, which is constituted by several thousands of those inequalitites. Dougherty, [12], have used the CI-method for studying the linear region of order six. He reported on the existence of more than a billion of independent linear rank inequalitites over six variables.

Dougherty et al, [13] asked the following two questions:

- Are the linear regions polyhedral?
- Is the CI-method a complete method?

Those two questions can be considered the most important open problems related to the structure of the linear regions. From now on, we will focus on the second question, that is, we will investigate the completeness of the CI-method. We think that a first important step is to clarify its scope. To this end, we can use the definitions introduced above.

QUESTION: Given $n \geq 1$, does $CI[n]$ generate the set $(\mathcal{L}_n)^\circ$?

The above question is the research problem that we will study in the remaining of this dissertation.

Chapter 4

Secret Sharing

Suppose that we have a secret, and we want to break this secret into n shares, in such a way that it can be reconstructed from those shares. To make things become more interesting, we can suppose that there exists a predetermined family of large subsets of $[n]$, the *qualified subsets,* such that the secret can be reconstructed only from the set of shares belonging to a given subset within the family. We will use the term *access structure* to denote the family of qualified sets.

Definition 42 (Access structure) *An access structure is a pair $(n, \mathcal{C})$, such that $\mathcal{C}$ is a filter over $[n]$, i.e. $\mathcal{C}$ is a non empty family of subsets of $[n]$ that is upward closed.*

Now, suppose that an access structure $(n, \mathcal{C})$ has been fixed, and suppose that we want to privately communicate our shares to n parties. We suppose that there is an eavesdropper who wants to know the secret. If the eavesdropper has the possibility of infiltrating the small sets of parties (the unqualified sets that do not belong to the access structure $(n, \mathcal{C})$), then we must choose the shares in such a way that no information about the secret can be obtained from the shares that were communicated to the small sets of parties. How can we choose (compute) the n shares of our secret? It is *The Secret Sharing Problem* see [11] and [23].

Given $n \geq 1$ and an access structure $(n, \mathcal{C})$, it determines an instance of the secret sharing problem. The solutions to this instance will be called *secret sharing schemes* for $(n, \mathcal{C})$. First some definitions.

Definition 43 (Distribution scheme) *Given $n \geq 1$, a distribution scheme for n parties, is a tuple $\Sigma = (S \times W, f_1, ..., f_n)$, where S and W are finite sets and $f_1, ..., f_n$ are mappings from $S \times W$ to $S \times W$.*

Given a distribution scheme $\Sigma = (S \times W, f_1, ..., f_n)$, it can be used to break secrets belonging to S. Given $s \in S$, one chooses $w \in W$ and then he computes $f_1(s, w), f_2(s, w), ..., f_n(s, w)$. Those are the shares of s that are computed using Σ and the random string w. Is it a safe way of sharing our secret? Given the access structure $(n, \mathcal{C})$ and given $I \in \mathcal{C}$, we must be able of reconstructing the secret s from the set of shares $\{f_i(s, w) : i \in I\}$. It means that this set of shares must determine the string s, and it means that, given $(s', w') \in S \times W$, if for all $i \in I$ the equality $f_i(s, w) = f_i(s', w')$ holds, then $(s, w) = (s', w')$. On the other hand, given $J \notin \mathcal{C}$, no information about s can be computed from the set $\{f_j(s, w) : j \in J\}$. It means that for all $s' \in S$, it happens that the equality

$$|\{u \in W : (\forall j \in J)(f_j(s, u) = f_j(s, w))\}| = |\{w' \in W : (\forall j \in J)(f_j(s', w') = f_j(s, w))\}|$$

holds. The above conditions on $\Sigma = (S \times W, f_1, ..., f_n)$ can be captured using Shannon entropy. Given $i \leq n$, we use the symbol R_i to denote the equivalence relation

$$(s, w) R_i (s', w'), \text{ if and only if, } f_i(s, w) = f_i(s', w')$$

and we use the symbol $\frac{S \times W}{R_i}$ to denote the quotient of $S \times W$ determined by R_i. Given X_Σ, a random variable uniformly distributed over $S \times W$, we use the symbol X_Σ^i to denote

the random variable that is distributed over $\frac{S \times W}{R_i}$, and that is defined in the following way

$$X_{\Sigma}^{i} = [f_i(v)]_{R_i}, \text{ if and only if, } X_{\Sigma} = v$$

and we use the symbol X_{Σ}^{n+1} to denote to the random variable

$$X_{\Sigma}^{n+1} = s, \text{ if and only if, } \pi_S(X_{\Sigma}) = s$$

Notation 2 *Given $I \subseteq [n+1]$, we use the symbol X_{Σ}^{I} to denote the join random variable $\{X_{\Sigma}^{i} : i \in I\}$.*

Definition 44 (Secret sharing scheme) *Let $(n, \mathcal{C})$ be an access structure and let Σ be a distribution scheme for n parties, we say that Σ is a secret sharing scheme for $(n, \mathcal{C})$, if and only if, the following conditions are satisfied:*

1. *CORRECTNESS: $H\left(X_{\Sigma}^{n+1} \mid X_{\Sigma}^{I}\right) = 0$, for all $I \in \mathcal{C}$.*
2. *PRIVACY: $H\left(X_{\Sigma}^{n+1} \mid X_{\Sigma}^{J}\right) = H\left(X_{\Sigma}^{n+1}\right)$, for all $J \notin \mathcal{C}$.*

4.0.1 An important example: Shamir Scheme

Let us introduce an important example of a secret sharing scheme, it is the famous Shamir scheme (see [31]).

Let $n > k$, we use the symbol $(n, T_{n,k})$ to denote the threshold access structure given by

$$T_{n,k} = \{I \subseteq [n] : |I| \geq k\}$$

The Shamir' scheme for (n, k), which is denoted with the symbol $S_{n,k}$, is a secret sharing scheme that solves the secret sharing problem for $(n, T_{n,k})$, and that is defined

in the following way. Suppose that s is the secret whose shares must be communicated to n parties. We can suppose that s is a non-null element of $\mathbb{F}$, where $\mathbb{F}$ is a finite field whose size is larger than n. We fix in advance $a_1, ..., a_n \in \mathbb{F} \setminus \{0\}$, which are pairwise different. We use the symbol $\overrightarrow{a}$ to denote the vector $(a_1, ..., a_n)$. We set:

- $S = \mathbb{F}$.
- $W = \mathbb{F}^{k-2}$.
- Let $r = (r_1, ..., r_{k-2})$ be a random vector in W. Given $i \leq n$, the mapping $f_i^{\overrightarrow{a}} : S \times W \to S \times W$ is defined by

$$f_i^{\overrightarrow{a}}(s, r) = (p_{r,s}(a_i), 0, ..., 0)$$

where $p_{r,s}(Y)$ is equal to the polynomial $Y^{k-1} + r_{k-2}Y^{k-2} + ... + r_1 Y + s$.

Let X be a random variable uniformly distributed over $\mathbb{F}^{k-1}$. Given $i \leq n$, we define a random variable X_i in the following way

$$X_i = a \text{ if } X = (r_1, ..., r_{k-2}, s) \text{ and } (a_i)^{k-1} + r_{k-2}(a_i)^{k-2} + ... + r_1(a_i) + s = a$$

and we define a random variable X_{n+1} as follows

$$X_{n+1} = s \text{ if } X = (r_1, ..., r_{k-2}, s)$$

Notice that $(X, X_1, ..., X_n, X_{n+1})$ is the tuple of random variables that is associated to the scheme $\left(\mathbb{F} \times \mathbb{F}^{k-2}, f_1^{\overrightarrow{a}}, ..., f_n^{\overrightarrow{a}}\right)$. Let $I \in T_{n,k}$, coalition I knows $|I| \geq k$ points of the graph of $p_{r,s}(Y)$, which is a polynomial of degree $k-1$, then they can use polynomial interpolation to compute the coefficients of $p_{r,s}(Y)$. Notice that the secret is one of those coefficients, hence $H(X_{n+1} \mid X_I) = 0$. On the other hand, given $J \notin T_{n,k}$, we have

that the coalition J knows less than $k-1$ points of the graph of $p_{r,s}(Y)$. Suppose that $q(Y)$ is chosen uniformly at random from the set of polynomials of degree k, let r be the independent term of $q(Y)$, and let $b_1, ..., b_k \in \mathbb{F}$ be k pairwise different elements of $\mathbb{F}$. Given $a, b \in \mathbb{F}$, we have that

$$\begin{aligned} \Pr[r = a \mid q(b_1) = c_1, q(b_2) = c_2, ..., q(b_k) = c_k] &= \\ \Pr[r = b \mid q(b_1) = c_1, q(b_2) = c_2, ..., q(b_k) = c_k] &= \frac{1}{|\mathbb{F}|} \end{aligned}$$

It means that from the point of view of coalition J, the secret could be any element of $\mathbb{F}$, and all those elements have the same probability of being the secret. Thus, we have that $H(X_{n+1} \mid X_J) = H(X_{n+1})$.

It is important to remark that the mappings $f_1^{\overrightarrow{a}}, ..., f_n^{\overrightarrow{a}} : \mathbb{F}^{k-1} \rightarrow \mathbb{F}^{k-1}$ are linear mappings.

4.1 Linear Secret Sharing

We are mainly interested in schemes whose underlying functions are linear maps (the so called linear secret sharing schemes).

Definition 45 (Linear distribution scheme) *Given $n \geq 1$, a linear distribution scheme is a tuple $\Sigma = (S \times W, f_1, ..., f_n)$, where S and W are vector spaces over the same finite field, and $f_1, ..., f_n$ are linear mappings from $S \times W$ to $S \times W$.*

Definition 46 (Linear secret sharing scheme) *We say that a linear distribution scheme Σ is a linear secret sharing scheme realizing the access structure $(n, \mathcal{C})$, if and only if, Σ satisfies the correctness and privacy constrains of definition 44.*

One can identify a secret sharing scheme with the tuple of random variables it determines. Can a secret sharing scheme be reconstructed from the related tuple of random variables? We think that the answer is just a partial yes: if one knows a *concrete representation* of the tuple, one can use this representation to construct a secret sharing scheme related to this tuple. Nevertheless, some authors (see [11]) use to define a secret sharing scheme as a tuple of random variables whose Shannon entropies satisfy the correctness-constraints and the privacy-constraints determined by the access structure under consideration.

Notation 3 *Let h be a polymatroid of order n and let $R, J, K \subseteq [n]$, we set:*

1. $h(R \mid J) = h(R \cup J) - h(J)$
2. $I_h(R; J) = h(R) + h(J) - h(R \cup J)$
3. $I_h(R; J \mid K) = h(R \cup K) + h(J \cup K) - h(R \cup J \cup K) - h(K)$

Let $n \geq 1$, let $(n, \mathcal{C})$ be an access structure over $[n]$ and let Σ be a linear secret sharing scheme, notice that Σ determines a linear polymatroid h_Σ defined by

$$\text{for all } I \subseteq [n+1],\ h_\Sigma(I) = H\left(X_\Sigma^I\right)$$

Moreover, we have that:

1. $h_\Sigma(n+1 \mid I) = 0$, for all $I \in \mathcal{C}$
2. $h_\Sigma(n+1 \mid J) = h_\Sigma(n+1)$, for all $J \notin \mathcal{C}$

4.2 Rates

Ito et al [20] proved that for any access structure there exists a linear secret sharing scheme realizing it. Unfortunately, those schemes exhibit an unpleasant feature: the size of the shares is exponential with respect to the size of the secret.

Given a secret sharing scheme, the ratio between the size of the shares and the size of the secret is a measure of the efficiency and applicability of the scheme. If the ratio is large, computing and communication times could become prohibitive. Moreover, if the ratio is large and the shares are huge, the security provided by the scheme can be corrupted for practical reasons: it could happens that the parties do not have enough internal memory to store such a huge shares, and then, they can become forced to store those shares in an unsafe external memory (as the cloud), which could be infiltrated by the eavesdropper.

Definition 47 (Information ratio) *Given an access structure $(n, \mathcal{C})$ and given a secret sharing scheme Σ realizing $(n, \mathcal{C})$, the information ratio denoted by $\sigma^*(\Sigma)$ is equal to $\frac{h_\Sigma([n])}{h_\Sigma(n+1)}$.*

Given Σ, the information ratio is usually defined as

$$\rho(\Sigma) = \frac{\max_{i \leq n}(h_\Sigma(i))}{h_\Sigma(n+1)}$$

We have prefered to introduce our definition of $\sigma^*(\Sigma)$, which is very similar to the standard one, and which will allow us to simplify the proofs of our main results. Next lemma ensures that our notion of information ratio is closely related to the classical notion. The proof of the lemma is straightforward, and we omit it.

Lemma 48 *Let $n \geq 1$, and let Σ be a distribution scheme for n parties, it happens that $\rho(\Sigma) \leq \sigma^*(\Sigma) \leq n \cdot \rho(\Sigma)$.*

Thus, if we were able to prove that for all $n \geq 1$, and for all distribution scheme for n parties, say Σ, it happens that $\rho(\Sigma) \in O(n^c)$, then, we would get as a corollary that $\sigma^*(\Sigma) \in O(n^{c+1})$. This easy fact will be used many times in the next chapters.

It is important to remark that some other notions of information ratio have been introduced in the literature. A third important notion is the notion of average ratio, which was introduced by Matúš (see [26]), and which is defined as follows:

Given $n \geq 1$, a distribution scheme Σ, the average ratio of Σ is equal to

$$\tau(\Sigma) = \frac{1}{n \cdot h_\Sigma(n+1)} \sum_{i \leq n} h_\Sigma(i)$$

Notice that

$$\tau(\Sigma) \leq \rho(\Sigma) \leq \sigma^*(\Sigma) \leq n \cdot \tau(\Sigma)$$

Definition 49 (Optimal linear information ratio) *Given an access structure $(n, \mathcal{C})$, the optimal linear information ratio $\sigma_{\mathcal{L}}(\mathcal{C})$ is defined by*

$$\sigma_{\mathcal{L}}(\mathcal{C}) = \inf\{\sigma^*(\Sigma) : \Sigma \textit{ is a linear secret sharing scheme for } (n, \mathcal{C})\}$$

Define $\rho_{\mathcal{L}}(\mathcal{C})$ as

$$\rho_{\mathcal{L}}(\mathcal{C}) = \inf\{\rho(\Sigma) : \Sigma \text{ is a linear secret sharing scheme for } (n, \mathcal{C})\}$$

Given an access structure $(n, \mathcal{C})$, it follows from the above discussion that $\rho_{\mathcal{L}}(\mathcal{C}) \leq \sigma_{\mathcal{L}}(\mathcal{C}) \leq n \cdot \rho_{\mathcal{L}}(\mathcal{C})$.

Thus, if one has to cope with the secret sharing problem determined by an access structure $(n, \mathcal{C})$, he must try to construct a linear secret sharing scheme whose information ratio approximates the optimal linear information ratio of $(n, \mathcal{C})$. To this end, it would be

useful to know, in advance, which is the exact value of this ratio. How can one compute the optimal linear information ratio of a given access structure? Using the right linear rank inequalities.

4.3 Secret Sharing Schemes and polymatroids

As we will see, given a scheme Σ, the property of being a secret sharing scheme for $(n, \mathcal{C})$ is fully captured by the polymatroid h_Σ.

Definition 50 (Secret sharing polymatroid) *Let $(n, \mathcal{C})$ be an access structure and let h be a polymatroid of order $n+1$, we say that h is a secret sharing polymatroid for $(n, \mathcal{C})$, if and only if, the following conditions are satisfied:*

1. *CORRECTNESS: $h(n+1 \mid I) = 0$, for all $I \in \mathcal{C}$.*
2. *PRIVACY: $h(n+1 \mid J) = h(n+1)$, for all $J \notin \mathcal{C}$.*

Given $h \in \Gamma_{n+1}$, if h is a secret sharing polymatroid for $(n, \mathcal{C})$, then we say that h is *compatible* with the access structure $(n, \mathcal{C})$, or that it realizes the access structure $(n, \mathcal{C})$. Given $(n, \mathcal{C})$, we are interested in the set of linear polymatroids which are secret sharing for $(n, \mathcal{C})$.

Definition 51 (Secret sharing linear polymatroid) *Let $(n, \mathcal{C})$ be an access structure and let h be a linear polymatroid of order n, we say that h is a secret sharing linear polymatroid for $(n, \mathcal{C})$, if and only if, h is compatible with $(n, \mathcal{C})$. We use the symbol $\mathcal{SSLP}(\mathcal{C})$ to denote the set of all the secret sharing linear polymatroids for $(n, \mathcal{C})$.*

Next lemma is straightforward

Lemma 52 *Given a linear distribution scheme Σ, and given an access structure $(n, \mathcal{C})$, it happens that Σ is a linear secret sharing scheme for $(n, \mathcal{C})$, if and only if, $h_\Sigma \in \mathcal{SSLP}(\mathcal{C})$.*

The notions of secret sharing scheme and secret sharing polymatroid are almost the same: any secret sharing scheme for $(n, \mathcal{C})$ determines a secret sharing polymatroid. And, on the other hand, if we have h, a secret sharing polymatroid for $(n, \mathcal{C})$, and we have subspace arrangement representing h, it is possible to use this representation in order to construct a secret sharing scheme for $(n, \mathcal{C})$. Let $h \in \mathcal{SSLP}(\mathcal{C})$, and let $\mathcal{V} = (V, V_1, .., V_{n+1})$ be a linear representation of h. The tuple $\mathcal{V}$ is a concrete representation of h, which can be used to construct a distribution scheme Σ, given by

$$\Sigma = \left(\frac{V}{V_{n+1}} \times V_{n+1}, \pi_1, ..., \pi_n \right)$$

where given $i \leq n+1$, the symbol π_i denotes the projection of V onto $\frac{V}{V_i}$. It is easy to check that h_Σ is equal to h, and that Σ is secret sharing for $(n, \mathcal{C})$. Thus, we can conclude that linear secret sharing schemes and linear secret sharing polymatroids are one and the same thing.

4.4 Completeness of linear polymatroids

In this section we prove a series of technical results, which ensure that if one knows a generating set for the linear rank inequalities on $n+1$ variables, then he can compute the exact optimal linear information ratio of any access structure on n parties. Most of the results contained in this section are included in [27].

Notation 4 *Given $h \in \Gamma_{n+1}$, we set $\mathcal{F}(h) = \frac{h([n])}{h(n+1)}$.*

If $h \in \Gamma_{n+1}$ is an abstract polymatroid which is compatible with $(n, \mathcal{C})$, it could happens that h does not encode a secret sharing scheme for $(n, \mathcal{C})$. Then, if one computes

$$\beta_{\mathcal{C}} = \min \{\mathcal{F}(h) : h \in \Gamma_{n+1} \text{ and } h \text{ is compatible with } (n, \mathcal{C})\}$$

he is not computing the optimal information ratio of $(n, \mathcal{C})$, he is computing a lower bound for this ratio, which could be very much smaller than the real ratio, because of the existence of spurious polymatroids encoding spurious solutions of $(n, \mathcal{C})$. Moreover, the seminal results of Csirmaz [11] indicate that, for infinitely many access structures, the value $\beta_{\mathcal{C}}$ is far away from the real ratio.

If h has a concrete representation by a subspace arrangement (i.e. h is a linear polymatroid), the polymatroid h effectively encodes a linear secret sharing scheme for $(n, \mathcal{C})$. Then, instead of computing $\beta_{\mathcal{C}}$, one must compute the minimum of $\mathcal{F}$ over the discrete (and infinite) set of linear polymatroids that are compatible with the given access structure. Thus, it makes sense to compute

$$\lambda_{\mathcal{C}} = \min \{\mathcal{F}(h) : h \text{ is in the conic closure of} \in \mathcal{SSLP}(\mathcal{C})\}$$

We have to take into account that $\mathcal{L}_n$ is not the set of linear polymatroids of order n, the cone $\mathcal{L}_n$ is topological closure of the conic closure of the former set, and it contains infinitely many polymatroids that are not linear polymatroids, and which are not related to any linear secret sharing scheme. Thus, it could happens that $\lambda_{\mathcal{C}}$ is just a lower bound for $\sigma_{\mathcal{L}}(\mathcal{C})$. We prove, in this section, that it is not the case. We prove that for all access structure $(n, \mathcal{C})$, the equality $\sigma_{\mathcal{L}}(\mathcal{C}) = \lambda_C$ holds.

Lemma 53 *Given $m > 0$, given $h_1, ..., h_m \in \Gamma_{n+1}$ and given $c_1, ..., c_m > 0$, we have that* $\mathcal{F}\left(\sum_{j=1}^{m} c_j h_j\right) \geq \min_{j \leq m} \{\mathcal{F}(h_j)\}$.

Proof. Given $h \in \Gamma_{n+1}$, we have that $\mathcal{F}(h)$ is the slope of the two-dimensional ray determined by the point $P_h = (h(n+1), h(\{1,...,n\}))$. Notice that P_h belongs to the first quadrant of $\mathbb{R}^2$. Now, we make the proof by induction on m.

- Let $m = 2$. Given $h_1, h_2 \in \Gamma_{n+1}$, and $c_1, c_2 > 0$, we have that $\mathcal{F}(c_1h_1 + c_2h_2)$ is equal to the slope of the ray determined by $P_{c_1h_1+c_2h_2}$. Notice that $P_{c_1h_1+c_2h_2}$ belongs to the cone determined by P_{h_1} and P_{h_2}. Thus, the slope of this ray is bigger than the minimum of the slopes of the rays determined by P_{h_1} and P_{h_2}, and it means that $\mathcal{F}(c_1h_1 + c_2h_2) \geq \min\{\mathcal{F}(h_1), \mathcal{F}(h_2)\}$.

- Now we suppose that the assertion holds for $m = k$, we make the proof for $m = k+1$. Given $h_1, h_2, ..., h_{k+1} \in \Gamma_{n+1}$, and given $c_1, c_2, ..., c_{k+1} > 0$, we set $h = c_1h_1 + c_2h_2 + ... + c_kh_k$ and we set $g = c_{k+1}h_{k+1}$. We have that $h, g \in \Gamma_{n+1}$, given that Γ_{n+1} is closed under positive linear combinations. Notice that

$$\mathcal{F}(c_1h_1 + c_2h_2 + ... + c_{k+1}h_{k+1}) = \mathcal{F}(h+g) \geq \min\{\mathcal{F}(h), \mathcal{F}(g)\}$$

  If $\min\{\mathcal{F}(h), \mathcal{F}(g)\} = \mathcal{F}(g)$, we have that

$$\mathcal{F}(c_1h_1 + c_2h_2 + ... + c_{k+1}h_{k+1}) \geq \mathcal{F}(g) = \mathcal{F}(h_{k+1}) \geq \min_{j \leq k+1}\{\mathcal{F}(h_j)\}$$

  On the other hand, if $\min\{\mathcal{F}(h), \mathcal{F}(g)\} = \mathcal{F}(h)$, we have that

$$\mathcal{F}(c_1h_1 + c_2h_2 + ... + c_{k+1}h_{k+1}) \geq \mathcal{F}(h) \geq \min_{j \leq k}\{\mathcal{F}(h_j)\} \geq \min_{j \leq k+1}\{\mathcal{F}(h_j)\}$$

  and the lemma is proved.

■

Next theorem asserts that one can correctly compute linear secret sharing ratios, if one works on the right sections of the linear regions. Thus, in some sense, this theorem

answers a question of Csirmaz, who asked the following: which is the right closure of the set of linear polymatroids? Is it either the set of all rays generated by linear polymatroids, or the topological closure of the convex closure of those rays? Notice that the later set behaves better than the former, which is not convex. Notice also that, according to our results, the later set allows one to compute exact lower bounds for secret sharing. Thus, both closures are equally correct, but the later (the topological closure of the set of cc-linear polymatroids) has the pleasant structure of a closed convex cone, which can be effectively exploited in the applications.

Theorem 54 *Given* $\Delta \subseteq \mathbb{R}^{2^{n+1}-1}$ *for which there exists a finite number of linear rank inequalities, say* $v_1, ..., v_k \in \mathbb{R}^{2^{n+1}-1}$*, such that*

$$\Delta = \left\{ v \in \mathbb{R}^{2^{n+1}-1} : \langle v, v_i \rangle = 0, \textit{ for all } 1 \leq i \leq k \right\}$$

and given

$$\alpha = \inf \left\{ \mathcal{F}(h) : h \in \Delta \cap \mathcal{L}_{n+1},\ h(n+1) \neq 0 \right\}$$

there exists a sequence $\{h_j\}_{j \geq 0} \subseteq \Delta \cap \mathcal{L}_{n+1}$ *such that:*

1. *For all* j, h_j *is a linear polymatroid*
2. $\lim_{i \to \infty} \mathcal{F}(h_j) = \alpha$

Proof. First at all we observe that $\mathcal{F}$ is constant on any ray, it means that

$$\alpha = \inf \left\{ \mathcal{F}(h) : h \in \Delta \cap \mathcal{L}_{n+1},\ h(n+1) \neq 0,\ \|h\| = 1 \right\}$$

Notice that the later set is a compact one and hence

$$\alpha = \min \left\{ \mathcal{F}(h) : h \in \Delta \cap \mathcal{L}_{n+1},\ h(n+1) \neq 0,\ \|h\| = 1 \right\}$$

Thus there exists $h \in \Delta \cap \mathcal{L}_{n+1}$ such that $\mathcal{F}(h) = \alpha$. Then, there must exist a sequence $\{g_j\}_{j\geq 0} \subseteq \Delta \cap \mathcal{L}_{n+1}$, such that $g_j \to h$ and for all $j \geq 0$, the polymatroid g_j is a positive linear combination of linear polymatroids. We have that $\lim_{j\to\infty} \mathcal{F}(g_j) = \alpha$. Charatheodory's convexity theorem asserts that for all $j \geq 0$, there exist linear polymatroids $h_{j_1}, h_{j_2}, ..., h_{j_{2^{n+1}}}$, and there exist $c_{j_1}, ..., c_{j_{2^{n+1}}} \geq 0$ such that $g_j = \sum_{l=1}^{2^{n+1}} c_{j_l} h_{j_l}$. Notice that for all $j \geq 0$ and for all $l \leq 2^{n+1}$, the polymatroid $h_{j_l} \in \Delta$.

Given $j \geq 0$, the inequality $\mathcal{F}(g_j) \geq \min_{l\leq 2^{n+1}} \{\mathcal{F}(h_{j_l})\}$ holds by lemma 53. Now, given $j \geq 0$, we use the symbol $h_{k(j)}$ to denote the element of $\left\{h_{j_1}, ..., h_{j_{2^{n+1}}}\right\}$ that minimizes the function $\mathcal{F}$ within this finite set. Then, we have that

$$\alpha \leq \lim_{j\to\infty} \mathcal{F}\left(h_{k(j)}\right) \leq \lim_{j\to\infty} \mathcal{F}(g_j) = \alpha$$

Thus, if for all $j \geq 0$ we set $h_j = h_{k(j)}$, the theorem is proved. ■

Let $(n, \mathcal{C})$ be an access structure, given $I \in \mathcal{C}$, we use the symbol v_I to denote the linear rank inequality

$$e_{\{n+1\}\cup I} - e_I$$

and given $J \notin \mathcal{C}$, we use the symbol w_J to denote the linear rank inequality

$$e_{n+1} + e_J - e_{\{n+1\}\cup J}$$

Finally, we use the symbol $\Delta_{\mathcal{C}}$ to denote the set

$$\left\{ v \in \mathbb{R}^{2^{n+1}-1} : \langle v, v_I\rangle = 0 \text{ for all } I \in \mathcal{C}, \text{ and } \langle v, w_J\rangle = 0 \text{ for all } J \notin \mathcal{C} \right\}$$

Notice that $\mathcal{SSLP}(\mathcal{C}) = \Delta_{\mathcal{C}} \cap \mathcal{L}_{n+1}$. Thus, we can get from theorem 54 the following two results.

Theorem 55 *Given $\alpha_{\mathcal{C}} = \min\{\mathcal{F}(h) : h \in \mathcal{SSLP}(\mathcal{C})\}$, we have that $\alpha_{\mathcal{C}}$ is the optimal linear information ratio of $(n, \mathcal{C})$.*

Proof. Given $\alpha_{\mathcal{C}}$ there exists a sequence $\{h_i\}_{i\geq 0}$ of linear polymatroids such that for all $i \geq 0$, $h_i \in \Delta_{\mathcal{C}}$ and such that $\lim_{i\to\infty} \mathcal{F}(h_i) = \alpha_{\mathcal{C}}$. Given $j \geq 0$, the linear polymatroid h_j is given by a tuple $\left(V^j, V_1^j, ..., V_{n+1}^j\right)$. Set:

- $S^j = \frac{V^j}{V_{n+1}^j}$
- W^j is a subspace of V^j such that V^j is isomorphic to $S^j \times W^j$.
- For all $i \leq n$, the linear mapping f_i^j is equal to the projection of V^j onto the subspace $\frac{V^j}{V_i^j}$

Now, set $\Sigma^j = \left(S^j \times W^j, f_1^j, ..., f_n^j\right)$, it is easy to check that Σ^j is a linear secret sharing scheme for $\mathcal{C}$, since h_i is equal to h_{Σ^i}. Moreover, the equality $\mathcal{F}(h_j) = \sigma^*(\Sigma^j)$ holds for all $j \geq 0$. Thus, the inequality $\alpha_{\mathcal{C}} \geq \sigma_{\mathcal{L}}(\mathcal{C})$ holds.

Given $\sigma_{\mathcal{L}}(\mathcal{C})$, there exists a sequence $\{\Sigma_i\}_{i\geq 0}$ of linear secret sharing schemes realizing $\mathcal{C}$ and such that $\lim_{i\to\infty} \sigma^*(\Sigma_i) = \sigma_{\mathcal{L}}(\mathcal{C})$. Given $j \geq 0$, we set $h_j = h_{\Sigma_j}$. We have that $\mathcal{F}\left(h_{\Sigma_j}\right) = \sigma^*(\Sigma_j)$. Thus, we have that $\alpha_{\mathcal{C}} \leq \sigma_{\mathcal{L}}(\mathcal{C})$ and the theorem is proved. ■

Let $\Psi = \{\Psi_n\}_{n\geq 1}$ be a sequence such that for all $n \geq 1$, we have that Ψ_n is a subset of the cone of linear rank inequalities on n variables. Given an access structure $(n, \mathcal{C})$, we set

$$\sigma_{\mathcal{L}}^{\Psi}(\mathcal{C}) = \min\left\{\mathcal{F}(h) : h \in \Delta_{\mathcal{C}} \cap \Psi_{n+1}^{\circ}\right\}$$

Corollary 56 *If there exists an access structure $(n, \mathcal{C})$ such that $\sigma_{\mathcal{L}}^{\Psi}(\mathcal{C}) < \sigma_{\mathcal{L}}(\mathcal{C})$, then we have that $\mathcal{L}_{n+1}$ is a proper set of Ψ_{n+1}°.*

Proof. Notice that if $\sigma_{\mathcal{L}}^{\Psi}(\mathcal{C}) < \sigma_{\mathcal{L}}(\mathcal{C})$, then the convex cone determined by Ψ_{n+1}, which is equal to Ψ_{n+1}°, is strictly larger than the set $\mathcal{L}_{n+1}$. ■

Last corollary asserts that, if a certain set of linear rank inequalities does not allow one to compute the exact linear information ratio of all access structure, then he is using a wrong set of linear rank inequalities, he is using an incomplete set.

Chapter 5

Attacking the second DFZ question: An asymptotic approach

We begin in this chapter with our attempts of proving that the CI-method is not complete. We will present a first attack to our conjecture, this attack is based on the seminal ideas of Csirmaz [11]. We will get some preliminary and promising results.

5.1 Csirmaz' criterion

Let $\chi : \mathbb{N} \to \mathbb{N}$ be the function

$$\chi(n) = \max\{\sigma(\mathcal{C}) : (n, \mathcal{C}) \text{ is an access structure on } n \text{ parties}\}$$

It is widely believed that function χ is a function of exponential growth [6], that is

Conjecture 57 *There exists $c > 0$ such that $\chi(n) \in \Omega(2^{c \cdot n})$.*

One can use any set of constrains, satisfied by all the polymatroids coming from secret sharing schemes, in order to compute lower bounds for χ. Let Φ be such a set of

constrains, and define χ^{Φ} in the following way

$$\chi^{\Phi}(n) = \max_{(n,\mathcal{C})} \{\min \{\mathcal{F}(h) : h \in \Delta_{\mathcal{C}} \text{ and } h \text{ satisfies } \Phi\}\}$$

We have that χ^{Φ} is dominated by χ. If the constrains in Φ are weak, the function χ^{Φ} can grow very much slowly than χ. A minimal set of constrains is the set of Shannon inequalities, which are satisfied by all the abstract polymatroids. Let Φ_S be the later set of constrains, it follows from the work of Csirmaz [11] that $\chi^{\Phi_S}(n) \in O(n^2)$. Thus, we have that either the conjecture 57 is false, or there must exist non-Shannon inequalities satisfied by all the polymatroids coming from secret sharing schemes (all the entropic polymatroids). It is important to remark that the existence of non-Shannon inequalities was confirmed shortly after the publication of Csirmaz' work (see [34]).

Csirmaz' criterion, as discussed above, can be used to prove that a given set of constrains is not enough to characterize the entropic polymatroids. The application of the criterion goes as follows:

Given the set Φ, prove that for all $c > 0$, it happens that $\chi^{\Phi}(n) \notin \Omega(2^{c \cdot n})$.

A warning is in order: Csirmaz' criterion, when applied to general secret sharing can only yield conditional results, given that the hypothesis $\chi(n) \in \Omega(2^{c \cdot n})$, is only a conjecture.

5.2 Focussing on Linear Secret Sharing

We are interested in linear secret sharing, therefore we consider the following function

$$\chi_{\mathcal{L}}(n) = \max \{\sigma_{\mathcal{L}}(\mathcal{C}) : (n, \mathcal{C}) \text{ is an access structure on } n \text{ parties}\}$$

It is know that $\chi_{\mathcal{L}}(n) \in \Omega\left(n^{\log(n)/\log(\log(n))}\right)$, see [21] and [2]. Thus, we can use Csirmaz ideas, but focussing on linear sharing, and get, with some luck, unconditional

results. Let Φ be a set of constrains, satisfied by all the linear polymatroids coming from linear secret sharing schemes, and define $\chi_{\mathcal{L}}^{\Phi}(n)$ as

$$\max_{(n,\mathcal{C})} \{\min \{\mathcal{F}(h) : h \in \Delta_{\mathcal{C}} \text{ and } h \text{ satisfies } \Phi\}\}$$

We have

Criterion 1 *If* $\chi_{\mathcal{L}}^{\Phi}(n) \notin \Omega\left(n^{\log(n)/\log(\log(n))}\right)$, *then we have that* Φ *does not characterize the set of linear polymatroids.*

We are interested in sets of constrains that are constituted by linear inequalities, as for example the set Φ_S. A first application of the above criterion give us a proof of a well known result.

Proposition 58 *There are linear rank inequalities which cannot be obtained from the Shannon inequalities.*

Proof. According to Csirmaz results, $\chi_{\mathcal{L}}^{\Phi_S}(n) \in O(n^2)$. Then Φ_S does not characterize the set of linear polymatroids. It means that there exists $n > 1$, such that $\mathcal{L}_n \subset \Gamma_n$. We know that $\mathcal{L}_n$ is a closed convex cone, and then, there must exist a linear inequality that is satisfied by all the linear polymatroids, but which is not satisfied by all the polymatroids. Such an inequality is a linear rank non-Shannon inequality. ■

Now, we would like to apply the same type of argument to the set of inequalities that can be obtained via the CI-method. Let us prove, as a warm up, a theorem of Kinser [22], which claims that there are new linear rank inequalities at any dimension $n \geq 4$.

Theorem 59 *Given* $n \geq 1$, *there exist* $N > n$ *and a linear rank inequality on* N *variables which cannot be derived from the linear rank inequalities on* n *variables.*

Proof. Let $\chi_{\mathcal{L}} : \mathbb{N} \to \mathbb{N}$ be the function defined by

$$\chi_{\mathcal{L}}(m) = \max\{\sigma_{\mathcal{L}}(\mathcal{C}) : (\mathcal{C}, m) \text{ is an access structure}\}$$

We know that $\chi_{\mathcal{L}}(m) \in \Omega(m^{\log m/\log\log(m)})$ i.e. $\chi_{\mathcal{L}}$ is a superpolynomial function. Given $1 \leq m < k$, we use the symbol $(\mathcal{L}_k^m)^\circ$ to denote the set of linear rank inequalities on k variables, such that, at most m variables actually occur. Consider the sequence $\Phi = \{\Phi_k\}_{k\geq 1}$, defined by

$$\Phi_k = \begin{cases} (\mathcal{L}_k)^\circ, \text{ if } k \leq n \\ (\mathcal{L}_k^n)^\circ, \text{ if } k > n \end{cases}$$

Given Φ, we define a function $\chi_{\mathcal{L}}^{\Phi} : \mathbb{N} \to \mathbb{N}$ like before. It follows from the work of Martin et al [23] that $\chi_{\mathcal{L}}^{\Phi}(m) \in O(m^{n-1})$. Thus, we have that $\chi_{\mathcal{L}}^{\Phi}$ is asymptotically dominated by $\chi_{\mathcal{L}}$, and then there must exist $N > n$, such that $\chi_{\mathcal{L}}^{\Phi}(N) < \chi_{\mathcal{L}}(N)$. Then, there exists an access structure $\mathcal{C}$ over $[N]$, such that $\sigma_{\mathcal{L}}^{\Phi}(\mathcal{C}) < \sigma_{\mathcal{L}}(\mathcal{C})$. It follows from corollary 56 that $\Phi_{N+1} \subset \mathcal{L}_{N+1}^\circ$, and the theorem is proved. ■

Csirmaz proved that Shannon inequalities do not yield superlinear lower bounds for secret sharing, it implies that Shannon inequalities cannot yield superlinear lower bounds for linear secret sharing. Notice that the output of the CI algorithm, on input $(n, 0, \Gamma_n)$, is a spanning set for the Shannon inequalities on n variables. Thus, according to Csirmaz, the outputs of the CI algorithm, on this restricted class of inputs, cannot constitute a complete set of linear rank inequalities. Martin et al [23] used the method of Csirmaz to prove that if one runs the CI algorithm, on the infinite set of inputs $\{(n, 2, \Gamma_n) : n \geq 1\}$, then the linear rank inequalities that can be obtained this way yield lower bounds for lineal secret sharing which are at most polynomial. Therefore, we have

Theorem 60 *There exists n such that CI$[n, 2]$ does not generate the cone $(\mathcal{L}_n)^\circ$.*

Proof. In this case we consider the sequence $\Psi = \{\Psi_k\}_{k\geq 1}$, where Ψ_k is the set constituted by the linear rank inequalities on k variables which can be obtained as outputs

of *CI,* when it runs on the input $(k, 2, \Gamma_{k+2})$. Now we define $\chi_{\mathcal{L}}^{\Psi} : \mathbb{N} \to \mathbb{N}$ as

$$\chi_{\mathcal{L}}^{\Psi}(m) = \max\left\{\sigma_{\mathcal{L}}^{\Psi}(\mathcal{C}) : (\mathcal{C}, m) \text{ is an access structure}\right\}$$

It follows from the work of Martin et al [23] that $\chi_{\mathcal{L}}^{\Psi}(m) \in O(m^4)$. Thus, we have that $\chi_{\mathcal{L}}^{\Psi} < \chi_{\mathcal{L}}$, and that there exists $N > n$, such that $\chi_{\mathcal{L}}^{\Psi}(N) < \chi_{\mathcal{L}}(N)$. Then, there exists an access structure $\mathcal{C}$ over $[N]$, such that $\sigma_{\mathcal{L}}^{\Psi}(\mathcal{C}) < \sigma_{\mathcal{L}}(\mathcal{C})$. It follows, once again from corollary 56, that $\Psi_{N+1} \subset (\mathcal{L}_{N+1})^{\circ}$, and the theorem is proved. ■

The application of Csirmaz' criterion is not free of intricacies (there is not free lunch). Given a target set Φ, if one wants to prove that Φ is not a complete set, then he must find a sequence of polymatroids, say $\{h_n\}_{n\geq 1}$, such that:

1. For all $n \geq 1$, and for all access structure $(n, \mathcal{C})$, it happens that $h_n \in \Delta_{\mathcal{C}}$.
2. For all $n \geq 1$, the polymatroid h_n satisfies Φ.
3. It occurs that the function $\chi_h : \mathbb{N} \to \mathbb{N}$ defined by

$$\chi_h(n) = \mathcal{F}(h_n)$$

does not belong to $\Omega(n^{\log n/\log\log(n)})$.

The construction of such a sequence is, most of the time, a hard piece of work. Recall that we are trying to prove that the common information method is not complete. The first thing that we could try, is to extend the results of Martin et al [23], and prove that for all $k \geq 1$, there must exist n such that $CI[n, k]$ does not span the cone $(\mathcal{L}_n)^{\circ}$. It seems that the method employed by those authors does not work for larger $k's$. And, on the other hand, if we were able to extend those results for all $k > 2$, we could not immediately conclude that, for some $n \geq 1$, the set $CI[n]$ does not generate the cone $(\mathcal{L}_n)^{\circ}$. Moreover, if we could prove that the set $CI[n]$ does not generate the cone $(\mathcal{L}_n)^{\circ}$,

we could not immediately conclude that the common information method is not complete. It is the case, given that we are restricting the application of the CI algorithm to a very special class of inputs: we are only considering inputs such that the third component of all of them is constituted by Shannon inequalities. Notice that one can include in the inputs of our CI algorithm, some of the already known non-Shannon inequalities [34], and it could happens that those non-Shannon inequalities were the key for obtaining the spanning sets of the cones of linear rank inequalities. Thus, we think that in order to prove our conjecture it is necessary to try a more robust approach. Fortunately, there are some options to try.

Chapter 6

The abelian attack

It seems that the asymptotic approach won't lead us to our goal. Fortunately, there are some other approaches to try.

Suppose that we can define a family of polymatroids $\mathcal{H}$, such that:

1. Any linear polymatroid belongs to $\mathcal{H}$.
2. For all $n \geq 1$, it happens that $\Gamma_n \cap \mathcal{H}$ is a closed convex cone.
3. Any linear inequality that can be generating by CI-method holds for all the polymatroids in $\mathcal{H}$.

If additionally we have that there exists $h \in \mathcal{H}$ such that h is not linear, then we would get as a corollary that the CI-method is not complete.

We will try to construct, in this chapter, such a family of polymatroids. It is easy to ensure properties 1 and 2. In order to ensure the third property, it is a good idea to think in a family of entropic polymatroids, such that the tuples of random variables that are related to this family have common information. With this in mind, we will introduce the notion of abelian polymatroid.

6.1 Abelian polymatroids

An abelian arrangement of order n is a tuple $\mathcal{G} = (G, G_1, ..., G_n)$ such that G is a finite abelian group and, for all $i \leq n$, it happens that G_i is a subgroup of G. Given $\mathcal{G}$, it determines a polymatroid of order n, denoted with the symbol $h_{\mathcal{G}}$, and such that, for all $I \subseteq [n]$ the equality

$$h_{\mathcal{G}}(I) = \log\left(\left|\frac{G}{\bigcap\limits_{i\in I} G_i}\right|\right)$$

holds. We say that $h_{\mathcal{G}}$ is an abelian polymatroid and we say that $\mathcal{G}$ is an abelian representation of $h_{\mathcal{G}}$. Given $\mathcal{G} = (G, G_1, ..., G_n)$, we use the symbol X to denote a random variable that is uniformly distributed over G. Given $i \leq n$, we use the symbol X_i to denote the random variable induced by X over the quotient $\frac{G}{G_i}$. Let $X_{\mathcal{G}}$ be the tuple $(X_1, ..., X_n)$, we say that $X_{\mathcal{G}}$ is an abelian tuple.

Lemma 61 *Let G be a finite abelian group, and let K, R be two subgroups of G. We have that $|\langle K \cup R\rangle| = \frac{|K||R|}{|R\cap K|}$.*

Proof. Let $P = K \times R$. Notice that $|P| = |K|\,|R|$. Let $\phi : P \to \langle K \cup R\rangle$ be the surjective homomorphism defined by $\phi(x, y) = xy$. Notice that $\ker(\phi)$ is equal to the set

$$\left\{\left(y, y^{-1}\right) : y \in K \cap R\right\}$$

it implies that $|\langle K \cup R\rangle| = \frac{|K||R|}{|R\cap K|}$. ■

Theorem 62 *Abelian tuples have common information.*

Proof. Let $\mathcal{G} = (G, G_1, ..., G_n)$ be an abelian arrangement, let X be a random variable uniformly distributed over G, we suppose that for all $i \leq n$, the random variable X_i is the variable induced by X over the quotient $\frac{G}{G_i}$. Let $\mathcal{X}_{\mathcal{G}} = (X_1, ..., X_n)$ be an abelian tuple defined by $\mathcal{G}$.

Given $I \subseteq [n]$, we notice that X_I, which is the join random variable determined by the set $\{X_i : i \in I\}$, is equal to the random variable that is induced by X over the quotient $\frac{G}{\bigcap\limits_{i\in I} G_i}$.

Let $I, J \subseteq [n]$, we have to prove that the pair (X_I, X_J) has common information, that is: we have to define a random variable Z such that:

- $H(Z \mid X_I) = H(Z \mid X_J) = 0$
- $I(X_I; X_J) = H(Z)$

To this end, we will define a subgroup $L \trianglelefteq G$ such that Z is the random variable induced by X over $\frac{G}{L}$. The first condition on Z indicates that $\bigcap\limits_{i\in I} G_i$ and $\bigcap\limits_{i\in J} G_i$ must be contained in L, while the second condition suggest that L must be as small as possible. We set $L = \left\langle \left(\bigcap\limits_{i\in I} G_i\right) \cup \left(\bigcap\limits_{i\in J} G_i\right) \right\rangle$. It is easy to check that $H(Z \mid X_I) = H(Z \mid X_J) = 0$. Let $K = \bigcap\limits_{i\in I} G_i$ and $R = \bigcap\limits_{i\in J} G_i$. We have

$$\begin{aligned} I(X_I; X_J) &= H(X_I) + H(X_J) - H(X_I, X_J) \\ &= \log\left(\left|\frac{G}{K}\right|\right) + \log\left(\left|\frac{G}{R}\right|\right) - \log\left(\left|\frac{G}{K \cap R}\right|\right) \\ &= \log\left(\frac{|G|\,|R \cap K|}{|K|\,|R|}\right) = \log\left(\frac{|G|}{|\langle K \cup R\rangle|}\right) \\ &= H(Z) \end{aligned}$$

■

Definition 63 *Let h be a polymatroid, we say that it is a weakly abelian polymatroid, if and only if, h is a positive scalar multiple of an abelian polymatroid. We say that h is a cc-abelian polymatroid, if and only if, it is a sum of weakly abelian polymatroids, and we say that h is almost abelian, if and only if, it is the limit of a sequence of cc-abelian polymatroids.*

Next proposition is straightforward.

Proposition 64 *Let $n \geq 1$ and let $\mathcal{A}_n$ be the class of almost abelian polymatroids of order n, we have:*

1. *Any linear polymatroid of order n belongs to $\mathcal{A}_n$.*
2. *For all $n \geq 1$, the set $\mathcal{A}_n \cap \Gamma_n$ is a closed convex cone.*
3. *Any linear inequality that can be generated using the CI-method holds for the polymatroids in $\mathcal{A}_n$.*

We have, from the above proposition, that the CI-method cannot distinguish between $\mathcal{A}_n$ and $\mathcal{L}_n$. Thus, if there exists an almost abelian polymatroid which is not almost linear, then the CI-method is not complete.

Let $\mathcal{A}$ the set of all almost abelian polymatroid, and let $\mathcal{E}$ be the set of all almost entropic polymatroids $\left(\text{notice that } \mathcal{E} = \bigcup_{n\geq 1} \overline{\Gamma_n^*}\right)$.

6.2 Abelian Sharing

Given h, an abelian polymatroid of order $n+1$, and given $\mathcal{G} = (G, G_1, ..., G_{n+1})$, an abelian representation of h, one can use $\mathcal{G}$ to construct a distribution scheme for n parties, which we denote with the symbol $\Sigma_{\mathcal{G}}$, and such that $h_{\Sigma_{\mathcal{G}}} = h$. The distribution scheme $\Sigma_{\mathcal{G}}$ is given by the tuple $\left(\frac{G}{G_{n+1}} \times G_{n+1}, \pi_1, ..., \pi_n\right)$, where given $i \leq n+1$, the symbol π_i denotes the projection of G onto $\frac{G}{G_i}$. Notice that $G \simeq \frac{G}{G_{n+1}} \times G_{n+1}$. Given $(n, \mathcal{C})$, the scheme $\Sigma_{\mathcal{G}}$ is an abelian secret sharing scheme for $(n, \mathcal{C})$, if and only if, h is a secret sharing polymatroid for $(n, \mathcal{C})$. Thus, there exists a natural correspondence between abelian polymatroids, abelian schemes and abelian arrangements.

Remark 65 *It is important to remark that the polymatroids that are related to general distribution schemes are the entropic polymatroids. Recall that given h, a polymatroid of order n, we say that it is an entropic polymatroid, if and only if, there exists a tuple of finite random variables, $\mathcal{X} = (X, X_1, ..., X_n)$, such that*

1. $X = X_{[n]}$
2. *For all* $I \subseteq [n]$, $h(I) = H(X_I)$

We use the symbol $\sigma_{\mathcal{A}}(\mathcal{C})$ to denote the abelian optimal information ratio of $(n, \mathcal{C})$, which is defined as

$$\sigma_{\mathcal{A}}(\mathcal{C}) = \inf \{\sigma^*(\Sigma) : \Sigma \text{ is an abelian secret sharing scheme for } (n, \mathcal{C})\}$$

Notice that:

Proposition 66 *If there exists $(n, \mathcal{C})$ such that $\sigma_{\mathcal{A}}(\mathcal{C}) < \sigma_{\mathcal{L}}(\mathcal{C})$, then the CI-method is not complete.*

We conjecture that there exists an access structure $(n, \mathcal{C})$ satisfying the above inequality. Proving our conjecture seems to be a hard piece or work, given that, it is not known if linear information ratios are computable, and then, for most access structures, we cannot compute neither their linear ratios nor their abelian ratios. Suppose we have an access structure $(n, \mathcal{C})$, and suppose we want to prove that $\sigma_{\mathcal{A}}(\mathcal{C}) < \sigma_{\mathcal{L}}(\mathcal{C})$, then we will have to look for a lower bound on $\sigma_{\mathcal{L}}(\mathcal{C})$ separating those two ratios. Those lower bounds have been studied in the related literature and some sharp lower bounds have been established for many different access structures, see [4]. As far as we know, all those lower bounds have been computed using linear rank inequalities, and it happens that all the known linear rank inequalities are satisfied by abelian polymatroids. Thus,

we cannot use the known techniques in order to establish a *separating lower bound* like the one we are looking for.

How can we overcome those difficulties? Our strategy is to look for very structured access structures admitting ideal abelian secret sharing but which do not admit linear ideal secret sharing (for definitions see below)

6.3 Matroids and access structures

Definition 67 *We say that M is a matroid without loops, if and only if, for all $i \leq n$, we have that $rk_M(\{i\}) = 1$.*

The natural examples of matroids are matroids without loops, and given a matroid with loops, it can be easily converted in a matroid without loops by simply deleting the loops. Thus, the class of matroids without loops is completely representative of the abstract notion of matroid. We will only consider, in this work, matroids without loops.

Definition 68 *Let M be a matroid, we set:*

- $\dim(M) = rk_M([n])$
- $Gen(M) = \{I \subseteq [n] : rk_M(I) = \dim(M)\}$
- $B(M) = \{I \subseteq [n] : rk_M(I) = \dim(M) = |I|\}$
- $Ind(M) = \{I \subseteq [n] : rk_M(I) = |I|\}$
- $Dep(M) = \{I \subseteq [n] : rk_M(I) < |I|\}$

Let M be a matroid, it determines a collection of large sets: the generators of the matroid, which are the elements of $Gen(M)$. Notice that $Gen(M)$ is a filter, and hence

the pair $(n, Gen(M))$ is an access structure. From now on, we will focus our attention on access structures of the form $(n, Gen(M))$. By an abuse of language we will use the symbol M to denote the access structure $(n, Gen(M))$.

The study of access structures determined by matroids is an old theme in secret sharing. One of the first works in this line of research (and perhaps the most influential) is the work of Davenport and Brickell, [7], who studied the access structures determined by the ports of connected matroids.

Definition 69 *Given a matroid M, and a secret sharing scheme for M, say Σ, we say that Σ is ideal, if and only if, $\sigma^*(\Sigma) = \dim(M)$.*

Ideal secret sharing schemes were introduced by Davenport and Brickell. Those schemes are called ideal because there do not exist secret sharing schemes for M achieving an information ratio strictly smaller than $\dim(M)$ (i.e. ideal schemes are optimal). We want to investigate the existence of linear and abelian ideal secret sharing schemes for different matroids, this research problem was, in some sense, the problem addressed by Davenport and Brickell, but, it is important to remark, there are important differences between our work and their seminal work:

- In their setting (access structures from matroid ports) the secret dealer belongs to the ground set of the matroid, while in our setting (see below) the ground set of the matroid is the set of parties, and the dealer lives out of the matroid.
- Davenport and Brickell studied general ideal secret sharing schemes, we focus on linear schemes and in the novel notion of abelian schemes.
- They consider only connected matroids, we work with the very much larger class of matroids without loops.

Definition 70 (Linear Sharable matroid) *Given M a matroid, we say that M is linear shareable ($\mathcal{L}$-shareable, for short), if and only if, $\sigma_{\mathcal{L}}(M) = \dim(M)$.*

We define entropic shareable matroids ($\mathcal{E}$-shareable) and abelian shareable matroids ($\mathcal{A}$-shareable) accordingly.

Let M be a matroid, we say that M has an array representation, if and only if, there exists an array $\mathcal{B} = (B, B_1, ..., B_n)$ such that rk_M is a multiple of $h_{\mathcal{B}}$. Here, the array $\mathcal{B}$ can be either a linear array, or an abelian array, or a tuple of random variables. If M has an array representation, we would like to use this representation to construct an ideal secret sharing scheme for M. If we were working in the Davenport-Brickell setting, we could easily construct the ideal secret sharing scheme from the given representation, it is not the case in our setting because the secret dealer (the secret space) is not encoded by the array representing M. Suppose that the order of M is equal to n, and suppose that $\mathcal{B} = (B, B_1, ..., B_n)$ is an array representation of M, in order to construct a secret sharing scheme from $\mathcal{B}$, first we have to extend $\mathcal{B}$ to an array $\mathcal{B}^+ = (B, B_1, ..., B_n, B_{n+1})$, satisfying some further requirements. Consider the following lemma.

Lemma 71 *If M is a linear representable matroid, then M is $\mathcal{L}$-shareable.*

Proof. Let M be a linear matroid, and let $\mathcal{V} = (V, V_1, ..., V_n)$ be a linear representation of M. We suppose that the ground field of V is large enough (very much larger than n), and then, we can suppose that there exists $v \in V$ such that $v \notin \bigcup_{I \notin Gen(M)} \left(\left\langle \bigcup_{i \in I} V_i^{\perp} \right\rangle \right)$. We set $V_{n+1} = (\langle v \rangle)$ and then we have that

$$\mathcal{V}^+ = (V, V_1, ..., V_n, V_{n+1})$$

Let $f_{\mathcal{V}^+}$ be the rank function of the arragment $\mathcal{V}^+$. Now we have to prove that $f_{\mathcal{V}^+}$ is a linear secret sharing polymatroid for M, encoding a linear secret sharing scheme.

- If $I \in Gen(M)$ then,

$$\begin{aligned} f_{\mathcal{V}^+}(n+1 \mid I) &= f_{\mathcal{V}^+}(I \cup \{n+1\}) - f_{\mathcal{V}^+}(I) \\ &= \dim(M) - \dim\left(\bigcup_{i \in I} V_i\right) \\ &= \dim(V) - \dim(V) = 0 \end{aligned}$$

- If $I \notin Gen(M)$ then,

$$\begin{aligned} f_{\mathcal{V}^+}(n+1 \mid I) &= f_{\mathcal{V}^+}(I \cup \{n+1\}) - f_{\mathcal{V}^+}(I) \\ &= f_{\mathcal{V}^+}(I) + f_{\mathcal{V}^+}(\{n+1\}) - f_{\mathcal{V}^+}(I) \\ &= f_{\mathcal{V}^+}(\{n+1\}) \\ &= \dim(V_{n+1}) = 1 \end{aligned}$$

Let $(\mathcal{V}^+)^* = \left(V, V_1^\perp, V_2^\perp, ..., V_n^\perp, V_{n+1}^\perp\right)$, then we know that there exists $h_{(\mathcal{V}^+)^*} = \lambda f_{\mathcal{V}^+}$, with $h_{(\mathcal{V}^+)^*}$ a linear polymatroid. Notice that $h_{(\mathcal{V}^+)^*}$ satisfies the secret sharing conditions. Then, there exists a secret sharing scheme, say $\Sigma_{h_{(\mathcal{V}^+)^*}}$, such that $h_{(\mathcal{V}^+)^*}$ is its polymatroid. Besides, $\Sigma_{h_{(\mathcal{V}^+)^*}}$ is an ideal scheme since

$$\frac{h_{(\mathcal{V}^+)^*}([n])}{h_{(\mathcal{V}^+)^*}(n+1)} = \frac{\lambda f_{\mathcal{V}^+}([n])}{\lambda f_{\mathcal{V}^+}(n+1)} = \frac{\dim(V)}{1} = \dim(V)$$

■

The above proof seems to indicate that working with linear rank functions could be easier than working with linear polymatroids. We can freely choose to work with any one of those two classes of submodular functions, given that, as we showed before, linear rank functions and linear polymatroids are one and the same thing.

6.4 On the shareability of weakly linear matroids

We know that any linear matroid is $\mathcal{L}$-shareable, is the converse true? We will prove, in next section, that any weakly linear matroid is $\mathcal{L}$-shareable. We know that there are non-linear matroids, which are weakly linear, and then we will establish that the converse of lemma 71 is not true.

Let $(M, \mathcal{V})$ be a pair such that M is a non-linear matroid, and such that $\mathcal{V} = (V, V_1, ..., V_n)$ is a weakly linear representation of rk_M. We would like to know if there exists V_{n+1}, a subspace of V, such that $(V, V_1, ..., V_n, V_{n+1})$ encodes a linear ideal secret sharing scheme for M.

There must exist $m > 1$, such that for all $i \leq n$, it happens that $\dim(V_i) = m$. We want to decide if there exists V_{n+1}, a m-dimensional subspace of V, such that for all $I \notin Gen(M)$, it happens that $V_{n+1} \cap \left\langle \bigcup_{i \in I} V_i \right\rangle = \{0\}$. We prove, in this section, that the above decision problem can be solved in randomized polynomial time [1].

Let $PB(M)$ be equal to

$$\left\{ I \subseteq [n] : \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle \right) = \dim(V) - m \right\}$$

and let W be a subspace of V, notice that, if for all $I \in PB(M)$ it happens that

$$\left(\left\langle \bigcup_{i \in I} V_i \right\rangle \right) \cap W = \{0\}$$

then the same is true for all $I \notin Gen(M)$. We have that there exists k such that $\dim(V) = k \cdot m$, and then we are trying to construct a m-dimensional subspace of V which does not intersect the subspaces of V that are determined by the subsets of $[n]$ whose rank is equal to $k - 1$. Let $I_1, ..., I_s$ be a enumeration of those subsets. Given $r \leq s$, one can compute a basis of $\left\langle \bigcup_{i \in I_r} V_i \right\rangle$, say $v_1^r, ..., v_{m(k-1)}^r$. Given W, a m-dimensional

subspace of V, one can always compute a basis of W, say $w_1, ..., w_m$. We have that

$$\left(\left\langle \bigcup_{i \in I_r} V_i \right\rangle\right) \cap W = \{0\}$$

if and only if,

$$\det\left[v_1^r, ..., v_{m(k-1)}^r, w_1, ..., w_m\right] \neq 0$$

We use the symbol $M(W, r)$ to denote the $k \cdot m \times k \cdot m$ matrix $\left[v_1^r, ..., v_{m(k-1)}^r, w_1, ..., w_m\right]$, whose columns are the vectors $v_1^r, ..., v_{m(k-1)}^r, w_1, ..., w_m$. Let $M(W)$ be the matrix

$$\begin{bmatrix} M(W,1) & 0 & \cdots & 0 \\ 0 & M(W,2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M(W,s) \end{bmatrix}$$

We have that, $\langle w_1, ..., w_m \rangle$ is a good subspace, a subspace satisfying the two conditions discussed above, if and only if, $\det(M(W)) \neq 0$.

Let $\mathbb{F}$ be the ground field of $\mathcal{V}$:

1. Given $i \leq s$, we set $M(X, i) = \left[X_1, .., X_m, v_1^i, ..., v_{(k-1)\cdot m}^i\right]$, where X_i is the vector $(X_1^i, ..., X_{k \cdot m}^i)$ and for all $j \leq k \cdot m$, the symbol X_j^i denotes a variable that ranges over $\mathbb{F}$.

2. $M(X)$ is the matrix

$$\begin{bmatrix} M(X,1) & 0 & \cdots & 0 \\ 0 & M(X,2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M(X,s) \end{bmatrix}$$

Notice that $\det(M(X))$ is a polynomial of degree $m \cdot s$, over the variables

$$\left\{X_l^i : i \leq m \text{ and } l \leq k \cdot m\right\}$$

and which is defined on $\mathbb{F}$. We have:

Proposition 72 *The weakly linear representation $\mathcal{V}$ can be effectively extended to a linear ideal secret sharing scheme for M over $\mathbb{F}$, if and only if,* $\det(M(X))$ *is a non-null polynomial over $\mathbb{F}$.*

The above facts imply that our problem can be reduced to the problem of deciding if a given multivariate polynomial is non-null, it implies that we can solve the former problem in randomized polynomial time [1], which means that there exists a randomized algorithm, which on input $(M, \mathbb{F})$, decides if M can be weakly represented over $\mathbb{F}$, and such that algorithm is bounded above by a polynomial $p\left(m, p, \frac{q}{\epsilon}\right)$, where m is the size of M, p is the size of $\mathbb{F}$ and ϵ is the error probability.

6.5 Characterizing shareability

Theorem 73 *Let M be a matroid without loops, we have:*

1. *M is $\mathcal{L}$-shareable, if and only if, rk_M is the limit of a sequence of weakly linear polymatroids.*
2. *If M is $\mathcal{E}$-shareable, then rk_M is almost entropic.*
3. *If M is $\mathcal{A}$-shareable, then rk_M is almost abelian.*

We will break the proof of the above theorem in a series of lemmas. From now on, we will suppose that M is a matroid without loops, of order n, and whose dimension is equal to m.

Lemma 74 *Let Σ be an ideal secret sharing scheme for M, we have that for all $i \leq n$, the equality $h_\Sigma(i) = h_\Sigma(n+1)$ holds.*

Proof. Let $i \leq n$ and let I be a basis of M such that $i \in I$. If we set $J = I \setminus \{i\}$, we get

$$\begin{aligned} h_\Sigma(J \cup \{n+1\}) &= h_\Sigma(J) + h_\Sigma(n+1) \\ &\leq h_\Sigma(I) \leq h_\Sigma(J) + h_\Sigma(i) \end{aligned}$$

and then we have that $h_\Sigma(n+1) \leq h_\Sigma(i)$.

Now, we suppose that there exists $i \leq n$ such that $h_\Sigma(i) > h_\Sigma(n+1)$. Let $I = \{i, i_2, ..., i_m\}$ be a basis of M. Given $k \in \{2, ..., m\}$ we set $I_k = I \setminus \{i_k\}$. Notice that

$$\begin{aligned} h_\Sigma(I_k) + h_\Sigma(n+1) &= h_\Sigma(I_k \cup \{n+1\}) \\ &\leq h_\Sigma(I_k \cup \{i_k\}) \end{aligned}$$

then, we have

$$\begin{aligned} h_\Sigma(\{i, i_2, ..., i_{k-1}, i_k\}) - h_\Sigma(\{i, i_2, ..., i_{k-1}\}) &\geq h_\Sigma(I_k \cup \{i_k\}) - h_\Sigma(I_k) \\ &\geq h_\Sigma(n+1) \end{aligned}$$

Now, we can prove, by induction on k, that for all $k \geq 2$ the inequality

$$h_\Sigma(\{i, i_2, ..., i_{k-1}, i_k\}) \geq h_\Sigma(i) + (k-1)\, h_\Sigma(n+1)$$

holds. It implies that

$$\begin{aligned} m \cdot h_{\Sigma}(n+1) &= h_{\Sigma}([n]) \\ &\geq h_{\Sigma}(I) \\ &\geq h_{\Sigma}(i) + (m-1)\, h_{\Sigma}(n+1) \\ &> m \cdot h_{\Sigma}(n+1) \end{aligned}$$

which is clearly a contradiction. Thus, we have that for all $i \leq n$, the inequality $h_{\Sigma}(i) \leq h_{\Sigma}(n+1)$ holds. ■

A similar argument, to the one used in the above proof, can be used to prove that

Lemma 75 *Let Σ be an ideal secret sharing scheme for M, and let $I \in Ind(M)$, we have that $h_{\Sigma}(I) = |I|\, h_{\Sigma}(n+1)$.*

Lemma 76 *Let Σ be an ideal secret sharing scheme for M, and let $I \in Dep(M)$, we have that $h_{\Sigma}(I) = rk_M(I) \cdot h_{\Sigma}(n+1)$.*

Proof. Let $I \in Dep(M)$, and suppose that $rk_M(I) = k$. There exists $K \subset I$, such that, $K \in Ind(M)$ and $rk_M(K) = k$. We have that

$$k \cdot h_{\Sigma}(n+1) = h_{\Sigma}(K) \leq h_{\Sigma}(I)$$

Now, we will suppose that there exists $I \in Dep(M)$ such that $h_{\Sigma}(I) > rk_M(I) \cdot h_{\Sigma}(n+1)$. Let K be a subset of I such that $K \in Ind(M)$ and $rk_M(K) = rk_M(I)$, and

let S be a subset of $[n]$ such that $S \cup K$ is a basis of M and $S \cap K = \emptyset$. We have that

$$\begin{aligned} h_\Sigma([n]) &\geq h_\Sigma(I \cup S) \\ &= h_\Sigma(I) + h_\Sigma(S) \\ &= h_\Sigma(I) + |S| h_\Sigma(n+1) \\ &> rk_M(I) \cdot h_\Sigma(n+1) + |S| h_\Sigma(n+1) \\ &= |K| h_\Sigma(n+1) + |S| h_\Sigma(n+1) \\ &= m \cdot h_\Sigma(n+1) \end{aligned}$$

and this is clearly a contradiction. Thus, we have for all $I \in Dep(M)$, the equality $h_\Sigma(I) = rk_M(I) \cdot h_\Sigma(n+1)$ holds. ■

Corollary 77 *Let M be a matroid and let $\mathcal{C}$ be a class of entropic polymatroids that is closed under restrictions and scalar multiples. If there exists an ideal secret sharing scheme for M, say Σ, such that $h_\Sigma \in \mathcal{C}$, we have that $rk_M \in \mathcal{C}$.*

Notice that the classes $\mathcal{L}$, $\mathcal{A}$ and $\mathcal{E}$ satisfy the conditions in the statement of the above corollary. Thus, we have

Corollary 78 *Let M be a matroid, we have:*

1. *If there exists an ideal linear secret sharing scheme for M, then rk_M is weakly linear.*
2. *If there exists an ideal abelian secret sharing scheme for M, then rk_M is weakly abelian.*
3. *If there exists an ideal secret sharing scheme for M, then rk_M is weakly entropic.*

The arguments used so far can be, easily, adapted to get the following result

Proposition 79 *Let M be a matroid without loops, we have*

1. *If M is $\mathcal{L}$-shareable, then rk_M is the limit of a sequence of weakly linear polymatroids.*

2. *If M is $\mathcal{A}$-shareable, then rk_M is the limit of a sequence of weakly abelian polymatroids.*

3. *If M is $\mathcal{E}$-shareable, then rk_M is the limit of a sequence of weakly entropic polymatroids..*

Now, we prove the converse in the linear case.

Lemma 80 *Let M be a matroid, if there exists a weakly linear polymatroid h realizing M (i.e. the polymatroid h is a secret sharing polymatroid for the matroid M) and $\frac{h([n])}{h(n+1)} = c$ for some $c \geq m$, then there exists a linear secret sharing scheme for M, say Σ, such that $\sigma^*(\Sigma) = c$.*

Proof. Suppose that h is a weakly linear polymatroid realizing M, we can suppose, without loss of generality, that h is linear. There exists a subspace arrangement $\mathcal{V} = (V, V_1, ..., V_n, V_{n+1})$ such that $h_{\mathcal{V}} = h$. We use the representation $\mathcal{V}$ to construct a linear secret sharing scheme for M. To this end, we set:

- $R = V_{n+1}$.
- $S = \frac{V}{V_{n+1}}$.
- Given $i \leq n$, π_i is the projection from $V \cong S \times R$ to $\frac{V}{V_i}$.

It is easy to check that $\Sigma_{\mathcal{V}} = (S, R, \pi_1, ..., \pi_n)$ is a linear secret sharing scheme for M, moreover $\sigma^*(\Sigma_{\mathcal{V}}) = \frac{h_{\mathcal{V}}([n])}{h_{\mathcal{V}}(n+1)} = c$. ■

Remark 81 *An analogous result can be proved if we put either the term abelian or entropic instead of the term linear in the statement of the above lemma. The proof for the abelian case is the same as above, while the proof of the entropic case can be obtained in a similar way using the fact that any entropic polymatroid can be approximated by a sequence of group representable polymatroids (see [8]).*

Lemma 82 *Let M be a matroid and suppose that rk_M is weakly linear, then there exists an ideal linear secret sharing scheme for M.*

Proof. Suppose that rk_M is weakly linear, there exists a subspace arrangement $\mathcal{V} = (V, V_1, ..., V_n)$, with base field $\mathbb{F}$, and there exists $c > 0$, such that:

1. For all $I \subseteq [n]$, the equality $rk_M(I) = \frac{1}{c} h_{\mathcal{V}}(I)$ holds. Notice that for all $i \leq n$ we have that $\dim\left(\frac{V}{V_i}\right) = \frac{c}{\log_2(|\mathbb{F}|)}$. From now on, we will use the symbol d to denote the quantity $\frac{c}{\log_2(|\mathbb{F}|)}$.
2. Moreover, $V = \left\langle \bigcup_{i \leq n} V_i \right\rangle$. Notice that $\dim(V) = d \cdot m$.

Recall that we are trying to construct an ideal linear secret sharing scheme for M, to this end we have to extend the polymatroid $h_{\mathcal{V}}$ to a linear polymatroid defined over $[n+1]$ and realizing the matroid M. Let $PB(M)$ be the set

$$\{I \in Ind(M) : rk_M(I) = m - 1\}$$

and let $\mathcal{W}$ be equal to $\bigcup_{I \in PB(M)} \left\langle \bigcup_{i \in I} V_i^{\perp} \right\rangle$. If we set $K_M = |PB(M)|$ (notice that $K_M \leq 2^n$), we get that $\mathcal{W}$ is equal to the union of K_M subspaces of V, each of dimension $d \cdot (m-1)$.

We say that a family $\{W_j\}_{j \in J}$ of subspaces of V is a *nonintersecting family*, if and only if, for all $s, l \in J$, *if* $s \neq l$ then $W_s \cap W_l = \{0\}$. It can be proved (see [28]) that

there exists a nonintersecting family of d-dimesional subspaces of V whose size is equal to $\frac{|\mathbb{F}|^{d\cdot m}-1}{|\mathbb{F}|^{d}-1}$. Let $\{W_j\}_{j\in J}$ be such a family and suppose that, for all $j \in J$ it happens that $\mathcal{W} \cap W_j \neq \{0\}$. Then, we have that

$$\begin{aligned} K_M\left(|\mathbb{F}|^{d\cdot(m-1)}\right) &\geq |\mathcal{W}| \\ &\geq \left(\frac{|\mathbb{F}|^{d\cdot m}-1}{|\mathbb{F}|^{d}-1}\right)(|\mathbb{F}|-1) \end{aligned}$$

We can suppose that the size of $\mathbb{F}$ is as large as we want, and then if we suppose that $|\mathbb{F}|$ is large (very much larger than 2^n) we get that the inequality

$$K_M\left(|\mathbb{F}|^{d\cdot(m-1)}\right) \geq \left(\frac{|\mathbb{F}|^{d\cdot m}-1}{|\mathbb{F}|^{d}-1}\right)(|\mathbb{F}|-1)$$

cannot be satisfied. It means that if $|\mathbb{F}|$ is large, there must exist W, a subspace V, such $\dim(W) = d$ and $W \cap \mathcal{W} = \{0\}$.

Thus, we suppose $|\mathbb{F}|$ large and we pick $W \trianglelefteq V$ as above. Let $\mathcal{V}^{\perp}$ be the subspace arrangement

$$\left(V, V_1, ..., V_n, W^{\perp}\right)$$

We check that $h_{\mathcal{V}^{\perp}}$ realizes M.

- Let $I \in Gen(M)$, we have that

$$\log_2\left(\left|\frac{V}{\bigcap\limits_{i\in I} V_i}\right|\right) = \log_2(|V|)$$

then $\bigcap_{i\in I} V_i = \{0\} = \left(\bigcap_{i\in I} V_i\right) \cap W^{\perp}$, and then

$$\log_2\left(\left|\frac{V}{\bigcap_{i\in I} V_i}\right|\right) = \log_2\left(\left|\frac{V}{\left(\bigcap_{i\in I} V_i\right)\cap W^{\perp}}\right|\right)$$

and it means that $h_{\mathcal{V}^{\perp}}(n+1 \mid I) = 0$.

- Let $I \notin Gen(M)$, then we have that

$$\left(\bigcup_{i\in I} V_i^{\perp}\right) \cap W = \{0\}$$

it implies that

$$\dim\left(\left\langle \bigcup_{i\in I} V_i^{\perp}\right\rangle \cup W\right) = \dim\left\langle \bigcup_{i\in I} V_i^{\perp}\right\rangle + \dim(W)$$

and it implies that

$$h_{\mathcal{V}^{\perp}}(n+1 \mid I) = h_{\mathcal{V}^{\perp}}(n+1)$$

Thus, we have the tuple $\left(V, V_1, ..., V_n, W^{\perp}\right)$ defines a secret sharing scheme for M. Notice that

$$\dim(V) = d \cdot m = \dim(W) \cdot m$$

then, the linear secret sharing scheme defined by $\mathcal{V}^{\perp}$ is ideal. ■

Lemma 83 *Let M be a matroid and suppose that rk_M is the limit of a sequence of weakly linear polymatroids, then, there exists a sequence of secret sharing schemes for M whose information ratios converge to m.*

Proof. Suppose that rk_M is as in statement of the lemma. Then, there exists a

sequence of weakly linear polymatroids, say $\{h_i\}_{i\geq 1}$, such that $\lim_{i\to\infty} h_i = rk_M$. Thus, we can suppose that for all $k \geq 1$, and for all $I \subseteq [n]$, the inequality $|h_k(I) - rk_M(I)| < \frac{1}{k}$ holds.

We fix a large integer N. Given $k \geq N$, we know that h_k is weakly linear, and then there must exist C_k such that $C_k \cdot h_k$ is a linear polymatroid. Let $\mathcal{V}_k = \left(V_k, V_1^k, ..., V_n^k\right)$ be a subspace arrangement such that $C_k \cdot h_k = h_{\mathcal{V}_k}$. We can suppose, without loss of generality, that for all $I \subseteq [n]$, the inequality

$$\left| \frac{\dim\left(\left\langle \bigcup_{i\in I} V_i^k \right\rangle\right)}{\dim\left(V_1^k\right)} - rk_M(I) \right| < \frac{1}{k}$$

holds.

Let $B(M)$ be the set of basis of M, and let $k_M = |B(M)|$ (notice that $k_M < 2^n$). Given $I \in B(M)$, it could happens that

$$\frac{C_k \cdot \dim\left(\left\langle \bigcup_{i\in I} V_i^k \right\rangle\right)}{\dim\left(V_1^k\right)} = \dim(V_k) - \delta \cdot \dim\left(V_1^k\right)$$

where $0 < \delta < \frac{1}{k}$. If it is the case, there must exist a nonempty set $A_I^k \subseteq V_k$ such that

$$\left\langle \left(\bigcup_{i\in I} V_i^k \right) \cup A_I^k \right\rangle = V_k$$

and

$$\dim\left(\left\langle A_I^k \right\rangle\right) < \delta \cdot \dim\left(V_1^k\right)$$

Let $A_k = \bigcup_{I\in B(M)} A_I^k$. We set

$$\mathcal{W}_k = \left(V_k, \left\langle V_1^k \cup A_k \right\rangle, ..., \left\langle V_n^k \cup A_k \right\rangle\right)$$

Notice that

1. For all $I \in B(M)$ we have that

$$\dim\left(\left\langle \bigcup_{i\in I} \langle V_i^k \cup A_k\rangle \right\rangle\right) = \dim(V_k)$$

2. For all $I \subseteq [n]$

$$\begin{aligned}\dim\left(\left\langle \bigcup_{i\in I} V_i^k \right\rangle\right) &\leq \dim\left(\left\langle \bigcup_{i\in I} \langle V_i^k \cup A_k\rangle \right\rangle\right) \\ &\leq \dim\left(\left\langle \bigcup_{i\in I} V_i^k \right\rangle\right) + k_M \cdot \delta \cdot \dim\left(V_1^k\right)\end{aligned}$$

Thus, we can suppose that there exists a sequence of subspace arrangements $\{\mathcal{U}_i\}_{i\geq 1}$ such that:

1. Given $i \geq 1$, the arrangement $\mathcal{U}_i$ is equal to $(U_i, U_1^i, ..., U_n^i)$.

2. For all $i \geq 1$ and for all $I \subseteq [n]$ the inequality

$$\left| \frac{\dim\left(\left\langle \bigcup_{k\in I} U_k^i \right\rangle\right)}{\dim(U_1^i)} - rk_M(I) \right| \leq \frac{1}{i}$$

holds.

3. For all $i \geq 1$ and for all $I \in B(M)$ the equality

$$\dim\left(\left\langle \bigcup_{k\in I} U_k^i \right\rangle\right) = \dim(U_i)$$

holds.

Let N be a large integer, we can suppose that $\dim(U_N) = m \cdot \dim\left(U_1^N\right)$. Let $I \in PB(M)$, we have that

$$\dim\left(\left\langle \bigcup_{k\in I} U_k^N \right\rangle\right) \leq (m-1)\cdot \dim\left(U_1^N\right) + \frac{1}{N}\cdot \dim\left(U_1^N\right)$$

Our aim is the construct a subspace of U_N, which we will denote with the symbol U_{n+1}^N, and such that

- $\dim\left(U_{n+1}^N\right)$ is close to $\dim\left(U_1^N\right)$.
- For all $I \in PB(M)$, it happens that $\left\langle \bigcup_{k\in I} U_k^N \right\rangle \cap U_{n+1}^N = \{0\}$.

Given $I \in PB(M)$, we use the symbol U_I^N to denote the subspace $\left\langle \bigcup_{k\in I} U_k^N \right\rangle$. Now, we set

$$W_I^N = \begin{cases} U_I^N, \text{ if } \dim\left(U_I^N\right) \leq (m-1)\cdot \dim\left(U_1^N\right) \\ A_I^N, \text{ otherwise} \end{cases}$$

where A_I^N is a subspace of U_I^N such that $\dim\left(A_I^N\right) = (m-1)\cdot \dim\left(U_1^N\right)$.

Consider the family $\left\{W_I^N : I \in PB(M)\right\}$, it is a small family of subspaces of U_N, each of dimension less or equal than $(m-1)\cdot \dim\left(U_1^N\right)$. We can use the argument employed in the proof of the previous lemma to guarantee the existence of a subspace B^N of U_N, whose dimension is equal to $\dim\left(U_1^N\right)$, and such that for all $I \in PB(M)$ it happens that $B^N \cap W_I^N = \{0\}$. Notice that

$$\dim\left(U_I^N\right) - \dim\left(W_I^N\right) \leq \frac{1}{N}\dim\left(U_1^N\right)$$

It implies that for all $I \in PB(M)$, the inequality

$$\dim\left(B^N \cap U_I^N\right) \leq \frac{1}{N}\dim\left(U_1^N\right)$$

holds, and it implies that we can construct a subspace of B^N, say C^N, such that:

1. For all $I \in PB(M)$ it happens that $C^N \cap U_I^N = \{0\}$.

2. $\left(1 - \frac{k_M}{N}\right) \cdot \dim\left(U_1^N\right) \leq \dim\left(C^N\right) \leq \dim\left(U_1^N\right)$.

Thus, if we choose to make $U_{n+1}^N = C^N$, we succeed. Thus, we set

$$\mathcal{U}_N^+ = \left(U_N, U_1^N, ..., U_n^N, C^N\right)$$

and we set $\left(\mathcal{U}_N^+\right)^\perp = \left(U_N, \left(U_1^N\right)^\perp, ..., \left(U_n^N\right)^\perp, \left(C^N\right)^\perp\right)$. Notice that for all N, the linear polymatroid $h_{\left(\mathcal{U}_N^+\right)^\perp}$ realizes M and notice that the inequality

$$\frac{h_{\left(\mathcal{U}_N^+\right)^\perp}([n])}{h_{\left(\mathcal{U}_N^+\right)^\perp}(n+1)} \leq \left(\frac{1}{1 - \frac{k_M}{N}}\right) \cdot m$$

holds. Thus, we have that the sequence $\left\{\left(\mathcal{U}_N^+\right)^\perp\right\}_{N \geq 1}$ witnesses that M is $\mathcal{L}$-shareable, and the lemma is proved. ■

With the proof of the above lemmas we have completed the proof of the first item of Theorem 73. For the abelian and entropic cases, we only have one of the two implications and the proofs of those implications are similar to the linear case.

6.6 A separating matroid

We are looking for a matroid M such that $\dim(M) = \sigma_{\mathcal{A}}(M) < \sigma_{\mathcal{L}}(M)$. We know that M must be a non-linear matroid, because linear matroids are $\mathcal{L}$-shareable. On the other hand, we know that M must be almost entropic, because our matroid must be, at least, shareable. It happens that some non-linear matroids are not useful for our purposes:

- Some non-linear matroids are more complex than expected, and because of this, they are not shareable. One important example is the Vamos matroid, it follows

from the work of Beimel [4], that the optimal information ratio of the Vamos matroid is strictly bigger than its dimension.

- Some non-linear matroids are more simple than expected, and, although they are non-linear, they are weakly linear, and as a consequence, they are $\mathcal{L}$-shareable. One important example is the Non Pappus matroid [32].

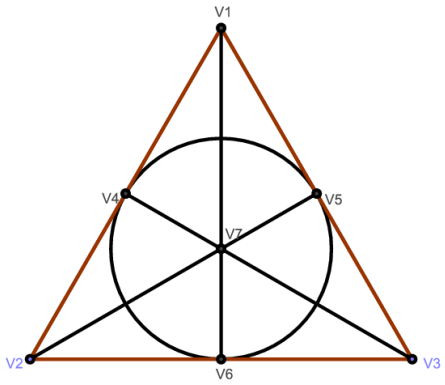
According to the previous results, we have to look for a non-linear matroid for which there exists an abelian representation. Thus, our problem is very close to a classical problem of matroid theory, which asks for the construction of a non-linear and entropic matroid [30]. We will not solve the former problem in this paper, but we will exhibit a non-linear matroid which is almost abelian (and then, almost entropic). Thus, we will "almost solve" the later problem.

Definition 84 *Let M be a matroid of order m, and let N be a matroid of order n. We will suppose that the ground set of N is equal to $\{m+1, ..., m+n\}$. The amalgamation of M and N is a matroid of order $m+n$ whose rank function is given by: Let $I \subseteq [m+n]$, we have*

$$rk_{M \oplus N}(I) = rk_M(I \cap [m]) + rk_N(I \cap \{m+1, ..., m+n\})$$

The amalgamation operation can be useful to construct non-linear matroids. To this end, one can amalgamate a strictly even matroid and a strictly odd matroid. The outcome of such a construction is a non-linear matroid, the rough idea is that if it were linear, then it must be strictly even and strictly odd.

An important example of a strictly even matroid is the Fano matroid, which is a matroid of order 7, and which we denote with the symbol F. The best way of defining the independent sets of F is by means of the picture below

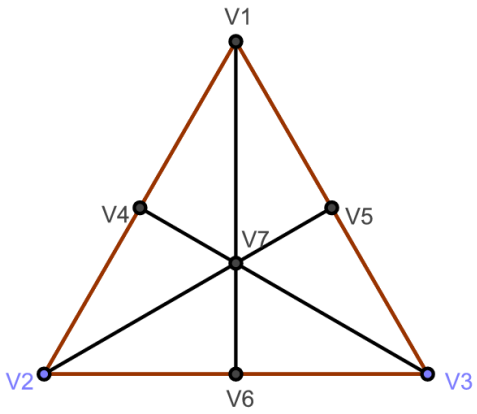


Given $A \subseteq \{1, 2, ..., 7\}$, the set A belongs to F, if and only if, either, $|A| \leq 2$, or $|A| = 3$ and the three points in A are not colinear (where the lines are the six line segments in the picture plus the circle). Let $\mathcal{V} = (V, V_1, ..., V_7)$ be a subspace arrangement, such that V is a three dimensional vector space and let

$$
\begin{aligned}
V_1 &= \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle, V_2 = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle, V_3 = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle, \\
V_4 &= \left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle, V_5 = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle, V_6 = \left\langle \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \\
V_7 &= \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle
\end{aligned}
$$

It can be checked that if the ground field of V is $GF\left(2^k\right)$, then $\mathcal{V}$ is a linear representation of F.

The Non-Fano matroid is an example of a strictly odd matroid, it is a matroid of order 7 whose elements can be best described by means of the following picture



We use the symbol F^{-} to denote the Non-Fano matroid whose elements (independent sets) are all the sets of size smaller than 3 plus the triples that are not colinear.

If we set $V = \mathbb{R}$, we get that for all $I \subseteq [7]$, the equality

$$rk_{F^{-}}(I) = \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right)$$

holds. Therefore, we say that F^{-} is representable over $\mathbb{R}$. It is known that a matroid is representable over $\mathbb{R}$, if and only if, it can be represented over a finite field (see [29]). On the other hand, it is known that F^{-} cannot be represented over $GF\left(2^k\right)$, for all $k \geq 1$. Thus, there must exists a prime number $p \neq 2$, such that, for all $k \geq 1$, the Non-Fano matroid is representable over $GF\left(p^k\right)$.

A second important operation on matroids is truncation.

Definition 85 *Given a polymatroid* $h : (\wp([n]) \setminus \{\emptyset\}) \to \mathbb{R}$*, we set*

$$\alpha_h = \max\{h(I) : h(I) \neq h([n])\}$$

The truncation of h*, denoted by* h^T*, is defined by: for all* $I \in (\wp([n]) \setminus \{\emptyset\})$*, the equality*

$$h^T(I) = \min\{\alpha_h, h(I)\}$$

holds.

Lemma 86 *Weakly linear polymatroids are closed under truncations.*

Proof. Let h be a weakly linear polymatroid, there exists $c \geq 0$ and there exists a subspace arrangement $\mathcal{V} = (V, V_1, ..., V_n)$ such that for all $I \subseteq [n]$, the equality

$$h(I) = c \cdot \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right)$$

holds. We suppose that $V = \left\langle \bigcup_{i \in [n]} V_i \right\rangle$. Let $PB(\mathcal{V})$ be the set

$$\left\{ I \subseteq [n] : \left\langle \bigcup_{i \in I} V_i \right\rangle \neq V \right\}$$

We can suppose that the ground field of $\mathcal{V}$ is as large as we want, and then, we can pick $v \in V$ such that $v \notin \bigcup_{I \in PB(\mathcal{V})} \left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right)$. Let π be the projection of V onto $\langle v \rangle^{\perp}$, and let

$$\mathcal{V}_1 = (\pi(V), \pi(V_1), ..., \pi(V_n))$$

It is easy to check that for all $I \subseteq [n]$, the equality

$$\dim\left(\left\langle \bigcup_{i \in I} \pi(V_i) \right\rangle\right) = \min\left\{ \dim(V) - 1, \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right) \right\}$$

holds. Let

$$\alpha_{\mathcal{V}} = \max\left\{ \dim\left(\left\langle \bigcup_{i \in I} V_i \right\rangle\right) : \left\langle \bigcup_{i \in I} V_i \right\rangle \neq V \right\}$$

We can iterate the above construction to define a subspace arrangement

$$\mathcal{V}^T = (W, W_1, ..., W_n)$$

such that for all $I \subseteq [n]$ the equality

$$\dim\left(\left\langle \bigcup_{i\in I} W_i \right\rangle\right) = \min\left\{\dim\left(\left\langle \bigcup_{i\in I} V_i \right\rangle\right), \alpha_{\mathcal{V}}\right\}$$

holds. Notice that, for all $I \subseteq [n]$, we have

$$h^T(I) = c \cdot \dim\left(\left\langle \bigcup_{i\in I} W_i \right\rangle\right)$$

■

Lemma 87 *$h_{F\oplus F^-}$ is not the limit of a sequence of weakly linear polymatroids.*

Proof. Suppose that $h_{F\oplus F^-}$ is the limit of a sequence of weakly linear polymatroids, and let $\{h_i\}_{i\geq 1}$ be such a sequence. It is easy to check that the sequence $\left\{h_i^T\right\}_{i\geq 1}$ converges to $(h_{F\oplus F^-})^T$. On the other hand, Chan et. al. [9] proved that $(h_{F\oplus F^-})^T$ is not almost linear. The lemma follows, given that if h is the limit of a sequence of weakly linear polymatroids, then it is almost linear. ■

Corollary 88 *$F \oplus F^-$ is not $\mathcal{L}$-shareable.*

Lemma 89 *$h_{F\oplus F^-}$ is the limit of a sequence of weakly abelian polymatroids.*

Proof. Let p be a prime number such that F^- is representable over $\mathbb{F}_p$. Given $\epsilon > 1$, we pick two positive integers r, k such that

$$1 - \epsilon < \frac{k \log_2(p)}{r} < 1 + \epsilon$$

Let $\mathcal{V}_1 = (V^1, V_1, ..., V_7)$ be a linear representation of F over $\mathbb{F}_{2^r}$, and let $\mathcal{V}_2 = (V^2, V_8, ..., V_{14})$ be a linear representation of F^- over $\mathbb{F}_{p^k}$. Notice that, for all $I \subseteq [7]$

and for all $J \subseteq \{8, 9, ..., 14\}$, it happens that

$$\begin{aligned} h_{\mathcal{V}_1}(I) &= r \cdot rk_F(I) \\ h_{\mathcal{V}_2}(J) &= k \cdot \log_2(p) \cdot rk_{F^-}(J) \end{aligned}$$

Thus, we can define a group arrangement

$$\mathcal{G} = \left(V^1 \times V^2, V_1 \times V^2, ..., V_7 \times V^2, V^1 \times V_8, ..., V^1 \times V_{14}\right)$$

such that, for all $I \subseteq [14]$, we have

$$\begin{aligned} h_{\mathcal{G}}(I) &= \log_2\left(\left|\frac{V^1 \times V^2}{\left(\bigcap_{i \in I \cap [7]} (V_i \times V^2)\right) \cap \left(\bigcap_{i \in I \cap \{8,...,14\}} (V^1 \times V_i)\right)}\right|\right) \\ &= \log_2\left(\left|\frac{V^1 \times V^2}{\left(\bigcap_{i \in I \cap [7]} V_i\right) \times \left(\bigcap_{i \in I \cap \{8,...,14\}} V_i\right)}\right|\right) \\ &= \log_2\left(\left|\frac{V^1}{\bigcap_{i \in I \cap [7]} V_i}\right|\right) + \log_2\left(\left|\frac{V^2}{\bigcap_{i \in I \cap \{8,...,14\}} V_i}\right|\right) \\ &= r \cdot h_{\mathcal{V}_1}(I \cap [7]) + k \log_2(p) \cdot h_{\mathcal{V}_2}(I \cap \{8, ..., 14\}) \end{aligned}$$

Notice that, for all $I \subseteq [14]$, the inequality

$$\left|\frac{h_{\mathcal{G}}(I)}{r} - rk_{F \oplus F^-}(I)\right| < 3\epsilon$$

holds.

Thus, we have that $rk_{F\oplus F^-}$ is the limit of a sequence of weakly abelian polymatroids.

■

Following Beimel, [4], we say that a group arrangement $\mathcal{G} = (G, G_1, ..., G_n)$ is a quasilinear arrangement, if and only if, G is equal to the direct product of two vector spaces (over possibly different fields). We define the notions of quasilinear polymatroid and quasilinear secret sharing scheme accordingly. Notice that we proved that $rk_{F\oplus F^-}$ can be approximated by a sequence of quasilinear polymatroids. We would like to use this sequence to construct a sequence of quasilinear secret sharing schemes for M, whose rates converge to $dim\left(F \oplus F^{-}\right)$. Unfortunately it is not possible. Such an impossibility is a particular case of the following fact.

Let $\mathcal{V} = (V \times W, V_1, ..., V_n)$ be a quasilinear array, we say that $\mathcal{V}$ is full, if and only if, there exist $I_1, I_2 \subset [n]$ satisfying the following conditions:

- $V_{I_1} = V \times U$, where U is a proper subspace of W.
- $V_{I_2} = H \times W$, where H is a proper subspace of V.

Let K be a subgroup of $V \times W$, we say that it is a nonintersecting subgroup for $\mathcal{V}$, if and only if, for all $I \subset [n]$, it happens that if $V_I \neq V \times W$ then $K \cap V_I = \{(0,0)\}$.

Proposition 90 *If $\mathcal{V}$ is full, and V and W are vector spaces over fields of different characteristic, there do not exist nonintersecting subgroups for $\mathcal{V}$.*

Proof. Let K be a subgroup of $V \times W$. If there exists $v \in V \setminus \{0\}$ such that $(v, 0) \in K$, then we have that $(v, 0) \in K \cap V_{I_1}$. On the other hand, if there exists $w \in W \setminus \{0\}$ such that $(0, w) \in K$, then we have that $(0, w) \in K \cap V_{I_2}$ Thus, given $(x, y) \in K \setminus \{(0,0)\}$, it must happens that x and y are nonnull. Let $(x, y) \in K \setminus \{(0,0)\}$, the subgroup $\langle (x, y) \rangle$ contains an element z such that $z \neq (0,0)$ and either $\pi_V(z) = 0$ or $\pi_W(z) = 0$. ■

Thus, it is by not means clear if all the matroids whose rank function is the limit of a sequence of weakly abelian polymatroids, are $\mathcal{A}$-shareables. Nevertheless we think that the quasi abelianicity of $F \oplus F^-$ provides us with strong evidence concerning its $\mathcal{A}$-shareability, and then, it also provides us with strong evidence supporting our conjecture that abelian sharing outperforms linear sharing.

6.7 Concluding remarks and applications

We have arrived to a very concrete problem of combinatorial nature, which is the question about the abelian shareability of the matroid $F \oplus F^-$. This problem cannot be discarded as unimportant, given that any solution to it will have far reaching consequences. Let us list some of those consequences.

1. If $F \oplus F^-$ is $\mathcal{A}$-shareable, then, abelian sharing outperforms linear sharing.
2. It follows from the work of Chan et al. [9], that if $F \oplus F^-$ is $\mathcal{A}$-shareable then, abelian network coding outperforms linear network coding.
3. If $F \oplus F^-$ is $\mathcal{A}$-shareable, then, the CI-method is not complete.
4. If $F \oplus F^-$ is not $\mathcal{A}$-shareable, then the class abelian polymatroids is not closed under truncations.

It is important to remark that we can reach the same conclusions, if we choose to work with a matroid M (instead of $F \oplus F^-$), such that, M is the amalgamation of two matroids, one of them connected and strictly even, while the other one is connected and strictly odd.

Bibliography

[1] S. Arora, B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University, New York, 2009.

[2] L. Babai, A. Gal, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19 (1999), 301 - 319.

[3] A. Beimel, A. Gal, and M. Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6 (1997), 29 - 45.

[4] A. Beimel and N. Livne. On Matroids and Non-ideal Secret Sharing. *IEEE Transactions on Information Theory*, 54 (2008), 236 - 241.

[5] A. Beimel and Y. Ishai. On the power of nonlinear secret-sharing. *SIAM Journal on Discrete Mathematics*, 19 (2005), 258 - 280.

[6] A. Beimel. *Secret-Sharing Schemes: A Survey*, 2011.

[7] E. F. Brickell and D. M. Davenport. On the classification of Ideal Secret Sharing Schemes. *Journal of Cryptology*, 4 (1991), 123 - 134.

[8] T. Chan and R. Yeung. On a relation between information inequalities and group theory. *IEEE Transactions on Information Theory*, 48 (2002), 1992 - 1995.

[9] T. Chan, A. Grant, and D. Puger. Truncation technique for characterizing linear polymatroids. *IEEE Transactions on Information Theory*, 57 (2011), 6364 - 6378.

[10] T. Cover and J. Thomas. *Elements of information theory*, John Wiley and Sons, New York, 1991.

[11] L. Csirmaz. The size of a share must be large. *Journal of Cryptology*, 10 (1997), 223 - 231.

[12] R. Dougherty. Computations of linear rank inequalities on six variables. *IEEE International Symposium on Information Theory* (ISIT) (Honolulu, Hawaii), (2014), 2819 - 2823.

[13] R. Dougherty, C. Freiling, and K. Zeger. Linear rank inequalities on five or more variables. (2010) arxiv.org: 0910.0284v3.

[14] _____. Networks, Matroids, and Non-Shannon Information Inequalities. *IEEE Transactions on Information Theory.* 53(2007), 1949 - 1969.

[15] S. Fujishige. *Submodular Functions and Optimization.* Ed. Elsevier, North-Holland, 2005.

[16] A. Gomez, C. Mejia, and J.A. Montoya. Linear network coding and the model theory of linear rank inequalities. *IEEE International Symposium on Network Coding* (NetCod) (Aalborg, Denmark), (2014), 1 - 6.

[17] D. Hammer, A. Romashchenko, A. Shen, and N. Vereshchagin. Inequalities for Shannon Entropy and Kolmogorov Complexity. *Journal of Computer and System Sciences*, 60 (2000). 442 – 464.

[18] J. Hiriart-Urruty and C. Lemaréchal. *Convex Analysis and Minimization Algorithms I.* Springer-Verlag, Berlín, 1991.

[19] A. W. Ingleton. Representation of matroids. Combinatorial mathematics and its applications. Proceedings, Oxford, (1969), 149 - 167.

[20] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Globecom* (Tokio, Japan), (1987), 99 - 102.

[21] M. Karchmer and A. Wigderson. On span programs. *Eighth Annual Structure in Complexity Theory Conference* (San Diego, USA), (1993), 102 - 111.

[22] R. Kinser, New inequalities for subspace arrangements. *Journal Combinatorial Theory Serie A*, 118 (2010), 152 - 161.

[23] S. Martin, C. Padro, and A. Yang. Secret sharing, rank inequalities and information inequalities. *Lecture Notes in Computer Science*, 8043 (2013), 277 - 288.

[24] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *Journal of Mathematical Cryptology*, 4 (2010), 95 - 120.

[25] F. Matúš. Infinitely many information inequalities. *International Symposium on Information Theory* (2007).

[26] _____ Two constructions on limits of entropy functions. *IEEE Transactions on Information Theory*, 53 (2006), 320 - 330.

[27] C. Mejia. Linear secret sharing and the automatic search of linear rank inequalities. *Applied Mathematical Science*, 9 (2015), 5305 - 5324.

[28] F. Oggier, N. Sloane, S. Diggavi, A. Calderbank. Nonintersecting subspaces based on finite alphabets. *IEEE Transactions on Information Theory* 51(2005), 4320 - 4325.

[29] J. Oxley. *Matroid Theory*. Oxford Mathematics, New York, 1992.

[30] C. Padró. *Lecture Notes in Secret Sharing*, 2013.

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

[32] J. Simonis, A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14 (1998) pp. 179–197

[33] R. Yeung. *A First Course in Information Theory*. Springer, Berlin, 2002.

[34] Z. Zhang and R. Yeung. A non-shannon-type conditional inequality of information quantities. *IEEE Transactions on Information Theory*, 43 (1997), 1982 - 1986.