Journal of Algebraic Combinatorics (2025) 62:50
https://doi.org/10.1007/s10801-025-01462-y

Optimizing extension techniques for discovering non-algebraic matroids

Michael Bamiloshin[1] · **Oriol Farràs**[1]

Received: 18 June 2024 / Accepted: 13 August 2025 / Published online: 30 October 2025

Abstract
In this work, we revisit some combinatorial and information-theoretic extension techniques for detecting non-algebraic matroids. These are the Dress–Lovász and Ahlswede–Körner extension properties. We provide optimizations of these techniques to reduce their computational complexity, finding new non-algebraic matroids on 9 and 10 points. In addition, we use the Ahlswede–Körner extension property to find better lower bounds on the information ratio of secret-sharing schemes for ports of non-algebraic matroids.

Keywords Matroid · Algebraic matroid · Information inequality · Secret sharing scheme

1 Introduction

The characterization of matroids that admit a linear representation over a field is a natural problem that was formulated in the early stages of matroid theory. This notion of linear representation can be extended to algebraic representation over field extensions, considering the rank function determined by the transcendence degree instead of the linear dimension. Matroids that admit such a representation are said to be algebraic, and the characterization of these matroids is the main objective of this work. In addition to linear and algebraic, other kinds of matroid representations, such as multilinear (or folded linear) and entropic (or by partitions), have also been studied. It is known that linearly representable matroids are multilinear, and multilinear matroids are entropic. The class of algebraic matroids contains the class of linear matroids, but

The authors are supported by the project HERMES, funded by INCIBE and by the European Union NextGeneration EU/PRTR, and the project ACITHEC PID2021-124928NB-I00, MCIN/AEI/10.13039/501100011033/FEDER, EU. Additionally, Oriol Farràs is supported by the grant 2021 SGR 00115 from the Government of Catalonia.

✉ Oriol Farràs
oriol.farras@urv.cat

[1] Universitat Rovira i Virgili, Tarragona, Spain

it does not contain the class of multilinear matroids [11]. And the class of entropic matroids does not contain the class of algebraic matroids [27].

The study of linearly representable matroids has attracted a lot of interest and has applications in different areas, such as information theory, cryptography (secret-sharing schemes) and coding theory (network coding). See [10, 14, 16, 39], for example. Results on the other matroid representation classes mentioned above have also been applied in these areas [11, 18, 27, 37, 38].

Ingleton and Main presented in [24] a necessary condition for a matroid to be algebraic: In a *full* algebraic matroid of rank at least 4, if there are three pairwise but not all coplanar lines, then all three lines have a common intersection. This result was later generalized by Lindström [26].

The rank function of a full linear matroid is modular, but it is not necessarily so for full algebraic matroids. Nevertheless, a similar combinatorial property to modularity was shown for full algebraic matroids by Dress and Lovász [17]: For every pair of flats in a full algebraic matroid, there exists a flat called the *quasi-intersection* (denoted *pseudo-intersection* in [12]) that simulates their intersection. The Ingleton–Main lemma and its generalizations can also be viewed as extension properties of algebraic matroids, similar to the Euclidean and generalized Euclidean intersection properties of linear matroids [4, 5, 7].

In [13], Bollen did extensive work on the problem of matroid algebraicity. Using Frobenius flocks, he found some matroids on 9 points that are not algebraic over fields of characteristic 2, and using a recursive implementation of the Ingleton–Main lemma, he was able to discover many matroids on 9 points that are not algebraic over any field. The Ingleton–Main lemma loses its efficacy when applied to sparse paving matroids with rank greater than 4, as such matroids will always satisfy the property. Also, some matroids might be Frobenius flock representable and still not be algebraic.

While the aforementioned techniques emanate from matroid theory works, other techniques coming from information theory can also be applied to the problem of matroid classification. These include the common information (`CI`), the Ahlswede–Körner (`AK`), and the copy lemma (`CL`) properties.

`CI` is an extension property of linear polymatroids that is used to show that a matroid does not admit a linear representation. It was used (sometimes, implicitly) in many works studying the classification of linearly representable matroids, e.g., [6, 23, 30].

`AK` is a property of almost entropic polymatroids and was used to find non-Shannon information inequalities. Since algebraic matroids are almost entropic [29], we bring `AK` to the core of techniques for discovering non-algebraic matroids.

The direct application of both the `AK` and `CI` techniques to the linear programming problems for finding lower bounds on the information ratio of secret-sharing schemes was introduced in [19]. Later, `CL` was also applied to this problem [22], and improved lower bounds were found in [5, 6, 21].

1.1 Our contributions

In this work, we revisit some combinatorial and information-theoretic tools for detecting matroids that do not admit an algebraic representation. We provide optimizations

for techniques based on the Dress–Lovász and Ahlswede–Körner extension properties. Similar to [5, 6, 13], we show recursive applications of these techniques. Finding new results on matroid extensions, we are able to reduce the computational cost of using these techniques.

Applying these optimized techniques, we find new non-algebraic and non-almost entropic matroids on 9 and 10 points. We continue the classification work of algebraic matroids of Bollen [13], completing the classification of $(4, 9)$ matroids (i.e., matroids with rank-4 on 9 points) that do not satisfy the Dress–Lovász property at recursive depths smaller than 8. For $(5, 9)$ matroids, we show some smallest sparse paving matroids that satisfy the Ingleton inequality, have rank greater than 4, and are not almost entropic. These particular matroids would not have been found using Frobenius flocks, as they are Frobenius flocks representable, nor using the Ingleton–Main lemma due to the fact that they are sparse paving. Additionally, we show an identically self-dual, sparse paving rank-5 matroid on 10 points that is not almost entropic. This matroid has both the Tic-Tac-Toe matroid and its dual as minors.

Another contribution of this work is an improvement on the linear programming technique for finding lower bounds on the information ratio of secret-sharing schemes presented in [15, 19]. We define an LP problem that uses a more restrictive property of almost entropic polymatroids [7], which is also a consequence of the AK lemma. Using this approach, we obtain improved lower bounds for ports of matroids that are not algebraic.

For the interested reader, the programs used in this paper are available at https://github.com/bmilosh/algebraic-matroids-extensions.

1.2 Organization

The organization of the rest of this paper is the following. In Sect. 2, we introduce the notations we use in this work. In Sect. 2.1, we talk about relationships between different ways of representing a matroid. We introduce the extension properties we are focused on in Sect. 3. We encounter the first set of optimizations in this work in Sect. 4. The next set of optimizations come in Sects. 5.1 and 5.2. We present some non-algebraic matroids we found in Sect. 6 and finish with some results on secret sharing in Sect. 7.

2 Matroids and polymatroids

We refer the reader to [33] for an in-depth discussion of matroids and to [4, 5, 7] for matroid extension properties and techniques.

Definition 2.1 Given a finite set Q and a function $f : \mathcal{P}(Q) \to \mathbb{R}$, 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 $X \subseteq Q$. For compactness, given any sets $X, Y \subseteq Q$, we write the union $X \cup Y$ as XY, $r(X; Y)$ to denote $r(X) + r(Y) - r(XY)$, and $r(X|Y)$ for $r(XY) - r(Y)$.

For a polymatroid $\mathcal{S} = (Q, f)$ and a set $B \subseteq Q$, the *deletion* $\mathcal{S}\backslash B$ of B from $\mathcal{S}$ is the polymatroid $(Q \setminus B, \widehat{f})$ with $\widehat{f}(X) = f(X)$ for every $X \subseteq Q \setminus B$, while the *contraction* $\mathcal{S}/B = (Q \setminus B, \widetilde{f})$ of B from $\mathcal{S}$ is such that $\widetilde{f}(X) = f(XB) - f(B)$ for every $X \subseteq Q \setminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by applying deletions and contractions is called a *minor* of $\mathcal{S}$. Finally, observe that minors of matroids are matroids.

Consider sets Q, Z with $Q \cap Z = \emptyset$. A polymatroid (QZ, g) is an *extension* of a polymatroid (Q, f) if they satisfy that $g(X) = f(X)$ for every $X \subseteq Q$.

Let $\mathcal{M} = (Q, r)$ be a matroid. The *independent sets* of $\mathcal{M}$ are the sets $X \subseteq Q$ with $r(X) = |X|$. Every subset of an independent set is independent. The *bases* of $\mathcal{M}$ are its maximal independent sets, and its minimal dependent sets are called *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 $\mathcal{M}$ if $r(Xx) > r(X)$ for every $x \in Q \setminus X$. The flats with rank $r(Q) - 1$ are called *hyperplanes*. Flats $X, Y \subseteq Q$ are *modular* if $r(X) + r(Y) = r(XY) + r(X \cap Y)$, and *non-modular* otherwise. 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 hyperplanes.

In a *simple* matroid, all sets with one or two elements are independent. 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, which are called *circuit-hyperplanes*. The *dual* of $\mathcal{M} = (Q, r)$ is the matroid $\mathcal{M}^* = (Q, r^*)$ with $r^*(X) = |X| - r(Q) + r(Q \setminus X)$ for every $X \subseteq Q$. Equivalently, $\mathcal{M}^*$ is the matroid on Q whose bases are the complements of the bases of $\mathcal{M}$.

Definition 2.2 Given a matroid $\mathcal{M} = (Q, r)$, a *modular cut* $\mathcal{F}$ of $\mathcal{M}$ is a family of flats of $\mathcal{M}$ satisfying the following properties:

1. For every $F_1 \in \mathcal{F}$ and for every flat F_2 such that $F_1 \subseteq F_2$, $F_2 \in \mathcal{F}$, i.e., $\mathcal{F}$ is monotone increasing.
2. For every modular pair $F_1, F_2 \in \mathcal{F}$, $F_1 \cap F_2 \in \mathcal{F}$, i.e., $\mathcal{F}$ is closed under intersection of modular pairs.

Every proper point extension of a matroid (i.e., an extension by a rank-1 element) corresponds to a modular cut and vice versa [33, Sect. 7.2]. The modular cut *generated* by the flats $\{F_1, F_2, \ldots, F_k\}$, for some $k > 0$ is simply the smallest modular cut that contains these flats. In general, we denote the modular cut generated by a flat X as $\mathcal{F}_X = \{F \subseteq Q : X \subseteq F \text{ and } F \text{ is a flat of } \mathcal{M}\}$.

2.1 Matroid representations

Definition 2.3 A matroid $\mathcal{M} = (Q, r)$ is *ℓ-linearly representable* over a field $\mathbb{F}$ for some $\ell \in \mathbb{N}$ if there exist a vector space $\mathcal{V}$ and a vector subspace collection $(V_x)_{x \in Q}$ defined over $\mathbb{F}$ with $V_x \subseteq \mathcal{V}$ such that

$$\dim\left(\sum_{x \in A} V_x\right) = \ell \cdot r(A) \text{ for every } A \subseteq Q.$$

If $\ell = 1$, then $\mathcal{M}$ is simply said to be linearly representable. Matroids that are ℓ-linearly representable for $\ell > 1$ are said to be *multilinear* (or *folded linear*) matroids. While all linear matroids are multilinear, the reverse is not true. Examples of multilinear matroids that are not linear were shown in, e.g., [35, 38].

Consider an extension $\mathbb{K}$ of $\mathbb{F}$. An element x of $\mathbb{K}$ is said to be *algebraic* over $\mathbb{F}$ if it is the root of some non-trivial polynomial in $\mathbb{F}$. Otherwise it is *transcendental*. Given a subset $X \subseteq \mathbb{K}$, an element y of $\mathbb{K}$ is *algebraically independent* with respect to X if it is transcendental over the field $\mathbb{F}(X)$. A subset $X \subseteq \mathbb{K}$ is *algebraically independent* over $\mathbb{F}$ if every element $x \in X$ is algebraically independent with respect to the set $X \backslash x$ (i.e., no element $x \in X$ is the root of some non-trivial polynomial in $\mathbb{F}(X \backslash x)$), and *algebraically dependent* otherwise. The *transcendence degree* of $\mathbb{K}$ over $\mathbb{F}$ is the size of the largest algebraically independent subset of $\mathbb{K}$ over $\mathbb{F}$.

Definition 2.4 A matroid $\mathcal{M} = (Q, r)$ is *algebraically representable* over a field $\mathbb{F}$ if there exist an extension $\mathbb{K}$ of $\mathbb{F}$ and a sequence of elements $(e_i)_{i \in Q} \subseteq \mathbb{K}$ such that, for every $A \subseteq Q$,

$$r(A) = \deg_{\text{tr}} \mathbb{F}((e_i)_{i \in A}),$$

where $\mathbb{F}((e_i)_{i \in A})$ is the smallest subfield of $\mathbb{K}$ containing $\mathbb{F}$ and $(e_i)_{i \in A}$, and $\deg_{\text{tr}}$ is the transcendence degree of $\mathbb{F}((e_i)_{i \in A})$ over $\mathbb{F}$.

A matroid $\mathcal{M}$ whose ground set Q consists of all elements of $\mathbb{K}$ and is such that $F \subseteq Q$ is a flat of $\mathcal{M}$ if and only if $\mathbb{F}((e_i)_{i \in F})$ is algebraically closed is called a *full algebraic* matroid.

Fujishige [20] observed that, given a set $Q = \{1, \ldots, n\}$ with an associated set of random variables $\{S_1, \ldots, S_n\}$, the entropy function $h : 2^Q \to \mathbb{R}_{\geq 0}$ on this set expressed as

$$h(A) = H(S_A)$$

for every $A \subseteq Q$ such that $A \neq \emptyset$, $h(\emptyset) = 0$, and $H(S_A)$ is the Shannon entropy of the random variables indexed by A, defines the rank function of a polymatroid. Such a polymatroid is called an *entropic polymatroid*. A matroid is said to be *almost entropic* if it is the limit of a sequence of entropic polymatroids, and *entropic* if its rank function is a multiple of the rank function of an entropic polymatroid.

All linear matroids are algebraic, but the converse is not true. Matroids with less than 8 points are linear, and therefore algebraic, with the Vámos matroid being the first matroid shown to be non-algebraic [24]. In the other direction, the non-Pappus matroid is an example of an algebraic matroid that is not linear [25]. Furthermore,

not every multilinear matroid is algebraic [11], and not every algebraic matroid is multilinear [27]. Since every multilinear matroid is entropic, then there are entropic matroids that are not algebraic. All algebraic matroids are almost entropic [29], but not all almost entropic matroids are algebraic (nor entropic) [28, Remarks 4 & 5]. For a visual depiction of these relationships, see [6, Fig. 1].

3 Extension properties of algebraic matroids

In this section, we present the techniques we use to find non-algebraic matroids. Our techniques are based on properties satisfied by algebraic matroids: Ahlswede–Körner extensions and Dress–Lovász extensions.

3.1 Dress–Lovász extensions

Every algebraic matroid can be embedded in its full algebraic matroid, and the same holds for linear matroids. However, unlike in the case of full linear matroids where all pairs of flats are modular, pairs of flats of full algebraic matroids are not necessarily modular. Instead, Dress and Lovász [17] showed that pairs of flats of full algebraic matroids have what they called a quasi-intersection.

Theorem 3.1 [17, Theorem 1.5] *Let $\mathcal{M} = (Q, r)$ be a full algebraic matroid. Then for every pair of flats $X, Y \subseteq Q$ of $\mathcal{M}$, there exists a flat $T \subseteq X$ such that, for every flat X' contained in X,*

$$T \subseteq X' \text{ if and only if } r(Y|X') = r(Y|X).$$

Moreover, X and Y are modular if and only if $T = X \cap Y$.

One can deduce a necessary condition for a matroid to be algebraic from the Dress–Lovász result as follows. If $\mathcal{M}$ is an algebraic matroid for which for some pair of flats (X, Y) there is no $T \subseteq X$ satisfying Theorem 3.1, then $\mathcal{M}$ admits a series of proper point extensions in which this flat T exists.

Definition 3.2 Let $\mathcal{M} = (Q, r)$ be a matroid and let $X, Y \subseteq Q$ be a non-modular pair of flats of $\mathcal{M}$. The *quasi-intersection of* (X, Y) is a flat $T \subseteq Q$ satisfying the following conditions

(DL1) $r(T|X) = 0$, and
(DL2) $r(T|X') = 0$ iff $r(Y|X') = r(Y|X)$ for every flat $X' \subseteq X$.

Note that the quasi-intersections of (X, Y) and (Y, X) are not necessarily the same.

Lemma 3.3 *For a pair of flats (X, Y) in a matroid (Q, r), if the quasi-intersection exists, it is unique.*

Proof Suppose $T_1, T_2 \subseteq Q$ are two quasi-intersections of (X, Y). Then by (DL2), we have $r(T_1|T_2) = 0 = r(T_2|T_1)$ and therefore, $r(T_1) = r(T_1T_2) = r(T_2)$. Since T_1 and T_2 are flats, it implies that $T_1 = T_2$.

□

Definition 3.4 Let $\mathcal{M} = (Q, r)$ be a matroid and let $X, Y \subseteq Q$ be a non-modular pair of flats of $\mathcal{M}$. A matroid (QZ, r) is a *Dress–Lovász (*DL*) extension* of $\mathcal{M}$ for (X, Y) if there exists a set $T \subseteq QZ$ that is the quasi-intersection of (X, Y).

Definition 3.5 A matroid $\mathcal{M} = (Q, r)$ satisfies the *Dress–Lovász property (*DL*)* if for every non-modular pair of flats (X, Y) of $\mathcal{M}$ there is a DL-extension.

Like the matroid extension properties studied in [5, 7], we can also give a recursive definition to the Dress–Lovász extension property as follows:

Definition 3.6 A matroid $\mathcal{M}$ is *1*-DL if for every pair of flats X, Y, there is a DL-extension. It is k-DL for some $k > 1$ if for every pair of flats X, Y, there is a DL-extension that is $(k-1)$-DL. Algebraic matroids are k-DL for every $k \geq 1$ due to [29].

3.2 Ahlswede–Körner lemma

The Ahlswede–Körner lemma describes a property of pairs of information sources [1, 2] that also holds for almost entropic polymatroids. We use it to find non-algebraic matroids, as in [6], because algebraic matroids are almost entropic [29].

In this work, we use a stronger statement of this property that was proved in [19, Proposition 3.14]. Instead of dealing with triples of sets, the AK property can still be determined using pairs of sets with extra conditions. The following is a formalization of that result and was recently defined in [7].

Definition 3.7 For a polymatroid (Q, f) and sets $X, Y \subseteq Q$, an extension (QZ, g) of (Q, f) is an *Ahlswede–Körner extension*, or *AK extension*, for the pair (X, Y) if the following conditions are satisfied:

(AK1) $g(Z|X) = 0$, and
(AK2) $g(X'|Z) = g(X'|Y)$ for every $X' \subseteq X$.

Following [6], we call Z the AK-*information* of (X, Y) and denote it AK(X, Y). We say that a polymatroid satisfies the AK property if for every (X, Y) there exists an AK extension.

Note that it can sometimes happen that there is a set $Z \subseteq X$ that satisfies the listed conditions. In such a case, by an abuse of notation, we still call such a set an AK information of (X, Y). The following result shows when this situation may arise.

Lemma 3.8 *Let $\mathcal{M} = (Q, r)$ be a matroid, and let $X, Y \subseteq Q$ be flats. There exists a set $Z \subset Q$ that satisfies (AK1) and (AK2) for (X, Y) if and only if (X, Y) is a modular pair.*

Proof The converse statement is straightforward (just take $Z = X \cap Y$) and its proof is therefore omitted. For the forward direction, note that setting $X' = Z$ in (AK2) gives $r(Z|Y) = 0$ and setting $X' = X$ gives $r(Z) = r(X; Y)$. Hence, $Z = X \cap Y$, and r is therefore modular on (X, Y). □

We conclude this section presenting a property of linear polymatroids, the *common information* property (CI). Though not a direct property of algebraic matroids, we introduce it here because we will use the fact that it implies the AK property [19] in some of our results.

Definition 3.9 For a polymatroid (Q, f) and sets $X, Y \subseteq Q$, an extension (QZ, g) of (Q, f) is a *common information extension*, or *CI extension*, for the pair (X, Y) if the following conditions are satisfied:

(CI1) $g(Z|X) = g(Z|Y) = 0$, and
(CI2) $g(Z) = g(X; Y)$.

Likewise, we call Z the *common information* of X and Y and denote it $\mathtt{CI}(X, Y)$. We say that a polymatroid satisfies the CI property if for every (X, Y) there exists a CI extension.

As shown in [7, Proposition 3.17], the AK property is preserved by minors. And, from [19, Proposition 3.16] (or, alternatively, [7, Proposition 3.13]), we have the following relationship between the CI and AK properties. We add its proof for the sake of completeness.

Proposition 3.10 *Let $\mathcal{M} = (Q, r)$ be a matroid, let $X, Y \subseteq Q$ be a non-modular pair of flats of $\mathcal{M}$, and let $x_o = AK(X, Y)$. Then $r(x_o) = r(X; Y)$. Hence, $x_o = AK(Y, X)$ if and only if x_o is the common information of X and Y.*

Proof If $x_o = \mathtt{AK}(X, Y)$, then $r(x_o|X) = 0$ and $r(Xx_o) = r(X)$ by (AK1). By (AK2),

$$0 = r(X|x_o) - r(X|Y) = r(Xx_o) - r(x_o) - r(XY) + r(Y) = r(X; Y) - r(x_o),$$

proving the first statement. If $x_o = \mathtt{AK}(Y, X)$, then $r(x_o|Y) = 0$, and x_o satisfies (CI1). Conversely, a common information of (X, Y) satisfies (AK1) and (AK2) for (X, Y) and (Y, X). □

Combining Lemma 3.8 and Proposition 3.10, we have that, for flats X and Y, $\mathtt{AK}(X, Y) = \mathtt{AK}(Y, X)$ if and only if r is modular on X and Y.

4 Optimizing AK for polymatroids

We observed that, similar to CI, checking if a matroid is AK can be restricted to only the flats of the matroid as opposed to checking all possible subsets of the ground set of the matroid. This fact is presented in the following theorem, which is proved later in this section.

Theorem 4.1 *A polymatroid (Q, f) satisfies the AK property if for every pair of flats (X, Y), there is an extension (QZ, f) that satisfies conditions (AK1) and (AK2'), where*

(AK2') *$f(X'|Z) = f(X'|Y)$ for every flat $X' \subseteq X$.*

As a consequence of this theorem, we can check the existence of AK extensions of a polymatroid with the following linear program. Note that while this is defined for a single extension, it can easily be extended to an arbitrary number of extensions of the polymatroid.

Linear Programming Problem 4.2 Given a polymatroid (Q, f), check if for every pair of flats (U, V) there exists a polymatroid extension (Qx_0, f) that satisfies (AK1) and (AK2').

Theorem 4.1 is proved in two steps. First, we show in Lemma 4.5 that (AK2) can be reduced to (AK2'). Then in Proposition 4.6, we show that it is enough to check (AK1) and (AK2) for pairs of flats. But first, the following results are some of the properties of polymatroids that will be used frequently (sometimes implicitly) in our discussions on AK.

Lemma 4.3 *Let $\mathcal{S} = (Q, f)$ be a polymatroid. For any $X, Y \subseteq Q$,*

$$f(XY) = f(\bar{X}Y) = f(\bar{X}\bar{Y}),$$

where $\bar{X}$ and $\bar{Y}$ are the closures of X and Y, respectively.

Proof It is enough to prove that $f(XY) = f(\bar{X}Y)$. By monotonicity, $f(\bar{X}Y) \geq f(XY)$. By submodularity, we have that

$$\begin{aligned} f(XY) + f(\bar{X}) &\geq f(XY\bar{X}) + f(XY \cap \bar{X}) = f(\bar{X}Y) + f(X \cup (\bar{X} \cap Y)) \\ &\geq f(\bar{X}Y) + f(X) = f(\bar{X}Y) + f(\bar{X}). \end{aligned}$$

Thus, $f(XY) = f(\bar{X}Y)$. □

Lemma 4.4 *Let $\mathcal{S} = (Q, f)$ be a polymatroid and let $\mathcal{S}' = (QZ, f)$ be an extension of $\mathcal{S}$. For any $U \subseteq Q$, $V \subseteq QZ$ and $\bar{U} = \mathrm{cl}_{\mathcal{S}}(U)$,*

$$f(UV) = f(\bar{U}V).$$

Proof Observe that $f(UV) \leq f(\bar{U}V) \leq f(\mathrm{cl}_{\mathcal{S}'}(U)V)$. By Lemma 4.3, the first and last terms above are equal, proving the result. □

In the next result, we show that one does not in fact need to check property (AK2) of Definition 3.7 for every subset X' of X; it is sufficient to check it only for subsets of X that are flats.

Lemma 4.5 *Let $\mathcal{S} = (Q, f)$ be a polymatroid and let $\mathcal{S}' = (QZ, f)$ be an extension of $\mathcal{S}$. Take $X, Y, \bar{X} \subseteq Q$ where $\bar{X} = \mathrm{cl}_{\mathcal{S}}(X)$. Then*

$$f(X|Z) = f(X|Y) \text{ if and only if } f(\bar{X}|Z) = f(\bar{X}|Y).$$

Proof By Lemma 4.4, we have that $f(\bar{X}Z) = f(XZ)$, and $f(\bar{X}Y) = f(XY)$ by Lemma 4.3. Thus, $f(\bar{X}|Z) = f(\bar{X}Z) - f(Z) = f(XZ) - f(Z) = f(X|Z)$ and, analogously, $f(\bar{X}|Y) = f(X|Y)$, completing the proof. □

As a consequence of this result, (AK2) is equivalent to (AK2'). We show next that for any matroid, the AK property can be checked using only flats of the polymatroid.

Proposition 4.6 *Let $\mathcal{S} = (Q, f)$ be a polymatroid, let $X, Y \subseteq Q$, and let $\bar{X} = \mathrm{cl}(X)$ and $\bar{Y} = \mathrm{cl}(Y)$. If $\mathcal{S}$ admits an AK extension for $(\bar{X}, \bar{Y})$ then it admits an AK extension for (X, Y).*

Proof Let $Z = \mathrm{AK}(\bar{X}, \bar{Y})$. Note that $f(Z|X) = 0$ by Lemma 4.3. And for all $X' \subseteq X$, since $f(X'|Z) = f(X'|\bar{Y})$, then $f(X'|Z) = f(X'|Y)$ again by Lemma 4.3, completing the proof. □

Hence, if the polymatroid admits an AK extension for every pair of flats, then it does so for every pair of sets, proving the theorem.

This reduction in the primary number of sets involved in the AK property from 3 to 2 greatly reduces computation time in checking the property. Given a matroid (Q, r) with flats $\{F_1, F_2, \ldots, F_k\}$ for some integer k, while the 3-set formulation of the AK property involves checking about $k!/(k-3)!$ triples of flats, the 2-set formulation involves about $k!/(k-2)!$ pairs of flats.

5 Optimizing AK and DL for matroids

Admitting an AK extension for (X, Y) does not necessarily indicate admitting an AK extension for (Y, X) [19, Proposition 3.16], and it might therefore be worthwhile to apply LP 4.2 for both (X, Y) and (Y, X) simultaneously when checking for AK extensions. Nevertheless, the results here show that this does not help in some cases.

It is important to note that results in Sect. 5.1 are *negative* in the sense that they implicitly show us which pairs of sets to avoid when testing for AK. This is due to the fact that a polymatroid satisfying the AK property does not necessarily mean it is almost entropic. But on the other hand, if it does not satisfy AK, then we know for sure it is not almost entropic, and therefore, also not algebraic. Hence, it is more practical using it to find polymatroids in the latter category.

The next two results are well-known properties of matroids that we will apply at various times for the rest of this section.

Lemma 5.1 *Let H_1 and H_2 be distinct circuit-hyperplanes of a matroid $\mathcal{M}$ of rank k. Then $r(H_1 \cap H_2) \leq k-2$. In addition, if $\mathcal{M}$ is paving, then $|H_1 \cap H_2| \leq k-2$.*

Proof By submodularity,

$$2(k-1) = r(H_1) + r(H_2) \geq r(H_1 H_2) + r(H_1 \cap H_2) = k + r(H_1 \cap H_2),$$

so $k - 2 \geq r(H_1 \cap H_2)$. The second part of the result holds because $H_1 \cap H_2$ is an independent set in a paving matroid. □

Lemma 5.2 *Let $\mathcal{M} = (Q, r)$ be a matroid of rank k and let X, Y be a non-modular pair of flats of $\mathcal{M}$.*

(i) If X is a line, then $r(X|Y) = 1$ and $r(X \cap Y) = 0$.

(ii) If Y is a hyperplane, then $r(Y|X') > r(Y|X)$ for every flat X' in X.

Proof Since (X, Y) are non-modular, $r(X)+r(Y) > r(XY)+r(X\cap Y)$ and $r(XY) \geq r(Y) + 1$. In (i), using that $r(X) = 2$ we get $2 + r(Y) > r(Y) + 1 + r(X \cap Y)$, which implies that $r(X \cap Y) = 0$ and $r(XY) = r(Y) + 1$. In (ii), if $X' \nsubseteq Y$, then $r(X'Y) = k = r(XY)$ and so $r(Y|X') > r(Y|X)$. If $X' \subseteq Y$, then $r(X) + r(Y) > r(XY) + r(X \cap Y) \geq r(XY) + r(X')$, which implies $r(Y|X') > r(Y|X)$. □

5.1 AK

The results in this section show how we reduce the computational cost of applying AK to the detection of non-algebraic matroids. We achieve this by identifying combinations of flats of the matroid for which the matroid is guaranteed to have an AK extension.

Proposition 5.3 *Let $\mathcal{M} = (Q, r)$ be a matroid of rank k. Let $X, Y \subseteq Q$ be a disjoint, non-modular pair of flats of $\mathcal{M}$ such that their union is a circuit of $\mathcal{M}$. Then $\mathcal{M}$ admits an AK extension $\mathcal{M}'$ for (X, Y).*

Proof Let $r(X) = \ell, r(Y) = m$ and $|XY| = s$. Since X and Y are disjoint, $s = \ell + m$. Now, let $\mathcal{M}' = (Qx_o, r)$ be the proper point extension of $\mathcal{M}$ corresponding to the modular cut $\mathcal{F}_X$. We show that $\mathcal{M}'$ is an AK extension for (X, Y). We have that $r(x_o|X) = 0$ and $r(X|x_o) = \ell - 1$. Also, note that

$$r(X|Y) = r(XY) - r(Y) = (|XY| - 1) - r(Y) = s - 1 - m = \ell - 1.$$

Any $X' \subset X$ is independent. Therefore, for every $X' \subset X$,

$$r(X'|x_o) = r(X'x_o) - 1 = |X'| + 1 - 1 = |X'| \text{ and}$$

$$r(X'|Y) = r(X'Y) - m = |X'| + m - m = |X'|,$$

completing the proof. □

Lemma 5.4 *Let $\mathcal{M} = (Q, r)$ be a matroid and let $X, Y \subseteq Q$ be a non-modular pair of flats of $\mathcal{M}$ such that $r(X) = 2$. Then $\mathcal{M}$ admits an AK extension for (X, Y).*

Proof Let $\mathcal{M}' = (Qx_o, r)$ be the proper point extension of $\mathcal{M}$ corresponding to $\mathcal{F}_X$. By Lemma 5.2, $r(X|Y) = 1$ and $r(X \cap Y) = 0$. Hence, for every flat $X' \subset X$ of rank-1, $r(X'|Y) = 1$ and

$$r(X'|x_o) = r(X'x_o) - r(x_o) = 2 - 1 = 1$$

Hence, $\mathcal{M}'$ is an AK extension of $\mathcal{M}$ by x_o. □

Lemma 5.5 *Let $\mathcal{M} = (Q, r)$ be a matroid of rank k and let $X, Y \subseteq Q$ be disjoint flats of $\mathcal{M}$. If Y is a hyperplane then $\mathcal{M}$ admits an AK extension for (X, Y).*

Proof Observe that the rank of the AK information of (X, Y) is

$$r(X; Y) = r(X) + r(Y) - r(XY) = r(X) + k - 1 - k = r(X) - 1.$$

Since AK extensions always exist for modular pairs (see Lemma 3.8), the case $r(X) = 2$ is trivial. Suppose that $r(X) > 2$. Consider the matroid (Qe_1, r) corresponding to the modular cut $\mathcal{F}_X$. Observe that $\mathrm{cl}(X_1e_1) = Xe_1$ for every flat $X_1 \subset X$ such that $r(X_1) = r(X) - 1$. Next, consider the matroid (Qe_1e_2, r) corresponding to the modular cut $\mathcal{F}_{Xe_1}$ and see that $\mathrm{cl}(X_2e_1e_2) = Xe_1e_2$ for every flat $X_2 \subset X$ such that $r(X_2) = r(X) - 2$. It is clear that one can continue this until we have $\mathrm{cl}(X_ce_1e_2 \dots e_c) = Xe_1e_2 \dots e_c$ for $c = r(X; Y)$ and for every flat $X_c \subset X$ such that $r(X_c) = r(X) - c$. Now, set $Z = e_1e_2 \dots e_c$. We have that, for every $X' \subseteq X$, $r(Z|X) = 0$ and $r(X'|Z) = r(X'Z) - r(Z) = r(X) - r(Z) = r(X) - c = 1 = r(X'|Y)$. Hence, (QZ, r) is an AK extension for (X, Y). □

Lemma 5.6 *Let $\mathcal{M} = (Q, r)$ be a matroid and let $H_1, H_2 \subseteq Q$ be hyperplanes of $\mathcal{M}$. Then $\mathcal{M}$ admits a CI extension for (H_1, H_2).*

Proof If H_1 and H_2 are modular, then it is enough to take the extension corresponding to the modular cut generated by their intersection. In the case where they are non-modular, take $\mathcal{F} = \{H_1, H_2, Q\}$. Since H_1 and H_2 are non-modular hyperplanes of $\mathcal{M}$, then $\mathcal{F}$ is the smallest modular cut of $\mathcal{M}$ generated by H_1 and H_2, and hence, $\mathcal{M}$ admits a proper point extension corresponding to $\mathcal{F}$, and therefore, a CI extension for (H_1, H_2). □

This next result takes into account the following fact. If X and Y are flats of a sparse paving matroid of rank k such that $r(X) + r(Y) \leq k$, then (X, Y) is a modular pair. While the result only applies to sparse paving matroids, its importance comes from the fact that sparse paving matroids are conjectured to predominate in any asymptotic enumeration of matroids [31, 32, 36]. Hence, results applying to such matroids will affect almost all matroids, asymptotically.

Proposition 5.7 *Let $\mathcal{M} = (Q, r)$ be a sparse paving matroid of rank k. Let $X, Y \subseteq Q$ be a disjoint, non-modular pair of flats of $\mathcal{M}$ such that $r(X) + r(Y) = k + 1$ and X is not a circuit-hyperplane. Then $\mathcal{M}$ admits an AK extension with respect to (X, Y).*

Proof First, note that if Y is a hyperplane (resp. X is a line), then Lemma 5.5 (resp. 5.4) applies. Therefore, since $r(X) + r(Y) = k + 1$, we have $r(X), r(Y) \leq k - 2$. Hence X and Y are independent because M is paving.

Since X and Y are disjoint independent sets, then $|XY| = |X| + |Y| = k + 1$, and since all sets of size greater than k have rank k, then $r(XY) = k$.

Any two subsets $Z_1, Z_2 \subset XY$ with $|Z_1| = |Z_2| = k$ have $|Z_1 \cap Z_2| = k - 1$. Then, by Lemma 5.1, there is at most one circuit-hyperplane in XY. If XY is a circuit, then Proposition 5.3 applies.

Now consider the case that XY contains a circuit-hyperplane. Let $X_1 \subseteq X$ and $Y_1 \subseteq Y$ be such that X_1Y_1 is a circuit-hyperplane. Without loss of generality, let $X_1 \subset X$ and $Y_1 = Y$. Let (Qx_o, r) be the extension of $\mathcal{M}$ corresponding to $\mathcal{F}_{X_1}$. It is

Table 1 Time taken to check AK for (5, 9) matroid 100736

3-Set AK	2-Set AK	2-Set AK with GE heuristic
$\approx$ 15 h	$\approx$ 1 h	$<$ 1 min

clear that (AK1) is trivially satisfied. For (AK2), first, we have $r(X|x_o) = r(X) - 1 = r(X|Y)$. And for all $X' \subset X$ such that $X' \neq X_1$, we have that, by independence of $X'x_0$ and $X'Y$, $r(X'|x_o) = |X'| = r(X'|Y)$, since no such X' is in $\mathcal{F}_{X_1}$. And finally, for $X_1 \subset X$, first note that $r(X_1) = r(X) - 1$ and so $r(X_1|x_o) = r(X) - 2$. Then, observe that $r(X_1|Y) = k - 1 - r(Y) = r(X) - 2$, which concludes the proof. □

From [5, Lemma 3.20], we know that, to check if a matroid $\mathcal{M}$ satisfies CI, it is enough to take pairs (X, Y) where X and Y are flats of the matroid. And from [19, Proposition 3.15], we know that a CI extension of $\mathcal{M}$ for (X, Y) is also an AK extension of $\mathcal{M}$ for the same pair.

Now, if a matroid satisfies the generalized Euclidean intersection (GE) property, then it also satisfies CI. This was first observed in [7] and we formalize it next.

Proposition 5.8 *Let $\mathcal{M} = (Q, r)$ be a matroid. For any non-modular pair of flats (X, Y) of $\mathcal{M}$, if $\mathcal{M}$ admits a GE extension for (X, Y), then it also admits a CI extension for the same pair.*

Thus, taking this into account, we see that checking if a matroid satisfies the AK property can be done even more efficiently by first eliminating the pairs for which the matroid admits a GE extension. In our experience, this leaves only a very limited number of pairs to check. Then, where possible, one can now apply the other results shown here to these remaining pairs. To illustrate just how much time is saved using this approach, we compare 3 different approaches used to check 1-AK for the (5, 9) matroid with Bollen identifier[1] 100736 in Table 1.

5.2 DL

In the case of the DL property, we note that, interestingly, all the optimizations shown above for AK also apply. We state and prove those results here, starting with the DL counterpart for Proposition 5.3.

Proposition 5.9 *Let $\mathcal{M} = (Q, r)$ be a matroid and let $X, Y \subseteq Q$ be a disjoint non-modular pair of flats such that XY is a circuit. Then X is a quasi-intersection of (X, Y).*

Proof Here, $r(XY) = r(X) + r(Y) - 1$, and so $r(Y|X) = r(Y) + r(X) - 1 - r(X) = r(Y) - 1$. And for every flat $X' \subset X$, $X'Y$ is independent; hence, we have $r(Y|X') = r(Y) + r(X') - r(X') = r(Y) > r(Y|X)$, completing the proof. □

[1] This refers to the way these matroids are organized in the computer programs available at https://github.com/gpbollen/Algebraicity-of-Matroids-and-Frobenius-Flocks/blob/master/Matroid Encyclopedia.ipynb.

This next one combines Lemmas 5.4, 5.5, and 5.6 into one result for DL.

Lemma 5.10 *Let X and Y be non-modular flats of a matroid $\mathcal{M} = (Q, r)$. If X is a line or Y is a hyperplane, then X is a quasi-intersection of (X, Y) in $\mathcal{M}$.*

Proof By Lemma 5.2 (i), if X is a line then $r(X \cap Y) = 0$. Hence $r(X'Y) = r(XY) = r(Y) + 1$ for every non-trivial flat $X' \subset X$ and $r(Y|X') > r(Y|X)$, completing the proof for when X is a line. The proof for when Y is a hyperplane follows immediately from Lemma 5.2 (ii). □

Finally, we have the DL counterpart for Proposition 5.7.

Proposition 5.11 *Let $\mathcal{M} = (Q, r)$ be a sparse paving matroid of rank k and let $X, Y \subseteq Q$ be a disjoint non-modular pair of flats. If $r(X) + r(Y) = k + 1$ and X is not a circuit-hyperplane, then there is a quasi-intersection of (X, Y) in $\mathcal{M}$.*

Proof The proof analogously follows that of its AK counterpart, so some details are omitted.

If Y is a hyperplane then Lemma 5.10 applies. Since $r(X \cap Y) = 0$, then $|XY| = |X| + |Y| = k + 1$ and $r(XY) = k$. If there is no circuit-hyperplane in XY then Proposition 5.9 applies. We finish by considering the case where XY contains a circuit-hyperplane.

For all flats $X' \subset X$ such that $X'Y$ is not a circuit-hyperplane, $r(Y|X') = r(Y) > r(Y|X)$ by the independence of X' and Y. Now, let $X_1 \subseteq X$ and $Y_1 \subseteq Y$ be such that X_1Y_1 is a circuit-hyperplane. If $X_1 \subset X$, then $r(X_1) = r(X) - 1$ and $r(Y|X_1) = r(X_1Y) - r(X_1) = k - 1 - r(X) + 1 = r(Y|X)$. Therefore, X_1 is a quasi-intersection of (X, Y) in $\mathcal{M}$. □

In general, we do not know if there is any link between DL and AK properties, but in the special case of rank-4 matroids, we have the following.

Proposition 5.12 *Let $\mathcal{M} = (Q, r)$ be a rank-4 matroid. Then it admits a DL extension if and only if it admits an AK extension that is a matroid.*

Proof Firstly, by Lemmas 5.10, 5.4, and 5.5, we only need to concern ourselves with non-modular pairs of flats (X, Y) of $\mathcal{M}$ where X is a hyperplane and Y is a line. Let $\mathcal{L}$ be the family of lines $X' \subset X$ satisfying that $X'Y$ is a hyperplane.

If $|\mathcal{L}|$ is 0 (resp., 1), then X (resp., $X' \in \mathcal{L}$) is a quasi-intersection of (X, Y), and $\mathcal{F}_X$ (resp., $\mathcal{F}_{X'}$) is the modular cut corresponding to an AK extension of (X, Y).

Now suppose that $|\mathcal{L}| > 1$. Note that

(i) $r(Y|X') = r(X'|Y) = r(Y|X) = 1$ for every $X' \in \mathcal{L}$, and
(ii) $r(Y|L) = r(L|Y) = 2$ for every line $L \subset X, \notin \mathcal{L}$.

Suppose that $\mathcal{M}$ admits a DL extension $\mathcal{M}'$. By (DL2) and (i), there exists T such that $T \in \mathrm{cl}_{\mathcal{M}'}(X')$ for every $X' \in \mathcal{L}$. Hence, $r(X'|T) = 1$. Also, $r(L|T) = r(L)$ for every line $L \subset X$, $L \notin \mathcal{L}$, proving (AK2). Hence, $\mathcal{M}'$ is an AK extension for (X, Y).

Now suppose that $\mathcal{M}'$ is an AK extension, and let $z_o = \mathrm{AK}(X, Y)$. For every flat $X' \subset X$, it is clear that when $r(X'|z_o) < r(X')$ then $r(z_o|X') = 0$ and $X' \in \mathcal{L}$. On the other hand, if $r(X'|z_o) = r(X')$ then $r(z_o|X') = 1$ and X' is a line not in $\mathcal{L}$ or $r(X') < 2$. Hence, z_o is a quasi-intersection of (X, Y) and $\mathcal{M}'$ is also a DL extension for (X, Y). □

6 Some new non-algebraic matroids

Using recursive applications of the DL and AK properties, we were able to discover some new non-almost entropic and/or non-algebraic matroids on 9 and 10 points.

Every almost entropic polymatroid $\mathcal{S}$ admits at least one AK extension for each pair of subsets (X, Y) of its ground set [7, 19]. Taking k pairs of subsets, we can find recursively an entropic polymatroid that is a recursive AK extension of $\mathcal{S}$.

Hence, to show that a matroid is not almost entropic, it is enough to find a sequence of pairs of sets for which there is no polymatroid extension of the original matroid that contains AK information of these pairs of sets.

Example 6.1 Let $A_1 = \{0, 1, 2\}$, $A_2 = \{3, 4, 5\}$, $A_3 = \{6, 7, 8\}$, $B_1 = \{0, 3, 6\}$, $B_2 = \{1, 4, 7\}$, and $B_3 = \{2, 5, 8\}$. The Tic-Tac-Toe matroid (T_3) is the sparse paving $(5, 9)$ matroid with ground set $Q = A_1A_2A_3$ and circuit-hyperplanes $\mathcal{C}(T_3) = \{A_iB_j : i, j \in \{1, 2, 3\}$ and $(i, j) \neq (2, 2)\}$ [3]. It is a nonlinearly representable matroid that satisfies the Ingleton inequality [3, 6]. Its dual (T_3^*) is not 3-AK (proved in Proposition 4.14 of [5]) and is therefore not almost entropic nor algebraic. Let $\mathcal{M} = (Qe, r)$ be the identically self-dual (ISD), sparse paving $(5, 10)$ matroid with circuit-hyperplanes $\mathcal{C}(T_3) \cup \{Ce : C \in \mathcal{C}(T_3^*)\}$. Note that $\mathcal{M}\backslash e = T_3$ and $\mathcal{M}/e = T_3^*$. Since T_3 is not CI and so not folded linear [6], and T_3 is a minor of $\mathcal{M}$, then $\mathcal{M}$ is not folded linear. Applying AK at depth 3, we found that it is not almost entropic, and therefore, not algebraic using the following combinations:

$$\alpha = \mathtt{AK}(4578e, 36), \qquad \beta = \mathtt{AK}(1245e, 03),$$
$$\gamma = \mathtt{AK}(258e\alpha\beta, 17).$$

The matroid $\mathcal{M}$ is a smallest ISD, Ingleton-compliant (i.e., satisfies the Ingleton inequality [23]) matroid that is not almost entropic. Though it is 2-DL, we do not yet know if it is 3-DL.

The question of whether the Tic-Tac-Toe matroid is algebraic remains open.

Example 6.2 Consider the $(5, 9)$ matroids with the following Bollen identifiers [13]: 100735, 100736, 100755, 103147, and 147269. These matroids are Ingleton-compliant sparse paving matroids that are not 2-CI. They are also Frobenius flock representable and satisfy Ingleton–Main at all depths. While they satisfy Dress–Lovász up to depth 3, we do not yet know if they are 4-DL. In any case, they are neither almost entropic nor algebraic as we found that they fail AK at depth 4 using the following:

$$\alpha = \mathtt{AK}(12678, 03), \qquad \beta = \mathtt{AK}(03678\alpha, 15),$$
$$\gamma = \mathtt{AK}(1257\alpha\beta, 48), \qquad \tau = \mathtt{AK}(0357\alpha\gamma, 26).$$

These matroids are among the smallest Ingleton-compliant sparse paving matroids that are not almost entropic. Since they are from the family mentioned in [5, Sect. 4.5.2], it is likely that many of those matroids will also not be almost entropic

Example 6.3 In [13], Bollen found all matroids that are not algebraic due to failing the Ingleton–Main lemma at depths up to 5 for (4, 9) and (5, 9) matroids. Due to time

Table 2 Dress–Lovász (DL) and Ingleton–Main (IM) check

(r, n)	(4, 8)	(4, 9)	(5, 9)
DL	39	27,137	27,137
DL depth 2	39	27,137	27,137
IM depth 3	39	28,418	27,144
IM depth 4	39	30,171	27,442
IM depth 5	39	30,658	27,500
DL depth 6	39	31,104	?
DL depth 7	39	31,370	?
DL depth 8	39	31, 373*	?

constraints, he was not able to find all (4, 9) matroids that fail the same property at depth 6, leaving some unchecked. Going at these unchecked matroids, we were able to find all that are not 6-DL and as well as those that are not 7-DL. And since DL and the Ingleton–Main lemma are equivalent for rank-4 matroids, then these are also the remaining (4, 9) matroids that fail Ingleton–Main at depths 6 and 7. These matroids are listed in [8]. Time constraints meant we were not able to do an exhaustive check for non-8-DL matroids. However, by randomly selecting and testing, we were able to find a few non-8-DL (4, 9) matroids. These are matroids 5635, 7262, and 103732. A summary of these results is shown in Table 2, which is an update on [13, Table 6]. That is, we updated the values for DL of depth 6,7, and 8, as discussed above. For depth 8, the search is not exhaustive, and so this number is a lower bound.

In addition to being non-algebraic, we found matroid 129075, a non-6-DL matroid, to be non-almost entropic due to failing AK at depth 6 with the following combinations:

$$\alpha = \mathtt{AK}(2678, 35), \qquad \beta = \mathtt{AK}(2356\alpha, 14),$$
$$\gamma = \mathtt{AK}(01234\beta, 57), \qquad \tau = \mathtt{AK}(01234\beta\gamma, 67),$$
$$\mu = \mathtt{AK}(3468, \alpha\gamma), \qquad \nu = \mathtt{AK}(2678\alpha\tau, \beta\mu).$$

As for the other (4, 9) matroids we found to be non-algebraic, we do not yet know if they are almost entropic.

7 Secret-sharing schemes

We conclude this work presenting new results on secret-sharing schemes obtained with the improvements of the AK technique presented in this paper. For an introduction to secret sharing, and more detailed definitions, see [6, 9, 34].

In order to get information-theoretic lower bounds on the efficiency of these schemes, we consider the following definition. A *secret-sharing scheme* on a set $P = \{1, 2, \ldots, n\}$ is a collection of discrete random variables $\Sigma = (S_0, S_1, \ldots, S_n)$ such that $H(S_0) > 0$ and $H(S_0|S_P) = 0$, where H is the Shannon entropy and S_0 is the random variable associated to the *dealer*, p_0.

We say that a subset $X \subseteq P$ is *authorized* if $H(S_0|S_X) = 0$, and we say that a subset is *forbidden* if $H(S_0|S_X) = H(S_0)$. In this work, we only consider *perfect* schemes, that is, schemes where every subset is either authorized or forbidden. The family of authorized subsets is called the *access structure* of the scheme, and it is denoted by Γ. The *information ratio* of the scheme is a measure of the scheme's efficiency given as $\max_i\{H(S_i)\}/H(S_0)$. If the information ratio is 1, we say that the scheme is *ideal*.

The access structure of ideal secret-sharing schemes is ports of matroids [14]. However, the converse is not true: Only ports of entropic matroids admit ideal schemes [14, 27, 37].

For a given access structure Γ, the infimum of the information ratio of all schemes realizing Γ is denoted as $\sigma(\Gamma)$. Bounds on this value can be obtained using information inequalities. Csirmaz [15] found a family of access structures $\{\Gamma_n\}_n$ satisfying that $\sigma(\Gamma_n) = \Omega(n/\log n)$. This is the best known lower bound for the information ratio. For matroid ports, finding non-trivial lower bounds requires using non-Shannon information inequalities, but until now all lower bounds that have been found are constant and smaller than 2 [6, 10, 19, 21].

Matroids that do not satisfy the AK property are not entropic. Therefore, they do not admit ideal schemes and the ports of such matroids will require schemes with information ratio greater than 1.

In this work, we improved the linear programming problems introduced in [19] with the optimizations presented in Theorem 4.1 and in Definition 3.7. The resulting linear programming problem is presented below. We define $Q = Pp_0$. The conditions for (QZ, f) being compatible with Γ are explained in [6, 19].

Linear Programming Problem 7.1 Let $X, Y \subseteq P$. The optimal value of this linear programming problem is a lower bound on $\sigma(\Gamma)$.

$$\begin{aligned} \text{Minimize} \quad & v \\ \text{subject to} \quad & v \geq f(x) \text{ for every } x \in P \\ & (QZ, f) \text{ is a polymatroid compatible with } \Gamma \\ & \text{(AK1), (AK2}') \text{ on } Z \text{ and } (X, Y) \end{aligned}$$

By solving LP 7.1 for the ports of the non-Ingleton-compliant matroids on 8 points, we were able to improve the bounds on $\sigma(\Gamma)$ for a number of them. In the case of some of the ports of the Q_8 matroid, the new AK definition (Definition 3.7) gave better bounds than the old one (see Sect. 3.2). Perhaps, this is an indication of the strength of the new definition over the previous one. Using this new definition, we now have that the current best bound on $\sigma(\Gamma)$ for a matroid port is 52/45, which was obtained for some of the ports of the $AG(3, 2)'$ matroid. Apart from the already mentioned ports of the Q_8 matroid which lower bound was gotten using 2-AK, the other results here were gotten using 4-AK. The bounds for the ports of the named matroids presented in Table 3 also match those gotten for the same matroid ports using the copy lemma [21], evidencing that even without knowing if there are any symmetries inherent in the matroid, the AK lemma can still be used to get bounds that are on par with those gotten when symmetry conditions are taken into account in using the copy lemma.

Table 3 Improved lower bounds on $\sigma(\Gamma)$ for some 8-point matroids. Best previous bounds were from [6] unless specified

Matroid	Port	Previous bound	Improved bound
1490	0, 2, 3, 4, 5, 6	8/7	53/46
1491	0, 3, 7	33/29	8/7
1491	2, 4, 6	8/7	84/73
1492	0, 1, 2, 3, 6, 7	49/43	38/33
1499	0, 2, 3, 4, 5, 6	8/7	38/33
1500	0, 2, 4, 5	8/7	38/33
1501	0, 1, 2, 3, 6, 7	33/29	8/7
1502	2, 3, 4, 7	33/29	8/7
1525	0, 2, 4, 5	33/29	8/7
1526	0, 2, 3, 4, 5, 6	8/7	38/33
1532	0, 1, 2, 3, 5, 6	33/29	8/7
1579	0, 2, 4, 5	33/29	8/7
$AG(3,2)'$	1, 3, 5, 7	49/43	52/45
F_8	3, 4, 5, 6	23/20 [21]	38/33
Q_8	1, 4, 6, 7	49/43	8/7

Table 4 Bounds on $\sigma(\Gamma)$ for some non-AK (5,9) matroids

Matroid	Sets	Best bound
100735	{1, 2, 6, 7, 8}, {0, 3}	$1.011\bar{36} = 89/88$
100755	{0, 3, 6, 7, 8, 9}, {1, 5}	
100736	{1, 2, 5, 7, 9, 10}, {8, 4}	
103147	{3, 5, 7, 0, 9, 11}, {2, 6}	
147269		

In addition to these 8-point matroids, we also present new bounds on $\sigma(\Gamma)$ for ports of the 9-point matroids described in Example 6.2. For each of these matroids, there is at least a port for which $\sigma(\Gamma) \geq 89/88$. This was the best bound we got for ports of these matroids. However, since we only tried one combination of sets to get the bounds, we do not rule out the possibility that other combinations might produce better bounds. These are shown in Table 4.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

1. Ahlswede, R., Körner, J.: On the connection between the entropies of input and output distributions of discrete memoryless channels. In: Proceedings of the 5th Brasov Conference on Probability Theory, Brasov, 1974. Editura Academiei, Bucuresti, pp. 13—23 (1977)
2. Ahlswede, R., Körner, J.: Appendix: on common information and related characteristics of correlated information sources. In: Ahlswede, R., Bärumer, L., Cai, N., Aydinian, H., Blinovsky, V., Deppe, C., Mashurian, H. (eds.) General Theory of Information Transfer and Combinatorics, pp. 664–677. Springer, Berlin (2006)
3. Alfter, M., Hochstättler, W.: On pseudomodular matroids and adjoints. Discrete Appl. Math. **60**, 3–11 (1995)
4. Bachem, A., Wanka, A.: Euclidean intersection properties. J. Combin. Theory Ser. B **47**, 10–19 (1989)
5. Bamiloshin, M.: Common information techniques for the study of matroid representation and secret sharing schemes. Ph.D. thesis. Universitat Rovira i Virgili (2021)
6. Bamiloshin, M., Ben-Efraim, A., Farràs, O., Padró, C.: Common information, matroid representation, and secret sharing for matroid ports. Des. Codes Cryptogr. **89**, 143–166 (2021)
7. Bamiloshin, M., Farràs, O., Padró, C.: A note on extension properties and representations of matroids. Discrete Appl. Math. **376**, 270–280 (2025)
8. Bamiloshin, M., Farràs, O.: Optimizing extension techniques for discovering non-algebraic matroids. arXiv:2406.18359 (2024)
9. Beimel, A.: Secret-sharing schemes: a survey. In: International Conference on Coding and Cryptology, pp. 11–46 (2011)
10. Beimel, A., Livne, N., Padró, C.: Matroids can be far from ideal secret sharing. In: Fifth Theory of Cryptography Conference, TCC 2008, Lecture Notes in Computer Science, vol. 4948, pp. 194–212 (2008)
11. Ben-Efraim, A.: Secret-sharing matroids need not be algebraic. Discrete Math. **339**(8), 2136–2145 (2016)
12. Björner, A., Lovász, L.: Pseudomodular lattices and continuous matroids. Acta Sci. Math. **51**, 295–308 (1987)
13. Bollen, G.P.: Frobenius flocks and algebraicity of matroids. Ph.D. thesis. Technische Universiteit Eindhoven, Eindhoven (2018)
14. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. Cryptology **4**, 123–134 (1991)
15. Csirmaz, L.: The size of a share must be large. J. Cryptology **10**, 223–231 (1997)
16. Dougherty, R., Freiling, C., Zeger, K.: Networks, matroids, and non-Shannon information inequalities. IEEE Trans. Inform. Theory **53**(6), 1949–1969 (2007)
17. Dress, A., Lovász, L.: On some combinatorial properties of algebraic matroids. Combinatorica **7**(1), 39–48 (1987)
18. Rouayheb, S., Sprintson, A., Georghiades, C.: On the index coding problem and its relation to network coding and matroid theory. IEEE Trans. Inform. Theory **56**(7), 3187–3195 (2010)
19. Farràs, O., Kaced, T., Martín, S., Padró, C.: Improving the linear programming technique in the search for lower bounds in secret sharing. IEEE Trans. Inform. Theory **66**(11), 7088–7100 (2020)
20. Fujishige, S.: Polymatroidal dependence structure of a set of random variables. Inf. Control **39**, 55–72 (1978)
21. Gürpinar, E: Symmetries in linear programming for information inequalities. ISIT, pp. 760–765 (2022)
22. Gürpinar, E., Romashchenko, A.E.: How to use undiscovered information inequalities: direct applications of the copy lemma. ISIT, pp. 1377–1381 (2019)
23. Ingleton, A.W.: Representation of matroids. In: Welsh, D.J.A. (ed.) Combinatorial Mathematics and Its Applications, pp. 149–167. Academic Press, London (1971)
24. Ingleton, A.W., Main, R.A.: Non-algebraic matroids exist. Bull. Lond. Math. Soc. **7**, 144–146 (1975)
25. Lindström, B.: The non-Pappus matroid is algebraic. Ars Combin. **16**(B), 95–96 (1983)
26. Lindström, B.: A generalization of the Ingleton-Main lemma and a class of non-algebraic matroids. Combinatorica **8**(1), 87–90 (1988)
27. Matúš, F.: Matroid representations by partitions. Discrete Math. **203**, 169–194 (1999)
28. Matúš, F.: Classes of matroids closed under minors and principal extensions. Combinatorica **38**, 935–954 (2018)
29. Matúš, F.: Algebraic matroids are almost entropic. Proc. Amer. Math. Soc. **152**(01), 1–6 (2024)

30. Mayhew, D., Royle, G.F.: Matroids with nine elements. J. Combin. Theory Ser. B **98**, 415–431 (2008)
31. Mayhew, D., Welsh, D.: On the number of sparse paving matroids. Adv. Appl. Math. **50**(1), 125–131 (2013)
32. Mayhew, D., Newman, M., Whittle, G., Welsh, D.: On the asymptotic proportion of connected matroids. European J. Combin. **32**, 882–890 (2011)
33. Oxley, J.G.: Matroid Theory, 2nd edn. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York (2011)
34. Padró, C.: Lecture Notes in Secret Sharing. Cryptology ePrint Archive, Report 2012/674 (2012)
35. Pendavingh, R., Zwam, S.H.M.: Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. Adv. Appl. Math. **50**(1), 201–227 (2013)
36. Pendavingh, R., Pol, J.G.: On the number of matroids compared to the number of sparse paving matroids. Electron. J. Combin. **22**, 1–17 (2014)
37. Seymour, P.D.: On secret-sharing matroids. J. Combin. Theory Ser. B **56**, 69–73 (1992)
38. Simonis, J., Ashikhmin, A.: Almost affine codes. Des. Codes Cryptogr. **14**(2), 179–197 (1998)
39. Sun, Q., Ho, S. T., Li, S. Y. R.: On network matroids and linear network codes. ISIT, pp. 1833–1837 (2008)