Research Article

Carolina Mejia and Juan Andres Montoya*

Abelian sharing, common informations, and linear rank inequalities

https://doi.org/10.1515/jmc-2022-0020
received May 31, 2021; accepted July 23, 2022

Abstract: Dougherty et al. introduced the common information (CI) method as a method to produce non-Shannon inequalities satisfied by linear random variables, which are called linear rank inequalities. This method is based on the fact that linear random variables have CI. Dougerthy et al. asked whether this method is complete, in the sense that it can be used to produce all linear rank inequalities. We study this question, and we attack it using the theory of secret sharing schemes. To this end, we introduce the notions of Abelian secret sharing scheme and Abelian capacity. We prove that: If there exists an access structure whose Abelian capacity is smaller than its linear capacity, then the CI method is not complete. We investigate the existence of such an access structure.

Keywords: secret sharing, polymatroids, linear rank inequalities

MSC 2020: 94D99

1 Introduction

This work is mainly devoted to the following three topics:
(1) Linear information inequalities.
(2) The common information (CI) method.
(3) Secret sharing schemes.

Linear information inequalities are the linear inequalities satisfied by Shannon entropy. It has been said that linear information inequalities are the fundamental laws of information processing. The true fact is that those inequalities are important tools in the analysis of communication networks [22]. This follows from the following fact:

Let G be a network topology, and let P_G be a communication problem related to G. The set of solutions for P_G can be suitably represented as the set of functions that satisfy all linear information inequalities plus some additional constraints that depend on G.

Access structures are a special type of network topology. An access structure is a pair $C = (P, \mathcal{A})$, where P is a finite set of parties and $\mathcal{A} \subset \mathrm{Pow}(P)$. Moreover, the set $\mathcal{A}$ must be upward closed as it is supposed to be constituted by the large *authorized* subsets of P. The sharing problem P_C is to distribute, to the parties in P, the shares of a secret s. The distribution protocol should guarantee the following:
(1) Large authorized sets of shareholders can reconstruct the secret.
(2) Small sets of shares convey zero information about the secret.

* **Corresponding author: Juan Andres Montoya,** Mathematics Department, Universidad Nacional de Colombia, Bogotá, Colombia, e-mail: jamontoyaa@unal.edu.co
Carolina Mejia: Mathematics Department, Universidad Nacional de Colombia, Bogotá, Colombia, e-mail: cmejiam@udistrital.edu.co

Distribution protocols that fulfill both conditions are called *secret sharing schemes*. Secret sharing schemes are the backbone of most protocols for secure multiparty computation. Therefore, it is important to construct efficient schemes for different access structures. We say that a secret sharing scheme is efficient when the shares can be quickly computed, when the secret can be quickly reconstructed, and when the sizes of the shares are close to the size of the secret. We are interested in efficient secret sharing schemes that can be constructed with linear maps or some more general types of algebraic morphisms.

Linear secret sharing schemes are the sharing schemes that are built using linear maps. The random variables that are determined by those schemes are called *linear random variables*. Those random variables satisfy all linear information inequalities and some other inequalities that are specific for the linear world. We use the term *linear rank inequalities* to designate the linear inequalities that are satisfied by linear random variables. The analysis of an access structure $C = (P, \mathcal{A})$ over n parties forces us to consider a set of $n + 1$ linear random variables that model the secret, the shares, and the topology of C. The same analysis forces us to work with the linear rank inequalities that involve $n + 1$ random variables. We would like to generate all those inequalities. It is natural to ask: Is the set of linear rank inequalities spanned by Shannon inequalities?

Ingleton discovered, long time ago, the first *non-Shannon inequality* satisfied by linear random variables [11]. We know that there are many *non-Shannon linear rank inequalities*. We also know that we need all of them to prove tight bounds for linear secret sharing over general access structures. Can we enumerate all those inequalities?

Dougherty et al. introduced *the CI method* as a method to produce non-Shannon linear rank inequalities [8]. This method is based on the fact that linear random variables have *CI* [10]. We observed earlier:

> If there exists a class of random variables, which is larger than the class of linear random variables, which have common information, and which outperforms the class of linear random variables. Then, the CI method cannot be complete.

This is the starting point of our investigations [16]. We introduced the novel notions of *Abelian random variable*, *Abelian secret sharing scheme*, and *Abelian capacity* [17]. We introduced those notions as a way of copying with the question of Dougherty et al. [18]. In this work, we prove that:

Suppose that there exists an access structure over n parties whose Abelian capacity is smaller than its linear capacity. Then, the CI method cannot produce all the linear rank inequalities over $n + 1$ variables.

We investigate the validity of the hypothesis, that is: we study the existence of access structures for which Abelian secret sharing outperforms linear secret sharing.

Relations to previous studies, contributions, and organization of the article.

This work is related to the research on linear information inequalities and linear rank inequalities [8]. We cope, in this study and in previous research, with a question of Dougherty et al. that is related to the completeness of the CI method [8]. This question led us to consider Abelian secret sharing schemes and to study the relations of those sharing schemes with linear secret sharing schemes [18]. The latter type of schemes has been profusely studied in the related literature (see [1] and references therein). We introduced the notions of Abelian random variable, Abelian secret sharing scheme, and Abelian capacity. We cannot find those exact notions in the previous literature. However, the idea of Abelian secret sharing is implicit in many previous studies related to secret sharing. The very basic idea of using Abelian groups to construct secret sharing schemes occurs many times in the research on *homomorphic secret sharing schemes* (see [2] and references therein). We say that a secret sharing scheme is homomorphic, if and only if, the secret and the shares are elements of suitable algebraic structures, and all the functions used in the scheme are homomorphisms (i.e., the functions that compute the shares, and the function that reconstructs the secret from the shares are homomorphisms). Homomorphic schemes are important in the construction of voting protocols and some other types of multiparty protocols [2]. Liu and Zhou studied the construction of homomorphic secret sharing schemes over cyclic groups [14]. Those authors were able to characterize the access structures that admit *ideal homomorphic secret sharing schemes* over cyclic groups. Recall that a secret sharing scheme is ideal, if and only if, it achieves the best possible *information ratio*, which is as a matter of fact equal to 1 (for the definition and characterization of ideal schemes see [3] and references therein).

It is important to stress that most of the aforementioned studies focus on cyclic groups. Desmedt and Fraenkel consider secret sharing schemes over general Abelian groups [5]. However, they did not construct secret sharing schemes using the pure algebraic structure of those groups. They used the algebra of finite Abelian groups to construct scrambled versions of Shamir's scheme [6]. Those scrambled versions of Shamir's scheme are linear schemes that hold a further property, namely, zero-knowledge [7]. We would like to stress that the sharing schemes constructed by Desmedt and Fraenkel are not Abelian schemes. We define Abelian secret sharing schemes as the secret sharing schemes that can be entirely constructed from a tuple of group homomorphisms defined over the same Abelian group. We use the term Abelian arrangement to designate those tuples. Abelian arrangements naturally occur in the representation theory of entropic vectors [4]. If we say that the secret sharing scheme D is obtained from the Abelian arrangement A, then the connection is transparent, since A is nothing less than a full set of assembly instructions for D: A includes all the details and all the mappings that are necessary for the construction of A. The sharing schemes of Desmedt and Fraenkel cannot be represented this way over the Abelian groups that are used in the construction. Those sharing schemes are linear schemes that can be represented over vector spaces, which in turn are constructed from the groups using tensor products.

We would say that our goal is to establish the superiority of Abelian schemes. We would like to find Abelian schemes that outperform all their linear counterparts. It could happen that this separation cannot be achieved with ideal schemes. Therefore, we cannot focus on ideal schemes and much less on access structures that are known to admit linear ideal schemes. Most of the previous studies on homomorphic secret sharing using groups focus on ideal secret sharing schemes [14]. Desmedt and Fraenkel focus on ideal schemes over threshold access structures [3]. It is well-known that those access structures admit ideal schemes that are linear.

Remark 1. We are obligated to mention the work of Jafari and Khazaei [13]. Jafari and Khazaei studied Abelian sharing in its full generality. Those authors arrived to the notion of Abelian sharing at the same time as us, independently, and motivated by different questions.

We have to observe that linear secret sharing schemes constitute a subset of the set of Abelian secret sharing schemes (any vector space is an Abelian group). Thus, if we are asked to provide examples of Abelian schemes, we can pick any linear scheme and present it as the requested example. However, we would like to remark that we do not know the construction of a nonlinear scheme based on Abelian groups. We study along the text a construction that is based on Chinese remaindering, which gets close to be a secret sharing scheme [19]. We discuss this construction in some depth and we show that it does not provide perfect secrecy.

The remainder of this article is organized into seven sections. In Section 1, we introduce linear polymatroids and linear random variables. In Section 2, we introduce the CI method and we use it to derive Ingleton inequality. In Section 3, we introduce a formal description of the CI method as an algorithm. In Section 4, we introduce Abelian polymatroids and Abelian random variables. We show that those random variables satisfy the linear inequalities that can be derived using the CI method. We conclude that tuples of random variables that violate some linear rank inequalities are witnesses of the conjectured incompleteness of the CI method. In Section 5, we introduce Abelian secret sharing. We begin in this section the search for Abelian secret sharing schemes that cannot be represented as linear schemes. In section 6 we study the connections between Abelian secret sharing, the existence of nonlinear schemes, and the completeness of the CI method complete. We finish in Section 7 asking some questions and sketching some concluding remarks.

2 Linear polymatroids and linear random variables

We introduce the notions of linear polymatroid, linear rank inequality, and linear random variable. All those notions are closely related to each other.

Definition 2. A function $h : (\wp([n]) - \varnothing) \to \mathbb{R}^+$ is a *polymatroid*, if and only if, it satisfies all Shannon information inequalities [22].

Polymatroids are abstract objects but some of them have concrete representations by entropies of random variables. We say that those latter polymatroids are *entropic polymatroids*. The set of all entropic polymatroids encodes the solutions to all communication problems one can figure out. The entropic vectors that admit algebraic representations are of special interest. We are interested in linear polymatroids. Those are the polymatroids that can be represented by linear spaces, and those are the polymatroids that encode solutions to communication problems that entirely depend on linear algebra.

Definition 3. A linear polymatroid of order n is a polymatroid $h : (\wp([n]) - \varnothing) \to \mathbb{R}^+$ for which there exists a tuple $(V, \pi_1, \ldots, \pi_n)$ such that:
(1) V is a finite vector space.
(2) $\pi_1, \ldots, \pi_n$ are linear maps with domain V.
(3) For all $I \in (\wp([n]) - \varnothing)$ the equality

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

holds.

Linear polymatroids come from linear random variables.

Definition 4. Let $(V, \pi_1, \ldots, \pi_n)$ be a tuple as above, let X_V be a random variable that is uniformly distributed over V, and let $X_1, \ldots, X_n$ be the random variables that are induced by X_V over the quotients $\frac{V}{\ker(\pi_1)}$, $\frac{V}{\ker(\pi_2)}, \ldots, \frac{V}{\ker(\pi_n)}$. We say that the tuple $(X_V, X_1, \ldots, X_n)$ is a tuple of linear random variables, and any tuple of linear random variables is constructed in this way from a suitable tuple of linear maps.

Notation 5. The symbol $H(X_I)$ denotes the joint entropy of the tuple $(X_i)_{i\in I}$.

We have the following basic result [16]:

Theorem 6. *Let $(X_V, X_1, \ldots, X_n)$ be a tuple of linear random variables, the function $h : (\wp([n]) - \varnothing) \to \mathbb{R}^+$ that is defined by*

$$h(I) = H(X_I),$$

is a linear polymatroid, and all linear polymatroids have entropic representations.

We obtain that linear polymatroids are the entropic vectors of tuples of linear random variables. Those polymatroids constitute a subset of the set of entropic vectors, satisfy all linear inequalities satisfied by those vectors, and satisfy some additional inequalities that are specific for the linear world.

Notation 7. Let $\mathbb{F}$ be a field, and let $v, w \in \mathbb{F}^k$. We use the symbol $\langle v|w\rangle$ to denote the *scalar product* of v and w, which is defined by

$$\langle v|w\rangle = v_1w_1 + v_2w_2 + \ldots + v_kw_k,$$

where the arithmetical operations are computed on $\mathbb{F}$.

We write $h(i)$ instead of $h(\{i\})$, whenever h is a polymatroid and i is an element of its domain. Moreover, if $I, J \subset [n]$, we write IJ instead of $I \cup J$.

Definition 8. (Linear rank inequalities). *Linear rank inequalities are the linear inequalities satisfied by the entropic vectors of linear random variables, that is*: a linear rank inequality of order n is a vector $v \in \mathbb{R}^{2^n-1}$ such that for all linear polymatroids $h \in \mathbb{R}^{2^n-1}$ the inequality $\langle h|v\rangle \geq 0$ holds.

The class of linear rank functions is a well-known class of functions coming from *matroid theory* and representation theory (see [20] and references therein).

Definition 9. A linear rank function of order n is a function $r : (\wp([n]) - \varnothing) \to \mathbb{R}^+$ that admits a linear representation. A linear representation of r is a tuple $(V, V_1, \ldots, V_n)$ that satisfies the following conditions:
(1) V is a finite vector space and $V_1, \ldots, V_n$ are subspaces of V.
(2) For all $I \in (\wp([n]) - \varnothing)$, the equality

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

holds.

Notation 10. Let $A \subset R^k$, we use the symbol $ch(A)$ to denote the convex hull of A.

We use the symbol $\mathcal{LRF}_n$ to denote the set of linear rank functions of order n, and we use the symbol $\mathcal{LP}_n$ to denote the set of linear polymatroids of order n.

We have [16]:

Theorem 11. *Let $n \geq 0$, the following facts hold true*:
(1) *The equality $ch(\mathcal{LRF}_n) = ch(\mathcal{LP}_n)$ holds.*
(2) *The set of linear rank inequalities of order n is equal to the set of linear inequalities that are satisfied by linear rank functions of the same order, that is*: *linear rank inequalities are the inequalities satisfied by dimensions of vector spaces.*

Definition 12. We use the symbol $\mathcal{L}_n$ to denote the set

$$\{v \in \mathbb{R}^{2^n-1} : v \text{ is a linear rank inequality}\},$$

and we say that it is the linear region of order n.

It is easy to check that $\mathcal{L}_n$ is a convex cone. It can also be checked that $\mathcal{L}_3$ is equal to the set of Shannon inequalities over three variables, which in turn is equal to the set of *linear information inequalities* over the same number of variables [16]. However, the symmetry is lost at $n = 4$:
(1) The set $\mathcal{L}_4$ is a polyhedral cone spanned by Shannon inequalities plus six non-Shannon inequalities called *Ingleton inequalities*. We use the symbol Γ_n to denote the polyhedral cone spanned by the Shannon inequalities over n variables. We obtain that $\Gamma_4 \subset \mathcal{L}_4$.
(2) Matuš proved that given $n \geq 4$ the set of linear information inequalities over n random variables is not polyhedral [15]. We obtain that $\mathcal{L}_4 \subset \mathcal{I}_4$, where $\mathcal{I}_4$ is the set of *linear information inequalities* over four random variables.

The linear region of order five is a polyhedral cone [8]. However, the geometrical complexity of the linear cones seems to grow dramatically with n:
(1) The cone $\mathcal{L}_5$ is spanned by several thousands of extreme rays [8].
(2) Dougherty reported on the existence of more than a billion of non-Shannon linear rank inequalities of order six, which are independent, and which do not span the linear region of order six [9].

Thus, it is natural to ask: Are the linear regions polyhedral cones?

3 Ingleton inequality and the CI method

We introduce, in this section, *the CI method* [8]. We use this method to prove that there exist non-Shannon inequalities that are satisfied by all linear polymatroids or, equivalently, by all linear rank functions.

Definition 13. Given random variables $X_1, \dots, X_n$ and given two sets $I, J \subseteq [n]$, a CI for X_I and X_J is a random variable Y such that:
- $H(Y|X_I) = H(Y|X_J) = 0$ and
- $H(Y) = H(X_I) + H(X_J) - H(X_{IJ})$.

Gács and Körner proved that CI are not common: most pairs of random variables do not have CI [10]. On the other hand, linear random variables do have CI:

Theorem 14. *Let $(X_V, X_1, \dots, X_n)$ be a tuple of linear random variables, and let $I, J \subseteq [n]$. The joint random variables X_I, X_J have CI.*

Proof. Suppose that $(X_V, X_1, \dots, X_n)$ is determined by the tuple $(V, \pi_1, \dots, \pi_n)$. Set $W = \langle \bigcup_{k \in IJ} \ker(\pi_k) \rangle$, and let $X_{I,J}$ be equal to the random variable that is induced by X over the quotient $\frac{V}{W}$. It is easy to check that $X_{I,J}$ is the CI of X_I and X_J. □

Notation 15. Let $n \geq 1$, we use the set $\{I : I \in \wp([n]) - \varnothing\}$ as the set of indices of the canonical basis of $\mathbb{R}^{2^n-1}$. We use this labeling of the canonical basis to express an entropic vector $(H(X_I))_{I \subseteq [n]}$ as a linear combination $\sum_{I \subseteq [n]} H(X_I) \cdot e_I$.

Definition 16. (Ingleton vector) The Ingleton vector is the 15-dimensional vector:

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

Theorem 17. *The Ingleton vector is a linear rank inequality, that is: for all linear rank functions of order 4, say the function f, the inequality $\langle \mathcal{I} | f \rangle \geq 0$ holds.*

Proof. Let α be equal to the vector

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

It can be checked that α encodes a Shannon inequality that holds for all the entropic polymatroids of order 5. Let $\mathcal{V} = (V, \pi_1, \dots, \pi_4)$ be a linear tuple, and let $(X_V, X_1, \dots, X_4)$ be the associated tuple of linear random variables. We suppose that X_5 is a CI of X_1 and X_2. We have that

$$-(H(X_{1,2,3}) + H(X_{1,2,4}) + H(X_{3,4}) + 2H(X_1) + 2H(X_2) + H(X_5)) + H(X_{1,3}) + H(X_{1,4}) + H(X_{2,3}) + H(X_{2,4}) + 2H(X_{1,5}) + 2H(X_{2,5}) \geq 0.$$

If we use the hypothesis (X_5 is the CI of X_1 and X_2), we obtain that

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

The theorem is proved. □

It can be checked that Ingleton's inequality is not spanned by Shannon inequalities [22]. Thus, given $n \geq 4$, the linear region $\mathcal{L}_n$ is not equal to the set of *Shannon inequalities* of order n.

Remark 18. One can obtain six different linear rank inequalities from the vector $\mathcal{I}$. Those six inequalities can be obtained from $\mathcal{I}$ by suitably permuting the variables $X_1, \ldots, X_4$.

Note that the above proof entails a method for generating linear rank inequalities. This method is called *the CI method*.

4 The CI method

Let h be a linear polymatroid of order n, let $(V, \pi_1, \ldots, \pi_n)$ be a linear representation of h, and let $(X_V, X_1, \ldots, X_n)$ be the tuple of linear random variables determined by this representation. Given $I, J \subseteq [n]$, the random variables X_I and X_J have CI. This fact is the basis of the CI method.

Definition 19. Let $n \geq 1$, let $J, K \subseteq [n]$, and let $v = \sum I \subseteq [n+1] a_I e_I$ be a linear rank inequality of order $n+1$. The vector v belongs to $\Delta^{n+1}_{J,K} \subset \mathcal{L}_{n+1}$, if and only if, the following two conditions are satisfied:
(1) Let $R \subseteq [n+1]$, and suppose that $a_R \neq 0$ and $\{n+1\} \subset R$. Then,

$$R \in \{J \cup \{n+1\}, K \cup \{n+1\}, \{n+1\}\}.$$

(2) The equalities

$$a_{J\{n+1\}} = a_J,\ a_{K\{n+1\}} = a_K \quad \text{and} \quad a_{\{n+1\}} = a_J + a_K - a_{JK}$$

hold.

Observe that we use a linear projection from $\mathcal{L}_5$ to $\mathcal{L}_4$ to obtain Ingleton inequality. The set $\Delta^{n+1}_{J,K}$ is constituted by linear rank inequalities of order $n+1$ to which we can apply a similar projection. Let us define this projection:

Definition 20. Given $v \in \Delta^{n+1}_{J,K}$, we define $T^{n+1}_{J,K}(v) = \sum_{I \subseteq [n]} a^*_I e_I$, where

$$a^*_I = \begin{cases} a_J + a_{J\{n+1\}} + a_{\{n+1\}}, & \text{if } I = J \\ a_K + a_{K\{n+1\}} + a_{\{n+1\}}, & \text{if } I = K \\ a_{JK} - a_{\{n+1\}}, & \text{if } I = J \cup K \\ a_I, & \text{otherwise}. \end{cases}$$

Note that for all $J, K \subseteq [n]$ the function $T^{n+1}_{J,K}$ is a linear map. Those linear maps are the projections that are employed in the CI method. Next theorem asserts that given $v \in \Delta^{n+1}_{J,K}$, the vector $T^{n+1}_{J,K}(v)$ is a linear rank inequality of order n. This is the mathematical core of the method.

Theorem 21. *Suppose that $v \in \Delta^{n+1}_{J,K}$, we have that $T^{n+1}_{J,K}(v) \in \mathcal{L}_n$.*

Proof. Let $v \in \Delta^{n+1}_{J,K}$ and suppose that $T^{n+1}_{J,K}(v) \notin \mathcal{L}_n$. There exists a tuple of linear random variables $\overrightarrow{X} = (X_V, X_1, \ldots, X_n)$, such that $\langle h_{\overrightarrow{X}}, T^{n+1}_{J,K}(v) \rangle < 0$. Consider the tuple $\overrightarrow{Y} = (X_V, X_1, \ldots, X_n, X_{n+1})$, where X_{n+1} is a CI of X_I and X_J. It is easy to check that the equality $\langle h_{\overrightarrow{Y}}, v \rangle = \langle h_{\overrightarrow{X}}, T^{n+1}_{J,K}(v) \rangle$ holds. It implies that $\langle v, h_{\overrightarrow{Y}} \rangle < 0$. Then, we have that v is not a linear rank inequality, but this is a contradiction. The theorem is proved. □

Example 22. (Ingleton inequality) Let α be equal to

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

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

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

It follows from Theorem 21 that the vector $T^5_{\{1\},\{2\}}(\alpha)$ is a linear rank inequality. Note that this linear rank inequality is the aforementioned Ingleton inequality [11], which was the first ever discovered non-Shannon inequality that holds for all linear polymatroids.

Let $\mathcal{ICI}$ be the set of linear inequalities that are satisfied by the tuples of random variables that have CI. The above method can be easily turned into an algorithm that recursively enumerates a spanning set for $\mathcal{ICI}$ (see [16]). Dougherty et al. used this algorithm to produce a spanning set for the cone $\mathcal{L}_5$, a spanning set that is constituted by several thousands of linear rank inequalities [8]. Dougherty et al. used the same algorithm to search for linear rank inequalities over six variables, and he reported on the discovering of more than one billion of those inequalities, which are independent and which do not span the cone $\mathcal{L}_6$ (see [9]). Dougherty et al. asked the following two questions [8]:

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

We consider that those two questions are the most important open problems related to the structure of the linear regions. From now on we focus on the second question. We attack this question using the following strategy:

(1) We detect a class of random variables that contain all the linear random variables. We use the term Abelian random variables to designate this new type of random variables.
(2) We prove that Abelian random variables have CI.
(3) We investigate the following question: Does there exist a linear rank inequality that is violated by a suitable tuple of Abelian random variables?

Linear random variables come from vector spaces. Then, if we want to detect a larger set of random variables, we can try with a larger set of algebraic structures that behave similar to vector spaces. Abelian groups constitute a possible choice. We prove that the random variables determined by Abelian groups have CI. Then, we cope with the question about the existence of a linear rank inequality that is violated by Abelian variables. We use the theory of secret sharing schemes to deal with this latter question.

5 Abelian polymatroids and Abelian random variables

We know that entropic polymatroids can be suitably represented by group arrangements [4]. What are the entropic polymatroids that can be represented using Abelian groups?

Definition 23. An *Abelian arrangement* of order n is a tuple $\mathcal{G} = (G, \pi_1, \ldots, \pi_n)$ such that:

(1) G is a finite Abelian group.
(2) π_i is a group homomorphism with domain G.

Given an Abelian arrangement $\mathcal{G}$, it determines a polymatroid of order n that is denoted by the symbol $h_{\mathcal{G}}$, and such that for each $I \subseteq [n]$ the equality

$$h_{\mathcal{G}}(I) = \log\left(\left|\frac{G}{\bigcap_{i\in I} \ker(\pi_i)}\right|\right)$$

holds. We say that $h_{\mathcal{G}}$ is an *Abelian polymatroid*, and we say that $\mathcal{G}$ is an *Abelian representation* of $h_{\mathcal{G}}$.

Definition 24. Given an Abelian arrangement $\mathcal{G} = (G, \pi_1, \ldots, \pi_n)$, we use the symbol X_G 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 that is induced by X_G over the quotient $\frac{G}{\ker(\pi_i)}$. Set $X_{\mathcal{G}} = (X_G, X_1, \ldots, X_n)$. We say that $X_{\mathcal{G}}$ is a *tuple of Abelian random variables*.

Remark 25. A reviewer pointed out to us that the notions of Abelian arrangement and Abelian random variable can be entirely given in terms of subgroups. Note that all that we use of π_i is the subgroup $\ker(\pi_i)$. Note that the same is true of linear arrangements and linear random variables. It could be more natural to think in substructures instead of homomorphisms but we prefer to stick with this presentation. We do this since we want to use algebraic arrangements to construct secret sharing schemes. And it happens that the mappings that constitute our arrangements are all the mappings that we use in the secret sharing schemes that we extract from those algebraic arrangements.

We prove that Abelian variables have CI. We need a famous lemma from group theory that is called The Product Lemma.

Lemma 26. *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 $P = K \times R$. Note that $|P| = |K||R|$. Let $\phi : P \to \langle K \cup R\rangle$ be the homomorphism defined by $\phi(x, y) = xy$. Note that $\ker(\phi)$ is equal to the set

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

We obtain that $|\langle K \cup R\rangle| = \frac{|K||R|}{|R \cap K|}$. □

Theorem 27. *Abelian random variables have CI.*

Proof. Let $\mathcal{X}_{\mathcal{G}} = (X_G, X_1, \ldots, X_n)$ be an Abelian tuple, and let $\mathcal{G} = (G, \pi_1, \ldots, \pi_n)$ be an Abelian arrangement that defines the tuple $\mathcal{X}_{\mathcal{G}}$. Pick $I \subseteq [n]$, we have 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_G over the quotient $\frac{G}{\bigcap_{i\in I} \ker(G_i)}$.

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

- $I(X_I : X_J) = H(Z)$,
- $H(Z|X_I) = H(Z|X_J) = 0$.

To this end, we define a subgroup $L \trianglelefteq G$ such that Z is the random variable induced by X over $\frac{G}{L}$. The second condition on Z indicates that $\bigcap_{i\in I} \ker(\pi_i)$ and $\bigcap_{i\in J} \ker(\pi_i)$ must be contained in L, while the first condition suggests that L must be as small as possible. We set $L = \langle((\bigcap_{i\in I} \ker(\pi_i)) \cup (\bigcap_{i\in J} \ker(\pi_i))\rangle$. Let $K = \bigcap_{i\in I} \ker(\pi_i)$ and $R = \bigcap_{i\in J} \ker(\pi_i)$. We have

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

It is easy to check that $H(Z|X_I) = H(Z|X_J) = 0$. □

Definition 28. We use the symbol $\mathcal{AP}_n$ to denote the set of Abelian polymatroids of order n.

We have $\mathcal{LP}_n \subseteq \mathcal{AP}_n$: any linear polymatroid is an Abelian polymatroid. On the other hand, we have:

Proposition 29. *There exist Abelian polymatroids that are not linear.*

Proof. Let M, N be two linear matroids of the same order. We can suppose that M does not have linear representations over fields of characteristic two. We can also suppose that N does not have linear representations over fields whose characteristic is odd [20].

Let $(V, \pi_1, \dots, \pi_n)$ and $(W, \sigma_1, \dots, \sigma_n)$ be linear representations of the above two matroids, and let $h_{\mathcal{V}}$, $h_{\mathcal{W}}$ be the corresponding linear polymatroids. We set $G = V \times W$, and given $i \leq n$ we define a function

$$\pi_i \times \sigma_i : V \times W \to \mathrm{Im}(\pi_i) \times \mathrm{Im}(\sigma_i)$$

by means of the equation

$$(\pi_i \times \sigma_i)(g, h) = (\pi_i(g), \sigma_i(h)).$$

The product $(G, \pi_1 \times \sigma_1, \dots, \pi_n \times \sigma_n)$ is an Abelian arrangement, and we have that $h_{\mathcal{G}} = h_{\mathcal{V}} + h_{\mathcal{W}}$. We obtain that $h_{\mathcal{V}} + h_{\mathcal{W}} \in \mathcal{AP}_n$ and $h_{\mathcal{V}} + h_{\mathcal{W}} \notin \mathcal{LP}_n$. The proposition is proved. □

We would like to prove that there exists a linear inequality that is satisfied by the elements of $\mathcal{LP}_n$ but which is not satisfied by some element of $\mathcal{AP}_n$. We know that $\mathcal{LP}_n \subset \mathcal{AP}_n$. However, this is not enough: we have to prove that $ch(\mathcal{AP}_n) \subset ch(\mathcal{LP}_n)$. How can we prove this? The sets $ch(\mathcal{AP}_n)$ and $ch(\mathcal{LP}_n)$ are convex cones. Then, if the containment is strict those two sets are separated by a linear program. We introduced *Abelian sharing* in our search for those linear problems [16].

6 Abelian secret sharing

Secret sharing schemes are used in secure multiparty computation to distribute shares of a secret into a set of parties. Secret sharing schemes must satisfy some basic requirements:
(1) The secret can be reconstructed from the shares.
(2) No information about the secret can be computed from small sets of shares.

Let us consider an important example of secret sharing scheme.

6.1 Shamir's secret sharing scheme

Suppose that we want to distribute a secret $w \in \{0, 1\}^l$ between a set of m parties. Let $n < m$, and let $U_{n,m}$ be the set

$$\{I \subseteq [m] : |I| \geq n\}.$$

We would like to share the secret w in such a way that:
(1) The secret can be reconstructed from any set of n different shares.
(2) $n - 1$ shares convey zero information about w.

Let us proceed, but let us first introduce the basic definitions of access structure and secret sharing scheme.

Definition 30. An access structure over m parties is a set $C \subset \mathcal{P}(\{1, \dots, m\})$ that is upward closed, that is: let $I \subset J \subseteq \{1, \dots, m\}$ and suppose that $I \in C$, we obtain that $J \in C$.

An access structure C determines a collection of large *authorized sets*.

Example 31. The set $U_{n,m}$ is an example of an access structure over a set of n parties. We say that $U_{n,m}$ is a threshold access structure since the condition that determines which sets of parties are the authorized sets is given by the threshold n.

Recall that we want to construct a secret sharing scheme for the access structure $U_{n,m}$. Let $\mathbb{F}$ be a finite field whose size is larger than $\max\{m+1, 2^l\}$. Note that $\{0,1\}^l$ can be embedded in $\mathbb{F}$. We can fix such an embedding, and we can assume that the secret to be distributed is an element a of the set $\mathbb{F}\setminus\{0\}$. The m shares of a are the images of this field element under a suitable set of m functions.

Definition 32. Let $\mathcal{V} = (V \times W, \pi_1, \ldots, \pi_m, \pi_{m+1})$ be a linear arrangement and let $h_{\mathcal{V}}$ be the linear polymatroid determined by $\mathcal{V}$. We say that $\mathcal{V}$ is a **Linear secret sharing scheme** *for* C, if and only if, the following two conditions are satisfied.

(1) **Perfect recovery**. For all $I \in C$ the equality

$$h_{\mathcal{V}}(I \cup \{m+1\}) = h_{\mathcal{G}}(I)$$

holds.

(2) **Perfect secrecy**. For all $I \notin C$ the equality

$$h_{\mathcal{V}}(I \cup \{m+1\}) = h_{\mathcal{G}}(I) + h_{\mathcal{G}}(m+1)$$

holds.

Let $a \in \mathbb{F}\setminus\{0\}$ be the secret, and let $a_1, \ldots, a_m$ be m different nonzero elements of $\mathbb{F}$ that are known by the m parties. The dealer can use linear algebra over $\mathbb{F}$ to construct a linear secret sharing scheme for the access structure $U_{n,m}$. First of all, she chooses uniformly at random $b_{n-2}, \ldots, b_0 \in \mathbb{F}$. She keeps secret this tuple, and then she computes the linear array

$$\mathcal{S}_{a,\mathbf{b}} = (V \times W, ev_1, \ldots, ev_m, ev_{m+1}),$$

where:

(1) V is the subspace of $\mathbb{F}[X]$ spanned by X^{n-1}. Note that V is isomorphic to $\mathbb{F}$.

(2) W is the subspace of $\mathbb{F}[X]$ spanned by $X^0, \ldots, X^{n-2}$.

(3) Given $i \leq m$ the linear map $ev_i : V \times W \to F$ is defined by

$$ev_i(a, b_{n-2}, \ldots, b_0) = aa_i^{n-1} + b_{n-2}a_i^{n-2} + \cdots + b_1a_i + b_0.$$

(4) Function $ev_{m+1} : V \times W \to V$ is equal to the linear map

$$ev_{m+1}(a, b_{n-2}, \ldots, b_0) = a.$$

Then, she uses this linear array to distribute the secret a. To do this she proceeds as follows:

(1) The dealer knows the polynomial

$$p_{a,\mathbf{b}}(X) = aX^{n-1} + b_{n-2}X^{n-2} + \cdots + b_1X + b_0,$$

and she also knows that $ev_{m+1}(p_{a,\mathbf{b}}(X)) = a$.

(2) The dealer uses the above polynomial to compute the shares $ev_1(p_{a,\mathbf{b}}), \ldots, ev_m(p_{a,\mathbf{b}})$: she evaluates the functions $ev_1, \ldots, ev_m$ at the vector $p_{a,\mathbf{b}}(X) \in ev_{m+1}^{-1}(p_{a,\mathbf{b}}(X))$.

(3) **Perfect recovery**. If we know n shares, we know n points in the graph of $p_{a,\mathbf{b}}(X)$, and we know the polynomial. Then, we can compute the secret $ev_{m+1}(p_{a,\mathbf{b}}(X))$. Thus, if we know $p_{a,\mathbf{b}}(X)$ the reconstruction of the secret reduces to evaluate ev_{m+1} at this vector.

(4) **Perfect secrecy**. If we know $n-1$ shares, we know no more than $n-1$ points in the graph of $p_{a,\mathbf{b}}(X)$. Let S be this set of $n-1$ points and let $b \in \mathbb{F}$. We use the symbol $\Pr(b|S)$ to denote the probability that b is the leading coefficient of $p_{a,\mathbf{b}}(X)$ given that the graph of $p_{a,\mathbf{b}}(X)$ contains the set S. It is easy to check that $\Pr(b|S) = \frac{1}{|\mathbb{F}|}$. This means that, if we know no more than $n-1$ shares, we know nothing about the secret a.

Note that Shamir's key idea gives us a mechanism to construct secret sharing schemes from linear arrangements that behave as the arrangement $\mathcal{S}_{a,\mathbf{b}}$ [12]. We can do the same with Abelian arrangements that behave similar to $\mathcal{S}_{a,\mathbf{b}}$. In the next section, we explore this possibility and we determine the conditions under which an Abelian arrangement $\mathcal{G}$ encodes a secret sharing scheme for an access structure C.

6.2 Abelian secret sharing schemes

Let

$$\mathcal{G} = (G, \pi_1, \dots, \pi_m, \pi_{m+1})$$

be an Abelian arrangement. We can use $\mathcal{G}$ to distribute m shares of a secret that belongs to the set $\frac{G}{\ker(\pi_{m+1})}$. We use the symbol $\Sigma_{\mathcal{G}}$ to denote this mechanism. Mechanism $\Sigma_{\mathcal{G}}$ works as follows:

(1) Set $S = \frac{G}{\ker(\pi_{m+1})}$.
(2) Let $s \in S$ be the secret.
(3) The secret dealer computes $g \in G$ such that $\pi_{m+1}(g) = s$.
(4) Given $i \leq m$, the secret dealer computes $\pi_i(g)$ and communicates this share to party i. Thus, the shares of s are $\pi_1(g), \dots, \pi_m(g)$.

Remark 33. Note that in the above distribution mechanism, the dealer does not use something extra to the group structure encoded by $\mathcal{G}$. She only has to compute $\pi_{m+1}^{-1}(s)$ and the tuple $(\pi_1(\pi_{m+1}^{-1}(s)), \dots, \pi_m(\pi_{m+1}^{-1}(s)))$.

Definition 34. We say that $\mathcal{G} = (G, \pi_1, \dots, \pi_m, \pi_{m+1})$ is an **Abelian distribution scheme** *for* C, if and only if, for all $I \in C$ the equality

$$h_{\mathcal{G}}(I \cup \{m+1\}) = h_{\mathcal{G}}(I)$$

holds.

Example 35. Let us consider an elementary example of an Abelian distribution scheme for the threshold structure $U_{2,2}$. Let p, q be two large primes that are close to each other. We use the symbol $D_{ch,p,q}$ to denote the Abelian distribution scheme (G, π_1, π_2, π_3), where:

(1) $G = \mathbb{Z}_{p^2q^2}$.
(2) π_1 is the projection of G onto $\frac{\mathbb{Z}_{p^2q^2}}{\mathbb{Z}_{q^2}}$.
(3) π_2 is the projection of G onto $\frac{\mathbb{Z}_{p^2q^2}}{\mathbb{Z}_{p^2}}$.
(4) π_3 is the projection of G onto $\frac{\mathbb{Z}_{p^2q^2}}{\mathbb{Z}_{pq}}$.

Let $a \in \{0, \dots, pq-1\}$ be the secret. The dealer chooses a random g such that g is equal to $lpq + a$ for some l. Then, the dealer computes b, c such that for some s and t the equalities

$$g = sq^2 + b = tp^2 + c$$

hold. Then, she sends share b to party 1 and share c to party 2.

Let us see that $D_{ch,p,q}$ provides perfect recovery. The single authorized set is the set $\{1, 2\}$. The shares given to the members of this coalition are b and c. We have that there exists a unique $g \in G$, such that

$$\pi_1(g) = b \quad \text{and} \quad \pi_2(g) = c.$$

This g can be computed from b and c using Chinese remaindering. Moreover, the secret $\pi_3(g)$ can be easily computed from g. We obtain that $D_{ch,p,q}$ is an Abelian distribution scheme.

Perfect recovery does not suffice for applications. We need perfect secrecy:

Definition 36. We say that $\mathcal{G} = (G, \pi_1, \ldots, \pi_m, \pi_{m+1})$ is an **Abelian secret sharing scheme** *for* C, if and only if, $\mathcal{G}$ is an Abelian distribution scheme and for all $I \in C$ the equality

$$h_{\mathcal{G}}(I \cup \{m+1\}) = h_{\mathcal{G}}(I)$$

holds.

Let C be an access structure over m parties. Next theorem provides us with a characterization of the Abelian arrangements that yield secret sharing schemes for C.

Theorem 37. *Let $\mathcal{G} = (G, \pi_1, \ldots, \pi_m, \pi_{m+1})$ be an Abelian arrangement, we have*:
(1) *$\mathcal{G}$ provides perfect recovery, if and only if, for all $I \in C$ the inclusion $\bigcap_{i\in I} \ker(\pi_i) \subseteq \ker(\pi_{m+1})$ holds.*
(2) *$\mathcal{G}$ provides perfect secrecy, if and only if, for all $I \notin C$ the equalities*

$$\left|\frac{G}{\bigcap_{i\in I}\ker(\pi_i)}\right| = \left|\frac{\ker(\pi_{m+1})}{(\bigcap_{i\in I}\ker(\pi_i)) \cap \ker(\pi_{m+1})}\right|$$

and

$$\left|\frac{G}{\ker(\pi_{m+1})}\right| = \left|\frac{\bigcap_{i\in I}\ker(\pi_i)}{(\bigcap_{i\in I}\ker(\pi_i)) \cap \ker(\pi_{m+1})}\right|$$

both hold.

Proof. Let us prove the second item, the proof of the first item is easy and we omit it.

Let us suppose that $\mathcal{G}$ provides secrecy and let us suppose that $I \notin C$. We have that

$$\begin{aligned} h_{\mathcal{G}}(I \cup \{m+1\}) &= \log\left(\left|\frac{G}{(\bigcap_{i\in I}\ker(\pi_i)) \cap \ker(\pi_{m+1})}\right|\right) \\ &= \log\left(\left|\frac{G}{(\bigcap_{i\in I}\ker(\pi_i))}\right|\right) + \log\left(\left|\frac{G}{\ker(\pi_{m+1})}\right|\right) \\ &= h_{\mathcal{G}}(I) + h_{\mathcal{G}}(m+1). \end{aligned}$$

We obtain that

$$\left|\frac{G}{(\bigcap_{i\in I}\ker(\pi_i)) \cap \ker(\pi_{m+1})}\right| = \left|\frac{G}{(\bigcap_{i\in I}\ker(\pi_i))}\right|\left|\frac{G}{\ker(\pi_{m+1})}\right|,$$

and also that both equalities in the statement of the theorem hold.

Let us prove the converse. Consider the group homomorphism $\pi : G \to \prod_{i\in I}\mathrm{Im}(\pi_i) \times \mathrm{Im}(\pi_{m+1})$, which is defined by

$$\pi(g) = ((\pi_i(g))_{i\in I}, \pi_{m+1}(g)).$$

We have that:
(1) $\ker(\pi) = (\bigcap_{i\in I}\ker(\pi_i)) \cap \ker(\pi_{m+1})$.
(2) The size of $\mathrm{Im}(\pi)$ is a subset of $\prod_{i\in I}\mathrm{Im}(\pi_i) \times \mathrm{Im}(\pi_{m+1})$, and the size of this subset is equal to $|\prod_{i\in I}\mathrm{Im}(\pi_i) \times \mathrm{Im}(\pi_{m+1})|$.

We obtain that π is onto, and we obtain that for all $k \in K$ and for all $h \in H$ there exists $x_{kh} \in G$ such that $k = [x_{kh}]_K$ and $h = [x_{kh}]_H$. Moreover, we obtain that for all pair (k, h) the number of solutions is the same. Altogether, we obtain that

$$h_{\mathcal{G}}(I \cup \{m+1\}) = H(X_{I\{m+1\}}) = H(X_{I\{m+1\}}) = h_{\mathcal{G}}(I),$$

and the theorem is proved. □

Example 38. Let us continue with the analysis of $D_{ch,p,q}$. Is $D_{ch,p,q}$ an Abelian secret sharing scheme? It is easy to check that

$$\left|\frac{\mathbb{Z}_{pq}}{\mathbb{Z}_{pq} \cap \mathbb{Z}_{p^2}}\right| = q \neq q^2 = \left|\frac{\mathbb{Z}_{p^2q^2}}{\mathbb{Z}_{p^2}}\right|.$$

We obtain that $D_{ch,p,q}$ cannot provide perfect secrecy.

6.3 Information rates

Let $\mathcal{G}$ be a secret sharing scheme for C. The secret dealer can claim that her scheme is efficient only if the shares that she distributes are small when compared with the secret.

Definition 39. Let $\mathcal{G}$ be a distribution scheme for C. We define the **average information ratio** of $\mathcal{G}$ as the quotient

$$\sigma^*(\mathcal{G}) = \frac{\sum_{i \leq n} h_{\mathcal{G}}(i)}{m \cdot h_{\mathcal{G}}(m+1)}.$$

Example 40. Let us continue with the analysis of the Abelian distribution scheme $D_{ch,p,q}$. The entropy of the message is $\log(pq)$, and the entropies of the shares are $\log(p^2)$ and $\log(q^2)$. Thus, the average information ratio is equal to $\frac{2\log p + 2\log(q)}{2\log(pq)}$, which is in turn equal to 1.

It can be checked that the average information ratio of Shamir's scheme is equal to 1. This is the best possible information ratio for a secret sharing scheme [1]. Therefore, we say that Shamir's scheme is an ideal secret sharing scheme [3].

Definition 41. Let C be an access structure and let $\mathcal{S}$ be a secret sharing scheme for C. We say that $\mathcal{S}$ is ideal, if and only if, the average information ratio of $\mathcal{S}$ is equal to 1.

We ask: Does there exist an access structure that admit ideal Abelian schemes but which do not admit ideal linear schemes? Note that this question is closely related to the basic DFZ question.

7 Abelian secret sharing and the DFZ questions

Let us go back with the question that motivated this work: Is the CI method complete?

Definition 42. Let C be an access structure. We use the symbol $\sigma_{\mathcal{A}}(C)$ to denote the *Abelian capacity* of C, which is defined as

$$\sigma_{\mathcal{A}}(C) = \inf\{\sigma^*(\mathcal{G}) : \mathcal{G} \text{ is an Abelian secret sharing scheme for } C\}.$$

We use the symbol $\sigma_{\mathcal{L}}(C)$ to denote the *linear capacity* of C, and we use the symbol $\sigma(C)$ to denote the *capacity* of C. Those two latter capacities are defined accordingly.

Example 43. The Abelian and linear capacities of threshold structures are all equal to 1. This follows from the construction of Shamir. Note that Shamir's scheme is a linear scheme as well as an Abelian scheme. Note that any linear scheme is also an Abelian scheme.

Given an access structure C the inequalities

$$\sigma(C) \leq \sigma_{\mathcal{A}}(C) \leq \sigma_{\mathcal{L}}(C)$$

hold. We conjecture that Abelian schemes outperform linear schemes, that is: we conjecture that there exists an access structure C such that

$$\sigma_{\mathcal{A}}(C) < \sigma_{\mathcal{L}}(C).$$

Definition 44. Let C be an access structure over n parties, we use the symbol $\mathcal{AP}(C)$ to denote the subset of $\mathcal{AP}_n$ that is defined by the following $2^n - 1$ linear equalities:
(1) For all $I \in C$ the equality $h(I\{n+1\}) = h(I)$ holds.
(2) For all $I \notin C$ the equality $h(I\{n+1\}) = h(I) + h(n+1)$ holds.

We define $\mathcal{AP}(C)$ accordingly.

Note that $\mathcal{AP}(C)$ is constituted by the polymatroids that come from Abelian secret sharing schemes for C.

Definition 45. Let Ω_C be the set

$$\{e_{I\{n+1\}} - e_I : I \in C\} \cup \{e_{I\{n+1\}} - e_I - e_{n+1} : I \in C\}.$$

Let $h \in \mathbb{R}^{2^n-1}$, we have that h belongs to $\mathcal{AP}(C)$, if and only if, for all $v \in \Omega_C$ the equality $\langle v|h\rangle = 0$ holds.

Notation 46. Let us fix some notations and some terminologies:
(1) If $h \in \mathcal{AP}(C)$, we say that h is an Abelian secret sharing polymatroid for C.
(2) If $h \in \mathcal{LP}(C)$, we say that h is a linear secret sharing polymatroid for C.
(3) Let $\Omega \subset \mathbb{R}^{2^n-1}$ and let h be a polymatroid. We use the symbol $h \models \Omega$ to indicate that for all $v \in \Omega$ the equality $\langle v|h\rangle = 0$ holds. We use the symbol $h \Vdash \Omega$ to indicate that for all $v \in \Omega$ the inequality $\langle v|h\rangle \geq 0$ holds.
(4) We use the symbol $\mathcal{A}_n$ to denote the set of linear inequalities that are satisfied by all the Abelian polymatroids of order n ($\mathcal{A}_n$ denotes the Abelian region of order n).

We have.

Theorem 47. *Let C be an access structure.*
(1) $\sigma_{\mathcal{A}}(C) = \min\left\{\frac{1}{n}\sum_{i\leq n} h(i) : h(n+1) = 1 \text{ and } h \Vdash \mathcal{A}_n \text{ and } h \models \Omega_C\right\}$.
(2) $\sigma_{\mathcal{L}}(C) = \min\left\{\frac{1}{n}\sum_{i\leq n} h(i) : h(n+1) = 1 \text{ and } h \Vdash \mathcal{L}_n \text{ and } h \models \Omega_C\right\}$.

Proof. Let us write the proof for $\sigma_{\mathcal{L}}(C)$. The proof for $\sigma_{\mathcal{A}}(C)$ is completely analogous.

Let $\mathcal{ES}(C)$ be the set of linear polymatroids realizing the access structure C. The set $\mathcal{ES}(C)$ is nonempty [12]. Let $v \in \mathbb{R}^{2^n-1}$, the ray $\langle v\rangle_+$ is the set

$$\{\lambda \cdot v : \lambda > 0\}.$$

We set

$$\mathcal{RES}(C) = \{\langle v\rangle_+ : h \in \mathcal{ES}(C)\},$$

and we note that our objective function, which is the function $\frac{\sum_{i\leq n} h_{\mathcal{G}}(i)}{n \cdot h_{\mathcal{G}}(n+1)}$, is constant over any ray. We obtain that

$$\sigma_{\mathcal{L}}(C) = \inf\left\{\frac{1}{n}\sum_{i\leq n} h(i) : h(n+1) = 1 \text{ and } h \in \mathcal{RES}(C)\right\}.$$

The function $\frac{1}{n}\sum_{i\leq n}h(i)$ is a linear function. We obtain that

$$\sigma_{\mathcal{L}}(C) = \min\left\{\frac{1}{n}\sum\nolimits_{i\leq n}h(i) : h(n+1) = 1 \text{ and } h \in ch(\mathcal{RES}(C))\right\},$$

and we obtain that

$$\sigma_{\mathcal{L}}(C) = \min\left\{\frac{1}{n}\sum_{i\leq n}h(i) : h(n+1) = 1 \text{ and } h \Vdash \mathcal{L}_n \text{ and } h \vDash \Omega_C\right\}.$$

The theorem is proved. □

We obtain an easy corollary from the above theorem

Corollary 48. *If there exists an access structure C that satisfies the inequality $\sigma_{\mathcal{A}}(C) < \sigma_{\mathcal{L}}(C)$ the CI method cannot be complete.*

It remains to look for an access structure C satisfying the inequality $\sigma_{\mathcal{A}}(C) < \sigma_{\mathcal{L}}(C)$. We conjecture that such an access structure actually exists. Where can we look for good candidates?

8 Concluding remarks

We have to ask: Have we exhibited a single example of an Abelian secret sharing scheme?

Shamir's scheme constitutes a good example of an Abelian secret sharing scheme. However, the above question is a question about the existence of Abelian schemes that cannot be represented by linear maps. We say that such a scheme is a nonlinear Abelian scheme. Do there exist nonlinear Abelian secret sharing schemes? We conjecture that there exist Abelian secret sharing schemes that outperform all its linear counterparts. Note that those schemes have to be nonlinear.

8.1 Nonlinear schemes based on Chinese remaindering

In this section, we study an interesting example of a nonlinear scheme that is based on Chinese remaindering [19].

Let $p_s < p_1 < \cdots < p_n$ be $n+1$ consecutive primes, and let $t \leq n$ be a positive integer such that the inequality

$$p_s \prod_{i=n-t+2}^{n} p_i < \prod_{i=1}^{t} p_i$$

holds. Set $G = \mathbb{Z}_{p_s p_1 \cdots p_n}$, and let π_i be the map

$$\pi_i(x) = x \bmod p_i.$$

We obtain the Abelian arrangement

$$\mathcal{G}_{p_s,p_1,\ldots,p_n} = (G, \pi_1, \ldots, \pi_n, \pi_s),$$

which can be used to define an Abelian distribution scheme for n parties. This distribution scheme works as follows:

(1) The dealer chooses a secret $s \in \{1, \ldots, p_s\}$.

(2) The dealer chooses an integer α such that $s + p_s\alpha$ belongs to the interval $(\prod_{i=n-t+2}^{n} p_i, \prod_{i=1}^{t} p_i)$.

(3) Given i, the dealer computes $\pi_i(s + p_s\alpha)$ and sends it to party i. Note that the secret is equal to $\pi_s(s + p_s\alpha)$.

It is easy to prove that any set of t shares allows the perfect recovery of the secret. Is $\mathcal{G}_{p_s,p_1,\ldots,p_n}$ an Abelian secret sharing scheme for the access structure $U_{n,t}$? Not really, but we have something close: $t-2$ shares give null information about the secret [19].

8.2 Nonlinear schemes for Fano and non-Fano

Our main goal is to prove that the CI method is not complete. We have to look for an access structure C satisfying the inequality $\sigma_{\mathcal{A}}(C) < \sigma_{\mathcal{L}}(C)$. We have a candidate that we denote with the symbol $\mathcal{F}+\mathcal{NF}$. Let us define this structure.

First, we have to define two access structures $\mathcal{F}$ and $\mathcal{NF}$. The set of participants of $\mathcal{F}$ is the set $A=\{1,\ldots,6\}$, while the set of participants of $\mathcal{NF}$ is the set $B=\{7,\ldots,12\}$. The *minterms* of $\mathcal{F}$ are

$$\{1,4\},\{2,5\},\{3,6\},\{1,2,6\},\{1,3,5\},\{2,3,4\}, \text{ and } \{4,5,6\},$$

and the minterms of $\mathcal{NF}$ are

$$\{7,10\},\{8,11\},\{9,12\},\{7,8,12\},\{7,9,11\},\{8,9,10\},\{10,11,12\}, \text{ and } \{9,10,11\}.$$

The set of participants of the access structure $\mathcal{F}+\mathcal{NF}$ is the set $\{1,\ldots,12\}$. We have that $I\in\mathcal{F}+\mathcal{NF}$, if and only if, $I\cap A\in\mathcal{F}$ and $I\cap B\in\mathcal{NF}$.

Remark 49. The symbol $\mathcal{F}$ stands for Fano, while the symbol $\mathcal{NF}$ stands for non-Fano. The access structure $\mathcal{F}+\mathcal{NF}$ comes from the amalgamation of the Fano and the non-Fano matroids [1].

The access structure $\mathcal{F}+\mathcal{NF}$ does not admit ideal linear secret sharing schemes. We know the exact linear capacity of $\mathcal{F}+\mathcal{NF}$. Jafari and Khazaei proved that $\sigma_{\mathcal{L}}(\mathcal{F}+\mathcal{NF})=\frac{41}{36}$ [13]. We ask:Question 50 Does the inequality $\sigma_{\mathcal{A}}(C_{\mathcal{F}+\mathcal{NF}})<\frac{41}{36}$ hold?

Acknowledgments: Juan Andres Montoya thanks Universidad Nacional de Colombia, and the financial support provided through the project Hermes 44048.

Conflict of interest: Authors state no conflict of interest.

References

[1] Beimel A. Secret-sharing schemes: a survey. Lecture Notes Comp Sci. 2011;6639:11–46.
[2] Benaloh J. Secret sharing homomorphisms: keeping shares of a secret secret. Lecture Notes in Comp Sci. 1987;263:251–60.
[3] Brickell E, Davenport D. On the classification of ideal secret sharing schemes. J Cryptol. 1991;4:123–34.
[4] Chan T, Yeung R. On a relation between information inequalities and group theory. IEEE Trans Inf Theory. 2002;48(5):1992–5.
[5] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. Lecture Notes Comp Sci. 1992;576:457–65.
[6] Desmedt Y, Frankel Y. Classification of ideal homomorphic threshold schemes over finite abelian groups. Lecture Notes Comp Sci. 1993;658:25–34.
[7] Desmedt Y, Frankel Y. Homomorphic zero-knowledge threshold schemes over any finite abelian group. SIAM J Discrete Math. 1994;7(4):667–79.
[8] Dougherty R, Freiling C, Zeger K. Linear rank inequalities on five or more variables. 2009. arxiv.org:0910.0284v3.
[9] Dougherty R. Computations of linear rank inequalities on six variables. In: Proceedings of IEEE International Symposium on Information Theory, 1–4 July 2014. Honolulu, USA: IEEE; 2014. p. 2819–23.
[10] Gács P, Körner J. Common information is far less than mutual information. Probl Contr Inform Theory. 1973;2(2):149–62.

[11] Ingleton A. Representation of matroids. In: Welsh D, editor. Combinatorial mathematics and its applications. Oxford: Academic Press; 1969. p. 142–67.
[12] Ito M, Saito A, Nishizeki T. Multiple assignment scheme for sharing secret. J Cryptol. 1993:6(1):15–20.
[13] Jafari A, Khazaei S. On Abelian secret sharing: duality and separation. IACR Cryptol. 2019;2019:575.
[14] Liu M, Zhou M. Ideal homomorphic secret sharing schemes over cyclic groups. Sci China Ser E-Technol Sci. 1998;41:650–60.
[15] Matuš F. Infinitely many information inequalities. In: Proceedings of IEEE International Symposium on Information Theory, 24–29 June 2007. Nice, France: IEEE; 2007. p. 41–4.
[16] Mejia C. On the theory of linear rank inequalities. Ph.D thesis. Bogota: Universidad Nacional de Colombia; 2016.
[17] Mejia C. Linear secret sharing and the automatic search of linear rank inequalities. Appl Math Sci. 2015;9:5305–24.
[18] Mejia C, Andres Montoya J. On the information rates of homomorphic secret sharing schemes. J Inform Optimiz Sci. 2018;39(7):1463–82.
[19] Preneel B, Quisquater M, Vandewalle J. On the security of the threshold scheme based on the Chinese remainder theorem. Lecture Notes Comp Sci. 2002;2274:199–210.
[20] Oxley J. Matroid theory. Oxford: The Clarendon Press, Oxford University Press; 1992.
[21] Shamir A. How to share a secret. Commun ACM. 1979;22:612–13.
[22] Yeung R. A first course on information theory. Berlin: Springer Verlag; 2002.