

Common Information, Matroid Representation, and Secret Sharing for Matroid Ports

Michael Bamiloshin¹, Aner Ben-Efraim², Oriol Farràs¹, and Carles Padró³

¹Universitat Rovira i Virgili, Tarragona, Catalonia, Spain

²Ariel University, Ariel, Israel

³Universitat Politècnica de Catalunya, Barcelona, Spain,
 michael.bamiloshin@urv.cat, anermosh@post.bgu.ac.il,
 oriol.farras@urv.cat, carles.padro@upc.edu

February 20, 2020

Abstract

Linear information and rank inequalities as, for instance, Ingleton inequality, are useful tools in information theory and matroid theory. Even though many such inequalities have been found, it seems that most of them remain undiscovered. Improved results have been obtained in recent works by using the properties from which they are derived instead of the inequalities themselves. We apply here this strategy to the classification of matroids according to their representations and to the search for bounds on secret sharing for matroid ports.

Key words. Matroid representation, Secret sharing, Information inequalities, Common information, Linear programming.

1 Introduction

Some of the concepts appearing next are defined in Section 2. The reader is referred to the books [44, 55] on matroid theory and [56] on information theory, and the surveys [4, 45] on secret sharing for additional information about these topics.

1.1 Matroid Representation

Relevant applications in information theory, especially in secret sharing and network coding, brought to light the class of *entropic* matroids, which contains the well-known class of linear matroids.

An *entropic vector* is formed by the joint Shannon entropies of all subsets of a finite set of discrete random variables. Every entropic vector is the rank function of a polymatroid. A polymatroid is *entropic* if its rank function is a multiple of an entropic vector. Limits of entropic

The first and third authors were supported by the grant 2017 SGR 705 from the Government of Catalonia and grant RTI2018-095094-B-C21 CONSENT from the Spanish Government. Also, the first author has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 713679 and from the Universitat Rovira i Virgili. The third author was supported by ISF grant 152/17. The fourth author was supported by the Spanish Government through grant MTM2016-77213-R.

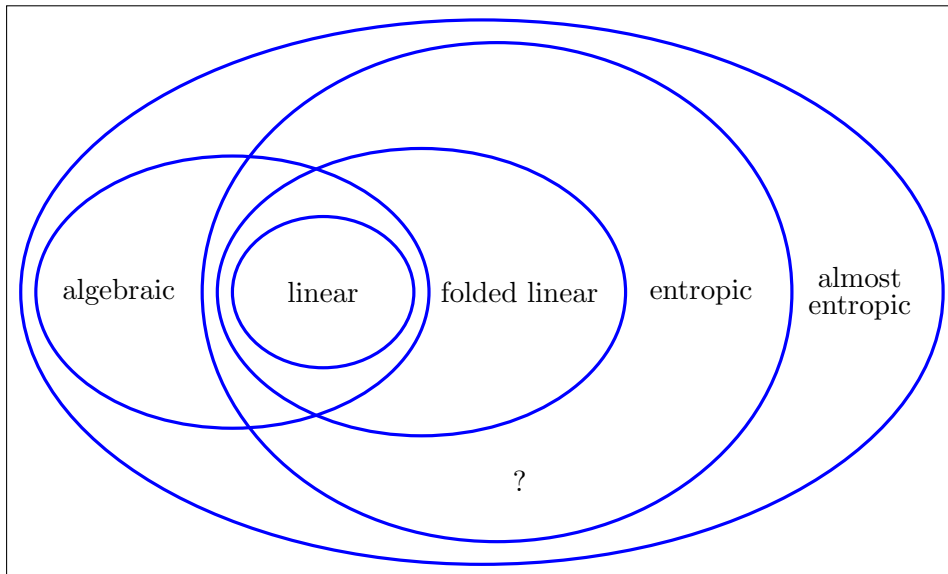


Figure 1: A classification of matroids. Discussed in Section 2.

polymatroids are called *almost entropic*. Both representation by partitions [35] and by almost affine codes [51] are characterizations of entropic matroids.

In the same way that linear matroids are defined from configurations of vectors in a vector space, configurations of vector subspaces determine *linear polymatroids*. A *folded linear* matroid is such that some multiple of its rank function corresponds to a linear polymatroid. Folded linear matroids have been called *multilinear* or *multilinearly representable* in the literature. Since no multilinear algebra is involved, that terminology may be misleading. The name proposed here is motivated by the analogy with folded Reed-Solomon codes.

It is well known that linear polymatroids and, consequently, folded linear matroids are entropic. František Matúš [38] recently proved that algebraic matroids are almost entropic.

Figure 1, an update of the corresponding diagram in [37], illustrates the current knowledge about the connections between the aforementioned classes of matroids. A detailed explanation is given in Section 2. There is a number of tools to deal with that classification. Among them, linear information and rank inequalities are especially useful. *Linear information inequalities*, such as Zhang–Yeung inequality [58], are the linear inequalities that are satisfied by the rank function of every entropic polymatroid. The ones that, like Ingleton inequality [25], are satisfied by the rank function of every linear polymatroid are called *linear rank inequalities*.

Ingleton inequality was used to prove the existence of an infinite number of excluded minors for the class of matroids that are linear over any given infinite field [40]. That result has been extended to the class of folded linear matroids over any given field and, by using Zhang–Yeung inequality instead of Ingleton inequality, to the classes of almost entropic matroids and algebraic matroids [37].

1.2 Common Information

Besides Ingleton and Zhang–Yeung inequalities, many other linear information and rank inequalities have been found [16, 18, 19, 30, 32, 36]. Nevertheless, only a few techniques to derive such inequalities are known, and it appears that many more inequalities remain unknown.

Linear information and rank inequalities are fundamental in the linear programming technique that has been used to find bounds on the information ratio of secret sharing schemes [7,

8, 34, 42, 46] and on the achievable rates in network coding [17, 53, 56]. An improvement to that technique has been recently proposed [20]. Specifically, instead of known inequalities, the properties from which most linear information and rank inequalities are derived are used as constraints. The notion of *common information* of two random variables is at the core of most of those properties. All known linear rank inequalities are derived from the *common information property* [18], while most of the known linear information inequalities are obtained from the concept of *AK-common information*, derived from Ahlswede–Körner lemma [1, 2, 14], or from the *copy lemma* [16, 19].

Several new lower bounds on the information ratio of secret sharing schemes have been obtained by using that improved linear programming technique [20]. For instance, by using the common information property, the exact values of the optimal information ratios of *linear* secret sharing schemes for *all* access structures on five players and *all* graph access structures on six players have been determined, concluding the projects undertaken in [15, 27] when restricted to linear schemes. Moreover, some of the existing lower bounds for general (that is, non-linear) secret sharing schemes for those and other access structures have been improved by using the AK-common information. The analogous application of the copy lemma has been described in [24].

On the negative side, the application of that technique is currently limited to solving linear programming problems that provide bounds for particular cases. Moreover, because of the huge number of variables and constraints, only problems with small size can be solved. In contrast, several general results, such as the best known general lower bound for secret sharing [12], have been obtained from the simpler technique involving only Shannon inequalities.

1.3 Secret Sharing for Matroid Ports

A perfect secret sharing scheme is *ideal* if all shares have the same size as the secret value, which is the smallest possible. The entropic vector given by the random variables defining an ideal scheme determines an entropic matroid [11, 35]. The access structure is a port of that matroid [11, 33]. As a consequence, the access structures of ideal secret sharing schemes are precisely the ports of entropic matroids, while the ports of folded linear matroids coincide with the access structures of ideal *linear* secret sharing schemes.

The optimal information ratio of secret sharing schemes for the ports of a matroid measures in some way how far it is from being entropic. This parameter has been studied for the Vamos matroid [6, 7, 20, 24, 33, 42], the first known example of a non-entropic matroid [50], and also for other non-entropic matroids [20, 46]. For the ports of the Vamos matroid, the application of the linear programming technique with the common information property yielded the exact value of the optimal information ratio of linear secret sharing schemes [20]. Moreover, Gürpınar and Romashchenko [24] recently obtained the current best lower bound for the general case by using that technique with the copy lemma.

1.4 Our Results

We investigate the application of the improved linear programming technique introduced in [20] to the classification of matroids according to the different representations discussed in Section 1.1. First, we prove in Theorem 3.14 an interesting consequence of the results by Nelson and van der Pol [43]. Namely, every almost entropic sparse paving matroid must satisfy Ingleton inequality. Second, we present an almost complete classification of the matroids on eight points. Our starting point is the paper by Mayhew and Royle [41], in which the linear matroids on eight points are determined. Specifically, up to isomorphism, there are exactly 44 matroids

on eight points that are not linear. All of them are sparse paving matroids. Exactly 39 of them do not satisfy Ingleton inequality, and hence they are not almost entropic. Therefore, there are five sparse paving matroids that are not linear but satisfy Ingleton inequality. We prove in Section 4.2 that exactly two of them are folded linear matroids. They are the smallest folded linear matroids that are not linear. Those two matroids were known to be algebraic. Unfortunately, we could not determine whether or not the other three matroids are algebraic or almost entropic. Some results about matroids on nine points are presented in Section 4.4. Specifically, we found 171 that satisfy Ingleton inequality but do not have the common information property. They are among the smallest matroids in that situation. One of those examples is the tic-tac-toe matroid. Those 171 matroids are not folded linear, but we could not determine whether or not they are algebraic or almost entropic.

In addition, by using the improved linear programming technique, we find new lower bounds on the information ratio of secret sharing schemes for several matroid ports. By combining our bounds for matroids on eight points with the results in [43], we present in Theorem 5.1 lower bounds that apply to every sparse paving matroid that do not satisfy Ingleton inequality. We found a lower bound on the information ratio of *linear* secret sharing schemes for the ports of the tic-tac-toe matroid and some of the aforementioned 171 related matroids. Finally, we determined the exact value of the optimal information ratio of linear secret sharing schemes for a port of the tic-tac-toe matroid.

2 Preliminaries

We use a compact notation for set unions, that is, we write XY for $X \cup Y$ and Xy for $X \cup \{y\}$. In addition, we write $X \setminus Y$ for the set difference and $X \setminus x$ for $X \setminus \{x\}$. The number of elements of the finite set X is denoted by $|X|$ and $\mathcal{P}(Q)$ denotes the power set of Q . For a positive integer m , we notate $[m] = \{1, \dots, m\}$.

2.1 Matroids and Polymatroids

Definition 2.1. Given a finite set Q and a function $f: \mathcal{P}(Q) \rightarrow \mathbb{R}$, the pair (Q, f) is called a *polymatroid* if the following properties are satisfied for all $X, Y \subseteq Q$.

- (P1) $f(\emptyset) = 0$.
- (P2) $f(X) \leq f(Y)$ if $X \subseteq Y$.
- (P3) $f(X \cap Y) + f(X \cup Y) \leq f(X) + f(Y)$.

The set Q and the function f are, respectively, the *ground set* and the *rank function* of the polymatroid. The rank function of an *integer polymatroid* only takes integer values. A *matroid* is an integer polymatroid (Q, r) such that $r(X) \leq |X|$ for every $X \subseteq Q$.

Some additional terminology and properties about matroids are needed. Let $M = (Q, r)$ be a matroid. The *independent sets* of M are the sets $X \subseteq Q$ with $r(X) = |X|$. Every subset of an independent set is independent. The *bases* of M are the maximal independent sets, and the minimal dependent sets are the *circuits*. All bases have the same number of elements, which equals $r(Q)$, the *rank of the matroid*. A set $X \subseteq Q$ is a *flat* of M if $r(Xx) = r(X)$ for every $x \in Q \setminus X$. In addition to the one given in Definition 2.1, there are other equivalent sets of axioms characterizing matroids which are stated in terms of the properties of the independent sets, the circuits, the bases, or the flats. A matroid of rank k is *paving* if the rank of every circuit is either k or $k - 1$. It is *sparse paving* if, in addition, all circuits of rank $k - 1$ are flats.

These are called *circuit-hyperplanes*. The *dual* of $M = (Q, r)$ is the matroid $M^* = (Q, r^*)$ with $r^*(X) = |X| - r(Q) + r(Q \setminus X)$ for every $X \subseteq Q$. Equivalently, M^* is the matroid on Q whose bases are the complements of the bases of M .

We introduce next the operations that are used to define *minors* of matroids and polymatroids. For a polymatroid $M = (Q, f)$ and a set $B \subseteq Q$, the *deletion* $M \setminus B$ of B from M is the polymatroid $(Q \setminus B, \hat{f})$ with $\hat{f}(X) = f(X)$ for every $X \subseteq Q \setminus B$, while the *contraction* $M/B = (Q \setminus B, \tilde{f})$ of B from M is defined by $\tilde{f}(X) = f(XB) - f(B)$ for every $X \subseteq Q \setminus B$. Every polymatroid that is obtained from M by applying deletions and contractions is called a *minor* of M . Finally, observe that minors of matroids are matroids.

Let $S = (S_x)_{x \in Q}$ be a discrete random vector, that is, a finite sequence of discrete random variables. For every $X \subseteq Q$, take $h(X) = H(S_X)$, the Shannon entropy of the discrete random variable $S_X = (S_x)_{x \in X}$. Then $(h(X))_{X \in \mathcal{P}(Q)}$ is the *entropic vector* associated to S . Because of the basic properties of Shannon entropy, every entropic vector is the rank function of a polymatroid [21, 22]. A polymatroid is *entropic* if its rank function is a multiple of an entropic vector. The closure in $\mathbb{R}^{\mathcal{P}(Q)}$ of the set of entropic vectors is a convex cone [56]. Each element in this convex cone is the rank function of an *almost entropic* polymatroid.

We introduce next some notation that is motivated by this connection between Shannon entropy and polymatroids. By analogy with the conditional mutual information, for a polymatroid (Q, f) and sets $X, Y, Z \subseteq Q$, we write

$$f(Y:Z|X) = f(XY) + f(XZ) - f(XYZ) - f(X)$$

and, in particular, $f(Y:Z) = f(Y:Z|\emptyset) = f(Y) + f(Z) - f(YZ)$ and $f(Y|X) = f(Y:Y|X) = f(XY) - f(X)$.

Consider a field \mathbb{F} , a vector space V with finite dimension over \mathbb{F} and a collection $(V_x)_{x \in Q}$ of vector subspaces of V . It is clear from basic linear algebra that the map f defined by $f(X) = \dim \sum_{x \in X} V_x$ for every $X \subseteq Q$ is the rank function of a polymatroid. Every such polymatroid is said to be *linearly representable*, or simply *linear*, over \mathbb{F} . For a positive integer k , a k -*folded \mathbb{F} -linear* matroid (Q, r) is such that the polymatroid (Q, kr) is \mathbb{F} -linear. As we mentioned in the Introduction, folded linear matroids are also called *multilinear* or *multilinearly representable* in the literature.

Suppose now that \mathbb{F} is a finite field and take the dual vector space V^* . The uniform probability distribution on V^* and the projections $V^* \rightarrow V_x^*$ for $x \in Q$ determine a discrete random vector $(S_x)_{x \in Q}$. Such random vectors are called *linear*. The entropic vector h associated to S satisfies $h(X) = f(X) \log |\mathbb{F}|$ for every $X \subseteq Q$. Since every linear polymatroid admits a linear representation over some finite field [48], linear polymatroids and folded linear matroids are entropic.

Consider a field extension \mathbb{K}/\mathbb{F} and a finite collection $(v_x)_{x \in Q}$ of elements in \mathbb{K} . For every $X \subseteq Q$, let $r(X)$ be the transcendence degree of the field extension $\mathbb{F}(\{v_x\}_{x \in X})/\mathbb{F}$. Then r is the rank function of a matroid M with ground set Q . In this situation, M is *algebraic over \mathbb{F}* and $(v_x)_{x \in Q}$ is an *algebraic representation of M* .

Given a positive integer m , a collection $(A_i)_{i \in [m]}$ of subsets of a finite set Q , and $I \subseteq [m]$, we notate $A_I = \bigcup_{i \in I} A_i$. A *linear information inequality*, respectively *linear rank inequality*, on m variables consists of a collection $(\alpha_I)_{I \in \mathcal{P}([m])}$ of real numbers such that $\sum_{I \in \mathcal{P}([m])} \alpha_I f(A_I) \geq 0$ for every entropic, respectively linear, polymatroid (Q, f) and for every collection $(A_i)_{i \in [m]}$ of subsets of Q . Since every linear polymatroid is entropic, every information inequality is also a rank inequality.

Shannon information inequalities are those that are derived from the polymatroid axioms

in Definition 2.1. Ingleton inequality [25], which can be written in a compact form as

$$f(A_2:A_3) \leq f(A_2:A_3|A_1) + f(A_2:A_3|A_4) + f(A_1:A_4) \quad (1)$$

was the first known example of a non-Shannon linear rank inequality. The information inequality

$$2f(A_2:A_3) \leq f(A_1:A_4) + f(A_1:A_2A_3) + 3f(A_2:A_3|A_1) + f(A_2:A_3|A_4) \quad (2)$$

which was presented by Zhang and Yeung [58], was the first known example of a non-Shannon linear information inequality.

Folded linear matroids are entropic. Every linear matroid is algebraic [44]. It has been recently proved that every algebraic matroid is almost entropic [38]. Vamos matroid is not almost entropic because it does not satisfy Zhang–Yeung inequality. Non-Pappus matroid is a folded linear matroid that is algebraic but not linear [44, 51]. Two examples of almost entropic matroids that are not entropic were given in [37, Remarks 4, 5]. Only one of them is algebraic. A folded linear matroid that is not algebraic was presented in [9]. It is not known if there exist entropic matroids that are not folded linear. These facts are illustrated in Figure 1.

For every positive integer k and any field \mathbb{F} , the class of k -folded \mathbb{F} -linear matroids is closed by duality [26, 44]. It is unknown whether or not this is the case for the classes of algebraic or entropic matroids. Remarkably, Kaced [29] recently proved that the class of almost entropic matroids is not closed by duality. An explicit counterexample is presented in [13].

Every minor of an \mathbb{F} -linear polymatroid is \mathbb{F} -linear. That is, the class of \mathbb{F} -linear polymatroids is closed under minors. The same applies to the class of almost entropic polymatroids [39, Lemma 1]. The classes of linear, folded linear, algebraic [44, Corollary 6.7.14], and almost entropic matroids are closed under minors.

2.2 Secret Sharing

Definition 2.2. An *access function* on a finite set P is a map $\Gamma: \mathcal{P}(P) \rightarrow \mathbb{R}$ satisfying the following properties.

1. $\Gamma(\emptyset) = 0$ and $\Gamma(P) = 1$.
2. $\Gamma(X) \leq \Gamma(Y)$ if $X \subseteq Y \subseteq P$.

An access function is *perfect* if its only values are 0 and 1. The *qualified* and *forbidden* sets of the access function Γ are the ones with $\Gamma(X) = 1$ and, respectively, $\Gamma(X) = 0$.

Definition 2.3. For a polymatroid (Q, f) and a point $p_o \in Q$ with $f(p_o) > 0$ and $f(Q \setminus p_o) = f(Q)$, the *port of the polymatroid* (Q, f) at p_o is the access function Γ on the set $P = Q \setminus p_o$ defined by

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

The *dual* Γ^* of an access function Γ on P is defined by $\Gamma^*(X) = 1 - \Gamma(P \setminus X)$ for every $X \subseteq P$. If Γ is the port of a matroid M at p_o , then its dual Γ^* is the port of the dual matroid M^* at p_o . Consider an access function Γ on P and a subset $B \subseteq P$. If $\Gamma(P \setminus B) = 1$, the access function $\Gamma \setminus B$ on $P \setminus B$ defined by $(\Gamma \setminus B)(X) = \Gamma(X)$ is the *deletion of B from Γ* . If $\Gamma(B) = 0$, the access function (Γ/B) with $(\Gamma/B)(X) = \Gamma(XB)$ is the *contraction of B from Γ* . Every access function that is obtained from Γ by deletions and contractions is a *minor* of Γ . If Γ is the port of a polymatroid $M = (Q, f)$ at p_o and $B \subseteq P = Q \setminus p_o$, then the minors $\Gamma \setminus B$ and Γ/B are the ports of $M \setminus B$ and, respectively, M/B at p_o .

Definition 2.4. Let P be a finite set of *players* and $Q = Pp_o$ with $p_o \notin P$. Let Γ be an access function on P . Let $S = (S_x)_{x \in Q}$ be a discrete random vector and (Q, h) the entropic polymatroid determined by S . Then S is a *secret sharing scheme* on P with access function Γ if the following properties are satisfied.

1. $h(p_o) > 0$ and $h(P) = h(Pp_o)$.
2. Γ is the port of (Q, h) at p_o .

The random variable S_{p_o} corresponds to the *secret value*, and the *share* for a player $x \in P$ is given by the random variable S_x . *Linear* secret sharing schemes are those defined by linear random vectors. A secret sharing scheme is *perfect* if its access function is perfect. The *information ratio* of a secret sharing scheme is $\max_{x \in P} h(x)/h(p_o)$, that is, the ratio between the maximum length of the shares and the length of the secret.

Only perfect secret sharing schemes are going to be considered in this work. Perfect access functions are also called *access structures*. Each of them is determined by its minimal qualified sets. An access structure is *connected* if every player is in some minimal qualified set. All access structures in this paper are supposed to be connected. In a perfect scheme, $h(x) \geq h(p_o)$ for every $x \in P$. A perfect secret sharing scheme is *ideal* if $h(x) = h(p_o)$ for every $x \in P$. The *optimal information ratio* $\sigma(\Gamma)$ of an access structure Γ is the infimum of the information ratios of the secret sharing schemes for Γ , while $\lambda(\Gamma)$ is the corresponding value when restricting the optimization to linear secret sharing schemes.

A matroid is *connected* if every pair of points in the ground set lie in a common circuit. All ports of a connected matroid are connected access structures. Moreover, a connected matroid is determined by any of its ports.

Let $S = (S_x)_{x \in Q}$ be an ideal secret sharing scheme and let h be the entropic vector associated to S . Then the polymatroid (Q, f) defined by $f(X) = h(X)/h(p_o)$ for every $X \subseteq Q$ is a matroid [11]. As a consequence, the access structures of ideal secret sharing schemes coincide with the ports of entropic matroids, and the ports of folded linear matroids are precisely the access structures of ideal linear secret sharing schemes.

3 How to Use Undiscovered Information and Rank Inequalities

The title of this section is borrowed from [24]. It precisely describes the main idea behind the technique introduced in [20], namely, using properties from which information and rank inequalities have been derived instead of using known inequalities.

3.1 Common Information

We say that a random variable S_3 *conveys the common information* of the random variables S_1 and S_2 if $H(S_3|S_2) = H(S_3|S_1) = 0$ and $H(S_3) = I(S_1:S_2)$. In general, given two random variables, it is not possible to find a third one satisfying those conditions [23]. Nevertheless, this is possible for every pair of random variables in a linear random vector and, according to [18], all known non-Shannon rank inequalities are derived from this fact. A combinatorial abstraction of concept of common information is given in the next definition.

Definition 3.1. Let (Q, f) be a polymatroid and let $A, B \subseteq Q$. Then every subset $X_o \subseteq Q$ satisfying

$$(C1) \quad f(X_o|A) = f(X_o|B) = 0, \text{ and}$$

$$(C2) \quad f(X_o) = f(A:B)$$

is called a *common information for the pair* (A, B) . If $X_o = \{x_o\}$, then the element x_o is also called a common information for the pair (A, B) .

Definition 3.2. Consider polymatroids (Q, f) and (Q', f') with $Q \subseteq Q'$. We say that (Q', f') is an *extension* of (Q, f) if $f(X) = f'(X)$ for every $X \subseteq Q$. In this situation we will generally use the same symbol for both rank functions.

Definition 3.3. A polymatroid (Q, f) is *1-CI-compliant* if, for every pair (A, B) of subsets of Q , there exists an extension (Qx_o, f) such that x_o is a common information for the pair (A, B) . Inductively, for every integer $k > 1$, a polymatroid $\mathcal{S} = (Q, f)$ is *k-CI-compliant* if, for every pair (A, B) of subsets of Q , there exists an extension (Qx_o, f) such that x_o is a common information for the pair (A, B) and (Qx_o, f) is $(k - 1)$ -CI-compliant. A polymatroid is *CI-compliant* if it is k -CI-compliant for every positive integer k .

Proposition 3.4. Let \mathbb{F} be a field. Consider an \mathbb{F} -linear polymatroid (Q, f) and a pair (A, B) of subsets of the ground set. Then there exists an \mathbb{F} -linear extension (Qx_o, f) such that x_o is a common information for (A, B) . As a consequence, linear polymatroids and, in particular, folded linear matroids are CI-compliant.

Proof. Consider a collection $(V_x)_{x \in Q}$ of vector subspaces providing an \mathbb{F} -linear representation of (Q, f) . For every $X \subseteq Q$, put $V_X = \sum_{x \in X} V_x$. Given a pair (A, B) of subsets of Q , take $V_{x_o} = V_A \cap V_B$. Then $(V_x)_{x \in Qx_o}$ is an \mathbb{F} -linear representation of a polymatroid (Qx_o, f) extending (Q, f) in which x_o is a common information for (A, B) . \square

3.2 Ahlswede and Körner's Information

Linear information inequalities can be derived from properties that are satisfied by every almost entropic polymatroid. Specifically, all known linear information inequalities have been derived from the copy lemma [58] and the Ahlswede–Körner lemma [1, 2, 14] as used in [32].

Definition 3.5. Let (Q, f) be a polymatroid, and let $U, V, Z \subseteq Q$. Then every subset $Z_o \subseteq Q$ such that

$$(AK1) \quad f(Z_o|UV) = 0,$$

$$(AK2) \quad f(U|Z_o) = f(U|Z) \text{ and } f(V|Z_o) = f(V|Z),$$

$$(AK3) \quad f(UV|Z_o) = f(UV|Z)$$

is called an *AK-information for the triple* (U, V, Z) .

We say that a polymatroid (Q, f) is *1-AK-compliant* if, for every triple (U, V, Z) of subsets of Q , there exists an extension (Qz_o, f) such that z_o is an AK-information for the triple (U, V, Z) . Analogously to the discussion on the common information property, we can define *k-AK-compliance* for every $k > 0$ and also *AK-compliance*. Next proposition was proved in [20] from [32, Lemma 5] and [28, Lemma 2]. As a consequence, almost entropic polymatroids are AK-compliant.

Proposition 3.6. For every almost entropic polymatroid (Q, f) and sets $U, V, Z \subseteq Q$, there exists an almost entropic extension (Qz_o, f) such that z_o is an AK-information for the triple (U, V, Z) .

As consequence of the following result from [20] (full version), k -CI-compliant polymatroids are also k -AK-compliant.

Proposition 3.7. *If x_o is a common information for the pair (UV, Z) , then x_o is an AK-information for the triple (U, V, Z) .*

3.3 Application to Secret Sharing

We describe next the linear programming technique that has been extensively used (see the references in [20]) to find lower bounds in secret sharing and the improvement on it proposed in [20].

Let $(S_x)_{x \in Q}$ be a secret sharing scheme with access structure Γ on the set of players $P = Q \setminus p_o$. Let (Q, h) be the entropic polymatroid determined by it and take the polymatroid (Q, f) given by $f(X) = h(X)/h(p_o)$. Then the vector $(f(X))_{X \in \mathcal{P}(Q)}$ satisfies the linear constraints

$$(N) \quad f(p_o) = 1,$$

$$(\Gamma) \quad f(X:p_o) = \Gamma(X) \text{ for every } X \subseteq P$$

and also the polymatroid axioms (P1)–(P3) in Definition 2.1. Therefore, the vector f is a feasible solution of Linear Programming Problem 3.8.

Linear Programming Problem 3.8. For an access structure Γ on the set P , the optimal value of this linear programming problem is, by definition, $\kappa(\Gamma)$.

$$\begin{aligned} & \text{Minimize} && v \\ & \text{subject to} && v \geq f(x) \text{ for every } x \in P \\ & && (N), (\Gamma), (P1), (P2), (P3) \end{aligned}$$

Since this applies to every secret sharing scheme with access structure Γ and the objective function equals the information ratio, the optimal value $\kappa(\Gamma)$ of this linear programming problem is a lower bound on $\sigma(\Gamma)$. It is the best lower bound that can be obtained by using only Shannon information inequalities [12, 33]. That linear program can be improved by adding non-Shannon information inequalities [7, 42, 46] or, as proposed in [20], constraints derived from AK-information or common information.

Linear Programming Problem 3.9. Consider an access structure Γ on a set P and a pair (A_0, A_1) of subsets of P . The optimal value of this linear programming problem is a lower bound on $\lambda(\Gamma)$.

$$\begin{aligned} & \text{Minimize} && v \\ & \text{subject to} && v \geq f(x) \text{ for every } x \in P \\ & && (N), (\Gamma1), (\Gamma2) \\ & && (C1), (C2) \text{ for } (A_0, A_1) \text{ and } x_o \\ & && (P1), (P2), (P3) \text{ on the set } Qx_o. \end{aligned}$$

Linear Programming Problem 3.10. Let $U, V, Z \subseteq P$. The optimal value of this linear programming problem is a lower bound on $\sigma(\Gamma)$.

$$\begin{aligned}
& \text{Minimize} && v \\
& \text{subject to} && v \geq f(x) \text{ for every } x \in P \\
& && (\text{N}), (\Gamma 1), (\Gamma 2) \\
& && (\text{AK1}), (\text{AK2}), (\text{AK3}) \text{ on } z_0 \text{ and } (U, V, Z) \\
& && (\text{P1}), (\text{P2}), (\text{P3}) \text{ on the set } Q_{z_0}.
\end{aligned}$$

These linear programming problems can be extended by adding the common information or the AK-information for more pairs or, respectively, triples of sets.

3.4 Application to Classification of Matroids

Linear information inequalities provide necessary conditions for a matroid to be almost entropic and, as a consequence of the result in [38], also to be algebraic. The same applies to linear rank inequalities with respect to the class of folded linear matroids. A polymatroid is *Ingleton-compliant*, respectively *ZY-compliant*, if Ingleton inequality (1), respectively Zhang–Yeung inequality (2), holds for every collection $(A_i)_{i \in [4]}$ of subsets of the ground set. As a consequence of the proofs for those inequalities [18, 28, 32], 1-CI-compliant and 1-AK compliant polymatroids are Ingleton-compliant and, respectively, ZY-compliant. Those inequalities are related to a special configuration introduced in [3].

Definition 3.11. A matroid (Q, r) satisfies the *bundle condition* if it does not contain four flats $(A_i)_{i \in [4]}$ such that every flat has rank 2, the union of every pair of flats has rank 3 except for $r(A_1 A_4) = 4$, and the union of every three or four flats has rank 4.

Vamos matroid is among the smallest ones violating the bundle condition, and the one with the minimum number of dependent hyperplanes. If a matroid does not satisfy the bundle condition, then the collection $(A_i)_{i \in [4]}$ described in the previous definition violates both Ingleton and Zhang–Yeung inequalities as expressed in (1) and (2), respectively. Therefore, almost entropic matroids and, in particular, algebraic matroids satisfy the bundle condition. Moreover, the sparse paving matroids that are Ingleton-compliant coincide with those satisfying a generalization of the bundle condition [43, Corollary 3.2].

Proposition 3.12. *Let M be a sparse paving matroid of rank $k \geq 4$. Then M is not Ingleton-compliant if and only if there exist five pairwise disjoint subsets B, A_1, A_2, A_3, A_4 of the ground set with $|B| = k - 4$ and $|A_i| = 2$ such that $BA_1 A_4$ is a basis and all the other sets of the form $BA_i A_j$ with $i \neq j$ are circuit-hyperplanes.*

Corollary 3.13. *If a sparse paving matroid M is not Ingleton-compliant, then there is a minor of M on eight points that is not Ingleton-compliant.*

As a consequence, the class of Ingleton-compliant sparse paving matroids has a finite number of forbidden minors [43, Theorem 1.3]. In contrast, the set of excluded minors for the class of Ingleton-compliant matroids is infinite [40]. By combining Proposition 3.12 with a recent result about algebraic matroids [38], the following remarkable property of sparse paving matroids is easily derived.

Theorem 3.14. *If a sparse paving matroid is not Ingleton-compliant, then it is not ZY-compliant and hence it is neither almost entropic nor algebraic.*

Proof. If a sparse paving matroid admits the configuration described in Proposition 3.12, then Zhang–Yeung inequality (2) does not hold for $(BA_i)_{i \in [4]}$. \square

By using the result in Proposition 3.12, Nelson and van der Pol [43] proved that the number of Ingleton-compliant matroids is doubly exponential on the size of the ground set. This indicates that the power of Ingleton inequality in the classification of matroids is quite limited. Of course, many more rank and information inequalities are available, but one may expect a better outcome from the strategy introduced in [20], which makes it possible to use undiscovered inequalities. This claim is supported by the results obtained in secret sharing [20, 24]. Specifically, the linear programming technique discussed in Section 3.3 can be adapted to the study of the classes of matroids described in Section 2.1 by using the following linear programming problems or their extensions to multiple pairs or triples of sets.

Linear Programming Problem 3.15. Given a polymatroid (Q, r) , and subsets $A, B \subseteq Q$, determine if there is an extension (Qx_o, r) such that x_o is a common information for the pair (A, B) .

Linear Programming Problem 3.16. Given a polymatroid (Q, r) and subsets $U, V, Z \subseteq Q$, determine if there is an extension (Qz_o, r) such that z_o is an AK-information for the triple (U, V, Z) .

Those linear programming problems can be used to disprove that a given matroid is folded linear or almost entropic. To that end, one can also apply Linear Programming Problems 3.9 or 3.10 (or their extensions) to any part of the given matroid. The corresponding common information or AK-information exists if and only if the optimal value is equal to 1.

Nevertheless, by Proposition 3.17, that technique is useless for matroids of rank 3. A *modular pair of flats* (A, B) in a matroid M consists of two flats such that $A \cap B$ is a common information for (A, B) . A flat A is *modular* if (A, B) is a modular pair of flats for every flat B . In a *modular matroid*, all flats are modular. Clearly, every matroid that admits a modular extension is CI-compliant. This is the case of the matroids with rank 3, because every such matroid can be extended to a projective plane [25].

Proposition 3.17. *Every matroid of rank 3 is CI-compliant, and hence also AK-compliant.*

In this work, we used the GurobiTM optimizer for solving the linear programming problems, and the SageMath matroid package for specific matroid operations.

4 Classification of Matroids on 8 Points

The matroids $AG(3, 2)$, $AG(3, 2)'$, F_8 , Q_8 , V_8 (Vamos matroid), P_8 , and L_8 appearing in this section and in Section 5 are described in the Appendix of Oxley’s book [44]. Given a sparse paving matroid M , a new such matroid M' can be obtained by *relaxing* one of its circuit-hyperplanes, that is, by transforming it into a basis. In that situation, M' is called a *relaxation* of M .

4.1 Matroids that are not Ingleton-compliant

Mayhew and Royle [41] provided a comprehensive list of matroids on up to 9 points, specifying how many of them are simple, paving, or sparse paving. They also presented the list of all 44 non-linear matroids on 8 points, which are sparse paving and of rank 4. Since every matroid on at most 7 points is linear, those are the smallest non-linear matroids. Exactly 39 of them are not

Ingleton-compliant, which implies by Theorem 3.14 that they are neither almost entropic nor algebraic. Those 39 matroids, which include F_8 and Q_8 , are relaxations of the binary affine cube $AG(3, 2)$, with $AG(3, 2)'$ and the Vamos matroid V_8 the ones among them with, respectively, most and fewest circuit-hyperplanes. The matroids in [41] are named according to the database provided by the same authors in [49]. In this work we follow the same notation.

4.2 Folded Linear Matroids

The 5 remaining non-linear matroids on 8 points are P_1 , P_2' , P_2'' , and P_3 , which are relaxations of P_8 , and a relaxation L_8' of L_8 . Take $Q = \{0, 1, \dots, 7\}$ as the ground set of those sparse paving matroids. The circuit-hyperplanes of P_8 are

$$0127, 0136, 0235, 1234, 0456, 1457, 2467, 3567, 0347, 1256,$$

while the ones of L_8 are

$$0246, 1357, 0156, 2347, 0127, 3456, 0457, 1236.$$

The matroid P_1 is obtained from P_8 by relaxing the circuit-hyperplane 3567 of P_8 . The relaxation of 0347 from P_1 gives the matroid P_2' , while P_2'' is obtained from P_1 by relaxing 1256. The relaxation of both 0347 and 1256 from P_1 produces the matroid P_3 . Finally, the matroid L_8' is obtained from L_8 by relaxing the circuit-hyperplane 0457.

By applying Linear Programming Problem 3.15 to those five non-linear matroids, we found out that they are 1-CI-compliant, and hence also 1-AK-compliant by Proposition 3.7. We explored the possibility that some of them were folded linear matroids. To that end, we combined the technique to find linear representations of matroids presented in [44, Section 6.4] with the tools for folded linear matroids given in [5] and we concluded that only P_3 and L_8' are folded linear matroids.

Proposition 4.1. *The smallest non-linear matroids that are folded linear are precisely P_3 and L_8' .*

Before proving Proposition 4.1, we describe how to use the techniques from [5, 44] to that end. Unless otherwise stated, the blocks in the matrices appearing in this section are square matrices of size ℓ . We use capital letters to represent them. As usual, the identity and zero matrices are denoted by I and 0 , respectively.

Consider a matroid $M = (Q, r)$ of rank m on n points, a field \mathbb{F} , and a positive integer ℓ . Assume that $Q = \{0, 1, \dots, n-1\}$ is the ground set of M . Every \mathbb{F} -linear representation of the polymatroid $(Q, \ell r)$ is called an (\mathbb{F}, ℓ) -linear representation of M , and it is determined by a block matrix over \mathbb{F} of the form

$$B = \begin{pmatrix} B_{0,0} & \cdots & B_{0,n-1} \\ \vdots & & \vdots \\ B_{m-1,0} & \cdots & B_{m-1,n-1} \end{pmatrix}, \quad (3)$$

where each block $B_{i,j}$ is a square matrix of size ℓ . If V_i is the vector subspace of $\mathbb{F}^{\ell m}$ spanned by the columns in the i -th block-column, then $(V_i)_{i \in Q}$ is an \mathbb{F} -linear representation of the polymatroid $(Q, \ell r)$. By the next result, there exists such a matrix in which every block is either invertible or zero.

Lemma 4.2. *Suppose that $A = \{0, 1, \dots, m-1\}$ is a basis of M . For each $j = m, \dots, n-1$, consider the fundamental circuit $C(j, A)$, that is, the only circuit contained in $A \cup j$. Then there exists a block matrix of the form*

$$\left(\begin{array}{ccc|ccc} I & \cdots & 0 & B_{0,m} & \cdots & B_{0,n-1} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & I & B_{m-1,m} & \cdots & B_{m-1,n-1} \end{array} \right), \quad (4)$$

providing an (\mathbb{F}, ℓ) -linear representation of M . Furthermore, in every such representation, each block $B_{i,j}$ with $j \geq m$ is invertible if $i \in C(j, A)$ and it is zero otherwise.

Proof. If B' , a block matrix of the form (3), is an (\mathbb{F}, ℓ) -linear representation of M , then the submatrix T formed by the block-columns corresponding to the basis A is invertible. Clearly, $B = T^{-1}B'$ is an (\mathbb{F}, ℓ) -linear representation of M of the form (4). Consider $j \geq m$. Without loss of generality, suppose that $C(j, A) = \{0, \dots, s-1, j\}$ for some $s \leq m$. Since the submatrix of B formed by the block-columns corresponding to $C(j, A)$ has rank ℓs , it is clear that $B_{i,j} = 0$ if $s \leq i \leq m-1$. If, otherwise, $0 \leq i \leq s-1$, the rank of the submatrix formed by the block-columns corresponding to $C(j, A) \setminus i$ equals ℓs , which implies that $B_{i,j}$ is invertible. \square

Following [5], we are going to use two operations on block matrices representing folded linear matroids. Namely, *block-column scaling* and *row-block scaling*.

Lemma 4.3 ([5] Proposition 2.12). *Let M be an ℓ -folded linear matroid represented by a block matrix B of the form (3) and let G be an invertible $\ell \times \ell$ matrix. Then, for each $i = 0, \dots, m-1$, the matrix*

$$\begin{pmatrix} B_{0,0} & \cdots & B_{0,n-1} \\ \vdots & & \vdots \\ GB_{i,0} & \cdots & GB_{i,n-1} \\ \vdots & & \vdots \\ B_{m-1,0} & \cdots & B_{m-1,n-1} \end{pmatrix}$$

is also an (\mathbb{F}, ℓ) -linear representation of M , and the same applies to the matrix

$$\begin{pmatrix} B_{0,0} & \cdots & B_{0,j}G & \cdots & B_{0,n-1} \\ \vdots & & \vdots & & \vdots \\ B_{m-1,0} & \cdots & B_{m-1,j}G & \cdots & B_{m-1,n-1} \end{pmatrix}$$

for each $j = 0, \dots, n-1$.

Block scaling can help significantly in simplifying the study of (\mathbb{F}, ℓ) -linear representations. By the following lemma, we can assume that several blocks $B_{i,j}$ in (4) equal the identity matrix. It is a straightforward generalization of [44, Theorem 6.4.7], the analogous result for linear representations of matroids.

Lemma 4.4. *Let \mathcal{M} be an ℓ -folded \mathbb{F} -linear matroid that admits an (\mathbb{F}, ℓ) -representation B' of the form (4). Take $V = \{0, \dots, m-1\}$ and $W = \{m, \dots, n-1\}$. Consider the bipartite graph G with set of vertices $V \cup W$ such that $(i, j) \in V \times W$ is an edge if and only if $B'_{i,j} \neq 0$. Let E be the set of edges of a maximal acyclic subgraph of G . Then a sequence of block scalings provides an (\mathbb{F}, ℓ) -representation B of the form (4) such that $B_{i,j} = I$ if $(i, j) \in E$.*

Proof. Adapt the proof of [44, Theorem 6.4.7] in the obvious way. \square

The graph G is connected for many matroids, and in this case we can assume that $n - 1$ blocks $B_{i,j}$ with $j \geq m$ are equal to I . We are now ready to prove Proposition 4.1.

Proof of Proposition 4.1. Let M be one of the matroids P_1, P_2', P_2'', P_3 and suppose that it is an ℓ -folded \mathbb{F} -linear matroid for some field \mathbb{F} and some positive integer ℓ . Since 0123 is a basis, by Lemmas 4.2 and 4.4, we can assume that M admits an (\mathbb{F}, ℓ) -linear representation of the form

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & 0 & I & I & I \\ 0 & I & 0 & 0 & I & 0 & I & A \\ 0 & 0 & I & 0 & I & B & 0 & C \\ 0 & 0 & 0 & I & I & D & E & 0 \end{array} \right) \quad (5)$$

We next consider the circuit-hyperplanes 0456, 1457, and 2467. The submatrices corresponding to those sets are, respectively,

$$\left(\begin{array}{cccc} I & 0 & I & I \\ 0 & I & 0 & I \\ 0 & I & B & 0 \\ 0 & I & D & E \end{array} \right), \left(\begin{array}{cccc} 0 & 0 & I & I \\ I & I & 0 & A \\ 0 & I & B & C \\ 0 & I & D & 0 \end{array} \right), \text{ and } \left(\begin{array}{cccc} 0 & 0 & I & I \\ 0 & I & I & A \\ I & I & 0 & C \\ 0 & I & E & 0 \end{array} \right)$$

Each of these matrices has rank 3ℓ . Gaussian elimination transforms those matrices into

$$\left(\begin{array}{cccc} I & 0 & I & I \\ 0 & I & 0 & I \\ 0 & 0 & B & -I \\ 0 & 0 & 0 & DB^{-1} + E - I \end{array} \right), \left(\begin{array}{cccc} I & I & 0 & A \\ 0 & I & D & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & C - B + D \end{array} \right), \left(\begin{array}{cccc} I & I & 0 & C \\ 0 & I & E & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & A - I + E \end{array} \right)$$

Therefore,

$$D = (I - E)B \quad (6)$$

$$C = B - D = EB \quad (7)$$

$$A = I - E \quad (8)$$

Since 3567 is a basis, the corresponding submatrix has full rank. Gaussian elimination on it yields

$$\left(\begin{array}{cccc} I & D & E & 0 \\ 0 & I & I & I \\ 0 & 0 & I & A \\ 0 & 0 & 0 & C - B + BA \end{array} \right).$$

By the previous equations, $C - B + BA = EB - BE$, and hence

$$EB \neq BE, \quad (9)$$

which is possible only if $\ell > 1$.

Clearly, the submatrix corresponding to the set 0347 has rank 3ℓ if and only if $C = A$. But $C \neq A$ because, otherwise, $B = E^{-1} - I$ by (7) and (8), and then $EB = BE$, a contradiction with (9). As a consequence, P_1 and P_2'' do not admit any (\mathbb{F}, ℓ) -linear representation.

Similarly, the submatrix corresponding to 1256 has rank 3ℓ if and only if $D = E$. We claim that this is impossible and, as a consequence, P_2' is not a folded linear matroid. Indeed, if $D = E$, and since $I - E = A$ by (8) and thus invertible, then $B = (I - E)^{-1}E$ by (6) and

$$(I - E)EB = (I - E)E(I - E)^{-1}E = E(I - E)(I - E)^{-1}E = E^2 = (I - E)BE$$

which is a contradiction with (9).

Since both 1256 and 0347 are bases of P_3 , it is still possible to find an (\mathbb{F}, ℓ) -linear representation for it. If there exists such a representation, then the matrices corresponding to 0347 and 1256 have full rank, and hence the matrices $B - E^{-1} + I$ and $E - (I - E)B$ are invertible. After substituting A , C , and D in (5) according to (8), (7) and (6), the following plausible (\mathbb{F}, ℓ) -linear representation for P_3 is obtained

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & 0 & I & I & I \\ 0 & I & 0 & 0 & I & 0 & I & I - E \\ 0 & 0 & I & 0 & I & B & 0 & EB \\ 0 & 0 & 0 & I & I & (I - E)B & E & 0 \end{array} \right). \quad (10)$$

As a matter of fact, if we take

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } E = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

it can be checked that it results in a $(GF(5), 2)$ -linear representation for that matroid.

We next prove in a similar fashion that L'_8 is also a folded linear matroid. If this is the case, by Lemmas 4.2 and 4.4, there exists an (\mathbb{F}, ℓ) -linear representation of the form

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & I & I & 0 & I \\ 0 & I & 0 & 0 & D & C & I & A \\ 0 & 0 & I & 0 & E & I & I & B \\ 0 & 0 & 0 & I & F & G & I & 0 \end{array} \right)$$

Proceeding in the same way as before, from the circuit-hyperplanes 0156, 0246, 1357, 2347, and 3456 we can conclude that

$$G = I, \quad F = D, \quad B = I, \quad A = D, \text{ and } C = I - E + D.$$

Since 0457 is a basis, the corresponding submatrix

$$\left(\begin{array}{cccc} I & I & I & I \\ 0 & D & C & A \\ 0 & E & I & B \\ 0 & F & G & 0 \end{array} \right) = \left(\begin{array}{cccc} I & I & I & I \\ 0 & D & I - E + D & D \\ 0 & E & I & I \\ 0 & D & I & 0 \end{array} \right)$$

has full rank. By Gaussian elimination, we obtain

$$\left(\begin{array}{cccc} I & I & I & I \\ 0 & I & D^{-1} & 0 \\ 0 & 0 & I - ED^{-1} & I \\ 0 & 0 & DED^{-1} - E & 0 \end{array} \right)$$

hence $DED^{-1} - E$ has full rank. In particular, this implies that $\ell > 1$. In conclusion, if L'_8 is a folded linear matroid, it admits an (\mathbb{F}, ℓ) -linear representation of the form

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & I & I & 0 & I \\ 0 & I & 0 & 0 & D & I - E + D & I & D \\ 0 & 0 & I & 0 & E & I & I & I \\ 0 & 0 & 0 & I & D & I & I & 0 \end{array} \right) \quad (11)$$

with $DE \neq ED$ and $I - E + D$ invertible. Take i , with $i^2 = -1$. The choice

$$D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } E = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

does result in a $(GF(5^2), 2)$ -linear representation of L'_8 . This can be checked by using a computer. \square

4.3 Algebraic Matroids and Skew-Field Representable Matroids

There exist folded linear matroids that are not algebraic [9], but none on 8 points.

Proposition 4.5. *Every folded linear matroid on 8 points is algebraic.*

Proof. Since linear matroids are algebraic, we only need to consider P_3 and L'_8 . Both are algebraic over all fields with finite characteristic [10, Example 35]. The result for P_3 was first proved by Lindström [31]. \square

The notion of linear representations of matroids over fields can be extended to linear representations over skew-fields. Matroids that admit such a representation are said to be *linearly representable over a skew-field*, or *skew-field representable* for short. The relation between skew-field representable matroids and folded linear matroids has been studied in [47, 54]. It is known that there exist folded linear matroids that are not representable over any skew-field [47]. In the other direction, some connections have been made in [54]. We found that, for matroids with at most 8 points, these two classes of matroids coincide.

Proposition 4.6. *A matroid on at most 8 points is skew-field representable if and only if it is a folded linear matroid.*

Proof. Every linearly representable matroid is also skew-field representable. Skew-field representable matroids are CI-compliant, so the 39 non-Ingletton compliant matroids discussed above are not representable over skew-fields. The techniques in Section 4.2 can also be adapted to representations over skew-fields. In particular, one can prove in that way that P_1 , P'_2 and P''_2 are not skew-field representable. Moreover, the matrix (11) provides a representation of L'_8 over the quaternion division ring $\mathbb{R}(i, j, k)$ by taking $E = i$ and $D = j$. A representation of P_3 over the quaternion division ring is obtained from the matrix (10) by taking $B = k$ and $E = j$. \square

Remark 4.7. The only matroids on 8 points for which it is not known whether they are algebraic, almost entropic, or entropic are P_1 , P'_2 , and P''_2 .

We can summarise the current classification of matroids on 8 points as follows. There are 44 matroids that are not linear (Section 4.1) and, among them, exactly two are folded linear (Proposition 4.1). Also, on 8 points, a matroid is skew-field representable if and only if it is a folded linear matroid (Proposition 4.6), and the folded linear ones are algebraic (Proposition 4.5). There are three matroids on 8 points for which it is not known whether they are algebraic, almost entropic, or entropic (Remark 4.7). A classification of these three matroids will conclude the characterization of algebraic, entropic, and almost entropic matroids on 8 points.

4.4 Exploring Larger Matroids

By taking into account the results in [18] about linear rank inequalities derived from the common information property, one may expect that there are Ingleton-compliant matroids that are not CI-compliant. As a consequence of the results in Sections 4.1 and 4.2, a matroid on 8 points is 1-CI-compliant if and only if it is Ingleton-compliant. Mayhew and Royle [41] found out that every matroid on 9 points that is not Ingleton-compliant contains a minor on 8 points with the same property. By solving Linear Programming Problem 3.15 for many matroids on 9 points from the database [49], we found 171 sparse paving matroids of rank 5 on 9 points that are Ingleton-compliant but not CI-compliant. All 171 matroids are listed in Table 1.

One of those examples is the tic-tac-toe matroid, which is described in Section 5. It was shown to be non-linearly representable by Alfter and Hochstättler [3]. Actually, they proved that it does not satisfy the so-called *generalized Euclidean intersection property*, and the same proof can be used to show that it is not CI-compliant. It is not known whether the tic-tac-toe matroid is algebraic or not. By solving Linear Programming Problem 3.16, we checked that it is 1-AK-compliant. We did not find among the other 170 examples any matroid that is not 1-AK-compliant but, due to computational limitations, our exploration was incomplete. Of course, the dual matroids of those 171 matroids are not folded linear. Nevertheless, we checked that they are 1-CI-compliant and hence, by Proposition 3.7, also 1-AK-compliant.

5 Secret Sharing for Matroid Ports

Consider a finite set of players P , a special player $p_o \notin P$ and $Q = Pp_o$. For a polymatroid (Q, f) , we notate $\Gamma_o(f)$ for its port at p_o and $\sigma(f) = \max_{x \in P} f(x)/f(p_o)$. Let Γ be a connected access structure on the set P . Then the parameters $\sigma(\Gamma)$ and $\lambda(\Gamma)$ introduced in Section 2.2 and the optimal value $\kappa(\Gamma)$ of Linear Programming Problem 3.8 are characterized as follows.

- $\kappa(\Gamma) = \min\{\sigma(f) : (Q, f) \text{ is a polymatroid with } \Gamma = \Gamma_o(f)\}$.
- $\sigma(\Gamma) = \inf\{\sigma(f) : (Q, f) \text{ is an entropic polymatroid with } \Gamma = \Gamma_o(f)\}$.
- $\lambda(\Gamma) = \inf\{\sigma(f) : (Q, f) \text{ is a linear polymatroid with } \Gamma = \Gamma_o(f)\}$.

The following parameter has been recently introduced by Csirmaz [13].

- $\bar{\sigma}(\Gamma) = \min\{\sigma(f) : (Q, f) \text{ is an almost entropic polymatroid with } \Gamma = \Gamma_o(f)\}$.

Clearly, $1 \leq \kappa(\Gamma) \leq \bar{\sigma}(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$. Moreover, Γ is a matroid port if and only if $\kappa(\Gamma) = 1$, and this is equivalent to $\kappa(\Gamma) < 3/2$ [33, Theorem 4.4]. An access structure admits an ideal secret sharing scheme if and only if it is the port of an entropic matroid. Besides, $\bar{\sigma}(\Gamma) = 1$ if and only if Γ is the port of an almost entropic matroid. The parameters κ and λ are invariant by duality, that is, $\kappa(\Gamma^*) = \kappa(\Gamma)$ and $\lambda(\Gamma^*) = \lambda(\Gamma)$ for every access structure Γ . By the recent results in [13, 29], this is not the case for the parameter $\bar{\sigma}$. If the access structure Γ' is a minor of Γ , then $\kappa(\Gamma') \leq \kappa(\Gamma)$, $\lambda(\Gamma') \leq \lambda(\Gamma)$, and also $\bar{\sigma}(\Gamma') \leq \bar{\sigma}(\Gamma)$.

By using the techniques described in Section 3.3, new lower bounds on $\bar{\sigma}(\Gamma)$ and $\lambda(\Gamma)$ were obtained in [20] for several access structures including the ports of the matroids $AG(3, 2)'$, F_8 , Q_8 , and V_8 . Moreover, the bounds on $\lambda(\Gamma)$ for the ports of Q_8 and V_8 are tight [20]. Subsequently, an improved lower bound on $\bar{\sigma}(\Gamma)$ for a port of the Vamos matroid V_8 was obtained in [24] by using the copy lemma instead of the Ahlswede–Körner lemma.

In this work, we continued the search for lower bounds for matroid ports by using those methods, which, of course, provide relevant lower bounds only when applied to matroids that

264950	265553	268475	275391	282271	304085
264955	265555	268476	275394	282272	306452
264956	265556	268477	275398	283581	308279
264978	265601	268486	275399	283624	308280
264984	265602	268611	275410	283626	308285
264994	265622	268613	275411	283630	308381
265008	265623	268765	275416	283631	308385
265012	265696	268774	275417	283632	308386
265014	265715	268805	276341	291383	319504
265018	265760	268958	276430	292609	320838
265020	266399	268961	276671	293346	327043
265023	266923	269060	276792	293347	327134
265026	266948	269061	277240	293361	327157
265028	267669	269062	277656	294990	328810
265129	267671	269550	277673	295231	328817
265237	267672	269551	280230	299715	328818
265262	267675	269558	280241	299721	328917
265270	267678	269559	280246	300609	328928
265389	267871	269704	280249	300831	328941
265421	267897	269824	280253	301018	335557
265422	267946	269895	280254	303086	335558
265423	268016	270130	280733	303094	350495
265424	268017	270133	280891	303095	351377
265437	268018	273139	281004	303158	351471
265465	268099	273141	281568	303165	351483
265468	268115	273582	281572	303175	tic-tac-toe
265547	268120	274066	281581	304062	
265551	268272	274247	281794	304066	
265552	268474	275082	282270	304067	

Table 1: Ingleton-compliant non-CI matroids with 9 Points

are not CI-compliant. We began by exploring the ports of the 39 matroids on 8 points that are not Ingleton-compliant and we found out that all of them satisfy $\lambda(\Gamma) \geq 4/3$ and $\bar{\sigma}(\Gamma) \geq 9/8$. A more general result is obtained by combining our bounds with Corollary 3.13.

Theorem 5.1. *If a sparse paving matroid is not Ingleton-compliant, then at least eight of its ports satisfy $\lambda(\Gamma) \geq 4/3$ and $\bar{\sigma}(\Gamma) \geq 9/8$.*

Proof. Let $M = (Q, r)$ be a sparse paving matroid that is not Ingleton-compliant. By Corollary 3.13, it has a minor $M' = (Q', r')$ with $|Q'| = 8$ that is not Ingleton-compliant. Hence M' is one of the 39 matroids on 8 points that are not Ingleton-compliant. For every $p_o \in Q' \subseteq Q$, the port Γ' of M' at p_o is a minor of the port Γ of M at p_o . Therefore, $\lambda(\Gamma) \geq \lambda(\Gamma') \geq 4/3$ and $\bar{\sigma}(\Gamma) \geq \bar{\sigma}(\Gamma') \geq 9/8$. \square

Better lower bounds on $\bar{\sigma}(\Gamma)$ have been obtained for some of those 39 matroids, which are presented in Table 2. The names or numbers of the matroids are as they appear in [41], and in the database [49].

We also applied the linear programs in Section 3.3 to the ports of matroids 265389, 265421, 265468, 265551, 265556 & 265622, and the tic-tac-toe matroid; all Ingleton-compliant but non-CI-compliant matroids on nine points. For all of them, we obtained the lower bound $\lambda(\Gamma) \geq 6/5$. We were not able to find any non-trivial bound on $\bar{\sigma}(\Gamma)$.

By presenting a suitable linear secret sharing scheme, we prove next that the bound $\lambda(\Gamma) \geq 6/5$ is tight for at least one of the ports of the tic-tac-toe matroid. Take $Q = \{0, 1, 2\} \times \{0, 1, 2\}$ and, for every $(a, b) \in Q$, the 5-element set

$$C_{ab} = \{(i, j) \in Q : i = a \text{ or } j = b\}$$

We introduce several sparse paving matroids with ground set Q and rank 5. We call M_o the one whose circuit-hyperplanes are all sets C_{ab} . The *tic-tac-toe matroid* M is obtained from M_o by relaxing the circuit C_{11} . Finally, for every $(a, b) \neq (1, 1)$, let M_{ab} be the matroid that is obtained from the tic-tac-toe matroid by relaxing the circuit C_{ab} . Clearly, every matroid M_{ab} is isomorphic to either M_{00} or M_{01} . The matroids M_o and M_{ab} with $(a, b) \neq (1, 1)$ are representable over every large enough field. We skip the proof of this fact, but we present \mathbb{F}_{11} -linear representations for M_o , M_{00} , and M_{01} , which are given, respectively, by the following matrices, whose columns are indexed as $(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)$.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 6 & 0 & 1 & 0 & 4 & 0 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 5 & 0 & 1 & 1 & 0 & 10 \\ 1 & 0 & 8 & 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 6 & 7 & 0 \\ 1 & 5 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 7 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 7 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 9 & 0 & 7 & 6 & 0 & 3 & 6 & 0 & 6 \end{pmatrix}$$

Let Γ be the port of the tic-tac-toe matroid M at $p_o = (0, 0)$. Let Γ_{11} be the port of M_o at p_o and, for $(a, b) \neq (1, 1)$, let Γ_{ab} be the port of M_{ab} at p_o . Since they are ports of \mathbb{F}_{11} -linear matroids, each of the nine access structures Γ_{ab} admits an ideal \mathbb{F}_{11} -linear secret sharing scheme. Every qualified set of Γ is qualified in at least five of the six access structures Γ_{11}, Γ_{00} ,

Matroid	Port	Improved bound on $\bar{\sigma}(\Gamma)$
1490	0, 2, 3, 4, 5, 6	8/7
1491	0, 3, 7	33/29
1491	2, 4, 5, 6	8/7
1492	0, 1, 2, 3, 4, 5, 6, 7	49/43
1494	3, 4, 5, 6	33/29
1499	0, 2, 3, 4, 5, 6	8/7
1500	0, 2, 3, 4, 5, 6	8/7
1501	0, 1, 2, 3, 6, 7	33/29
1501	4, 5	8/7
1502	5, 6	8/7
1502	2, 3, 4, 7	33/29
1508	3, 4, 5, 6	33/29
1509	3, 4, 5, 6	33/29
1510	3, 4, 5, 6	33/29
1518	3, 4, 5, 6	33/29
1520	2, 3, 4, 7	33/29
1524	3, 4, 5, 6	33/29
1525	0, 2, 4, 5	33/29
1525	3, 6	8/7
1526	0, 2, 3, 4, 5, 6	8/7
1527	0, 2, 4, 5	33/29
1528	0, 2, 3, 6	8/7
1529	1, 4, 5, 7	33/29
1531	2, 5, 6, 7	33/29
1532	4, 7	8/7
1532	0, 1, 2, 3, 5, 6	33/29
1549	3, 4, 5, 6	33/29
1568	3, 4, 5, 6	33/29
1572	2, 3, 4, 7	33/29
1576	3, 4, 5, 6	33/29
1578	3, 4, 5, 6	33/29
1579	0, 2, 4, 5	33/29
1579	3, 6	8/7
1580	0, 2, 3, 6	33/29
1641	3, 4, 5, 6	33/29
1646	2, 5, 6, 7	33/29
1654	3, 4, 5, 6	33/29
1656	0, 2, 3, 6	33/29
1657	0, 2, 3, 6	33/29
1660	0, 2, 3, 6	33/29
$AG(3, 2)'$	1, 3, 5, 7	49/43
F_8	1, 7	8/7
F_8	3, 4, 5, 6	33/29
Q_8	1, 4, 6, 7	49/43
V_8^+	0, 2, 3, 6	33/29
V_8	2, 3, 6, 7	33/29 [†]

Table 2: Bounds on ports of matroids on 8 points. [†]Improved in [24]

Γ_{01} , Γ_{02} , Γ_{10} , and Γ_{20} . In addition, the unqualified sets of Γ are also unqualified in those six access structures. Therefore, by combining the ideal linear secret sharing schemes for those six access structures in a λ -decomposition with $\lambda = 5$, we obtain a linear secret sharing scheme for Γ with information ratio $6/5$. The reader is referred to [45, 52] for more information about λ -decompositions.

Acknowledgements: We thank Dillon Mayhew and Gordon F. Royle for helpful suggestions and also for providing us the matroid database [49].

References

- [1] Ahlswede, R., Körner, J.: On the connection between the entropies of input and output distributions of discrete memoryless channels. Proceedings of the 5th Brasov Conference on Probability Theory, Brasov, 1974. Editura Academiei, Bucuresti, 13-23 (1977)
- [2] Ahlswede, R., Körner, J.: Appendix: On Common Information and Related Characteristics of Correlated Information Sources. *General Theory of Information Transfer and Combinatorics*. pp. 664–677. Springer, Berlin Heidelberg (2006)
- [3] Alfter, M., Hochstättler, W.: On pseudomodular matroids and adjoints. *Discrete Applied Mathematics* 60, 3–11 (1995)
- [4] Beimel, A.: Secret-Sharing Schemes: A Survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) *IWCC 2011*. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011)
- [5] Beimel, A., Ben-Efraim, A., Padró, C. and Tyomkin, I.: Multi-linear secret-sharing schemes, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8349, LNAI:394–418 (2014).
- [6] Beimel, A. and Livne, N.: On matroids and nonideal secret sharing. In *IEEE Transactions on Information Theory*, 54(6):2626–2643, 2008
- [7] Beimel, A., Livne, N., Padró, C.: Matroids Can Be Far From Ideal Secret Sharing. *Fifth Theory of Cryptography Conference, TCC 2008, Lecture Notes in Comput. Sci.* **4948** (2008) 194–212.
- [8] Beimel, A., Orlov, I.: Secret Sharing and Non-Shannon Information Inequalities. *IEEE Trans. Inform. Theory* 57, 5634–5649 (2011)
- [9] Ben-Efraim, A.: Secret-sharing matroids need not be algebraic. *Discrete Mathematics*, 339(8):2136–2145, 2016.
- [10] Bollen, G.P., Dustin Cartwright, D., Draisma, J.: Matroids over one-dimensional groups. arXiv:1812.08692 [math.CO] (2018)
- [11] Brickell, E.F., Davenport, D.M.: On the Classification of Ideal Secret Sharing Schemes. *J. Cryptology*, 4 123–134 (1991)
- [12] Csirmaz, L.: The size of a share must be large. *J. Cryptology* 10, 223–231 (1997)
- [13] Csirmaz, L.: Secret sharing and duality. *Cryptology ePrint Archive*, Report 2019/1197 <https://eprint.iacr.org/2019/1197> (2019)

- [14] Csiszar, I., Körner, J.: Information theory : coding theorems for discrete memoryless systems. Academic Press ; Akademiai Kiado, New York : Budapest, (1981)
- [15] van Dijk, M.: On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.* 6, 143–169 (1995)
- [16] Dougherty, R., Freiling, C., Zeger, K.: Six new non-Shannon information inequalities. In: 2006 IEEE International Symposium on Information Theory, pp. 233–236 (2006)
- [17] Dougherty, R., Freiling, C., Zeger, K.: Networks, matroids, and non-Shannon information inequalities. *IEEE Trans. Inform. Theory* 53 (2007), no. 6, 1949–1969.
- [18] Dougherty, R., Freiling, C., Zeger, K.: Linear rank inequalities on five or more variables. Available at arXiv.org, arXiv:0910.0284v3 (2009)
- [19] Dougherty, R., Freiling, C., Zeger, K.: Non-Shannon Information Inequalities in Four Random Variables. Available at arXiv.org, arXiv:1104.3602v1 (2011)
- [20] Farràs, O., Kaced, T., Martín, S., Padró, C.: Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing. *Advances in Cryptology — Eurocrypt 2018, Lecture Notes in Comput. Sci.* **10820** (2018) 597–621. Full version is available at Cryptology ePrint Archive, Report 2017/919, <https://eprint.iacr.org/2017/919>
- [21] Fujishige, S.: Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* 39, 55–72 (1978)
- [22] Fujishige, S.: Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* 61, 14–18 (1978)
- [23] Gács, P., Körner, J.: Common information is far less than mutual information. *Problems of Contr. and Inf. Th.* 2, 149–162 (1973)
- [24] Gürpınar, E., Romashchenko, A.: How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma. Available at arXiv:1901.07476v2 (2019)
- [25] Ingleton, A.W.: Representation of matroids. In: *Combinatorial Mathematics and its Applications*, D.J.A Welsh (ed.), pp. 149–167. Academic Press, London (1971)
- [26] Jackson, W.A., Martin, K.M.: Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* 4, 83–95 (1994)
- [27] Jackson, W.A., Martin, K.M.: Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* 9, 267–286 (1996)
- [28] Kaced, T.: Equivalence of Two Proof Techniques for Non-Shannon Inequalities. arXiv:1302.2994 (2013)
- [29] Kaced, T.: Information inequalities are not closed under polymatroid duality. *IEEE Trans. Inform. Theory* 64, 4379–4381 (2018)
- [30] Kinser, R.: New inequalities for subspace arrangements. *J. Combin. Theory Ser. A* 118, 152–161 (2011)
- [31] B. Lindström. A Non-Linear Algebraic Matroid with Infinite Characteristic Set. *Discrete Mathematics*, 59: 319–320, 1986.

- [32] Makarychev, K., Makarychev, Y., Romashchenko, A., Vereshchagin, N.: A new class of non-Shannon-type inequalities for entropies. *Communications in Information and Systems* 2, 147–166 (2002)
- [33] Martí-Farré, J., Padró, C.: On secret sharing schemes, matroids and polymatroids. *J. Math. Cryptol.* 4, 95-120 (2010)
- [34] Martín, S., Padró, C., Yang, A.: Secret sharing, rank inequalities, and information inequalities. *IEEE Trans. Inform. Theory* 62, 599-609 (2016)
- [35] Matúš, F.: Matroid representations by partitions. *Discrete Mathematics* 203, 169–194 (1999)
- [36] Matúš, F.: Infinitely many information inequalities. In: *Proc. IEEE International Symposium on Information Theory, (ISIT)*, pp. 2101–2105 (2007)
- [37] Matúš, F.: Classes of matroids closed under minors and principal extensions. *Combinatorica* 38, 935–954 (2018)
- [38] Matúš, F.: Algebraic matroids are almost entropic. To appear in *Proceedings of the AMS*
- [39] Matúš, F., Csirmaz, L.: Entropy region and convolution. *IEEE Trans. Inform. Theory* 62, 6007–6018 (2016)
- [40] Mayhew, D., Newman M., Whittle, G.: On excluded minors for real representativity, *J. Comb. Th. B* 99, 685–689 (2009)
- [41] Mayhew, D., Royle, G.F.: Matroids with nine elements. *J. Combin. Theory Ser. B* 98, 415-431 (2008)
- [42] Metcalf-Burton, J.R.: Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. *Discrete Math.* 311, 651–662 (2011)
- [43] Nelson, P. and van der Pol, J.: Doubly exponentially many Ingleton matroids. *SIAM Journal on Discrete Mathematics*, 32(2):1145–1153, 2018.
- [44] Oxley, J.G: *Matroid theory*. Second edition. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York (2011)
- [45] Padró, C.: *Lecture Notes in secret sharing*. Cryptology ePrint Archive, Report 2012/674 (2912)
- [46] Padró, C., Vázquez, L., Yang, A.: Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Discrete Applied Mathematics* 161, 1072–1084 (2013)
- [47] Pendavingh, R.A., van Zwam, S.H.M.: Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. *Adv. in Appl. Math.* 50, 201–226 (2013)
- [48] Rado, R.: Note on independence functions. *Proc. London Math. Soc. (3)* 7, 300–320 (1957)
- [49] Royle, G. and Mayhew, D.: Matroids on 9 elements. <http://doi.org/10.26182/5e3378f0ca2cd>
- [50] Seymour, P.D.: On secret-sharing matroids. *J. Combin. Theory Ser. B* 56, 69–73 (1992)

- [51] Simonis, J. and Ashikhmin, A.: Almost affine codes. *Designs, Codes, and Cryptography*, 14(2):179–197, 1998.
- [52] Stinson, D.R.: Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory* 40, 118–125 (1994)
- [53] Thakor, S., Chan, T., Grant, A.: Capacity bounds for networks with correlated sources and characterisation of distributions by entropies. *IEEE Trans. Inform. Theory* 63, 3540-3553 (2017)
- [54] Vertigan, D.: Dowling Geometries Representable over Rings. *Annals of Combinatorics*. 19 (2015).
- [55] Welsh, D.J.A.: *Matroid Theory*. Academic Press, London (1976)
- [56] Yeung, R.W.: *Information theory and network coding*. Springer (2008)
- [57] Zhang, Z., Yeung, R.W.: A non-Shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory* 43, 1982-1986 (1997)
- [58] Zhang, Z., Yeung, R.W.: On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory* 44, 1440–1452 (1998)