Combinatorica April 13, 2017

Classes of matroids closed under minors and principal extensions*

František Matúš †

Abstract. This work studies the classes of matroids that are closed under minors, addition of coloops and principal extensions. To any matroid M in such a class a matroid M° is constructed such that it contains M as a minor, has all proper minors in the class and violates Zhang-Yeung inequality. When the class enjoys the inequality the matroid M° becomes an excluded minor. An analogous assertion was known before for the linear matroids over any infinite field in connection with Ingleton inequality. The result is applied to the classes of multilinear, algebraic and almost entropic matroids. In particular, the class of almost entropic matroids has infinitely many excluded minors.

1. Introduction

In matroid representation theory, configurations of vectors in linear spaces or points in projective geometries have been intensively investigated for decades. Classes of *linear* matroids over fields are traditional. Configurations of subspaces of a linear space occasionally give rise to integer multiples of the matroidal rank functions, and thus to *multilinear* matroids. In the transcendental field extension theory, the algebraic dependence exhibits the matroidal structure as well, inducing *algebraic* matroids.

It is likely less known that a matroid can be represented by a random vector indexed by the ground set. The collection of Shannon entropies of all subvectors sometimes provides a multiple of a matroidal rank function. This forces the distribution of the vector to obey a highly regular form. In an equivalent approach, perhaps the most straightforward to start with, configurations in the lattices of partitions are examined, see Remark 2. The resulting matroids are called here *partition representable* [27]. The matroidal rank

*This work was supported by Grant Agency of the Czech Republic under Grant 13-20012S.

AMS 2000 Mathematics Subject Classification. Primary 05B35; secondary 94A17, 94A24.

Key words and phrases. Matroid, polymatroid, excluded minor, principal extension, multilinear matroid, algebraic matroid, partition representable matroid, almost entropic matroid, Ingleton inequality, Zhang-Yeung inequality, ideal secret sharing, almost affine code, selfadhesivity.

†F. Matúš is with Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Pod vodárenskou věží 4, 182 08 Prague, Czech Republic (matus@utia.cas.cz).

functions can also become limits of the collections of the Shannon entropies of random subvectors in which case *almost entropic* matroids arise [28].

Rigorous definitions of the above notions, known relations between them, discussion and references are presented in Section 2. Figure 1 may provide initial insight.

The present work unfolds from [31, Theorem 1.1] asserting that over an infinite field any linear matroid is a minor of a non-linear matroid whose proper minors are linear. The latter matroid violates the Ingleton inequality [31, p. 688], a classical necessary condition for linear representability. As a corollary there exist infinitely many excluded minors for the class of linear matroids over any infinite field.

The first result of this work opens a unified viewpoint of the structure of some classes of matroids and their excluded minors. It features, for the first time in this context, Zhang-Yeung inequality (6), originally proved for Shannon entropies in [42, Theorems 3 and 5]. The inequality is weaker than Ingleton one.

Theorem 1. *Let $\mathcal{M}$ be a class of matroids that is closed under minors, addition of coloops and principal extensions. Given any $\mathsf{M} \in \mathcal{M}$, a matroid M° exists such that*
(i) M is a proper minor of M°,
(ii) each proper minor of M° belongs to the class $\mathcal{M}$,
(iii) M° violates Zhang-Yeung inequality.

The presented proof is based on six lemmas. Section 3 reviews the principal extensions, presents three lemmas and recalls Zhang-Yeung inequality. An *encompassing* matroid $\mathsf{M}_{\text{enc}} \in \mathcal{M}$ is constructed to contain M as a minor in Section 4. It serves for the majority of computations and argumentations. In Section 5, the matroid M° is obtained from a restriction of M_{enc} by relaxation, and Theorem 1 is proved. The construction mimics that of the Vámos matroid.

Theorem 1 is applied to above classes of matroids in Section 2 where several new results are summarized in Theorem 2. The proof is presented in Section 6 and is preceded by lemmas on principal extensions of representable matroids.

2. Excluded minors for classes of matroids

A matroid $\mathsf{M} = (N, r)$ consists of a finite ground set N and rank function r [33].

Over a field $\mathbb{F}$, the matroid M is *multilinear* of degree $\delta \geqslant 1$ if there exist subspaces E_i, $i \in N$, of a linear space over $\mathbb{F}$ such that $\delta \cdot r(I) = \dim E_I$, $I \subseteq N$. Here, E_I denotes the inner sum $\bigoplus_{i \in I} E_i$. In the special case $\delta = 1$, the *linear* matroids over $\mathbb{F}$ arise.

The matroid M is *algebraic* over a field $\mathbb{F}$ if there exist not necessarily different elements e_i, $i \in N$, of an extension field of $\mathbb{F}$ such that $r(I) = \dim_{\text{tr}} \mathbb{F}(I)$ for $I \subseteq N$. Here, $\dim_{\text{tr}}$ denotes the transcendence dimension over $\mathbb{F}$ and $\mathbb{F}(I)$ the smallest subfield of the extension field that contains $\mathbb{F}$ and $\{e_i \colon i \in I\}$.

The matroid M is *partition representable* of the degree $d \geqslant 2$ if a $d^{r(N)}$-element set Ω admits partitions π_i, $i \in N$, such that the meet-partition $\pi_I = \bigwedge_{i\in I} \pi_i$ has $d^{r(I)}$ blocks of the same size, $I \subseteq N$ [27].

A polymatroid $\mathsf{M} = (N, h)$ has a real-valued rank function h [24, 32].

For random variables ξ_i, $i \in N$, that take only finitely many values, the mapping that sends $I \subseteq N$ to the Shannon entropy of $(\xi_i \colon i \in I)$ is a polymatroidal rank function [9]. The polymatroids constructed in this way are called *entropic*. Their rank functions exhaust the entropy region [30].

A polymatroid (N, g) is called *almost entropic* if there exists a sequence of entropic polymatroids (N, h_n) such that $h_n \to g$, pointwise, thus if g belongs to the closure of the entropy region. This defines in particular the *almost entropic* matroids, represented by infinite sequences of the distributions of random vectors. The class of these matroids has an appeal because it provides a description of the entropy regions [28, Theorem 5].

The classes of matroids defined above are denoted by $\mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},\delta}$, $\mathcal{M}^{\mathrm{alg}}_{\mathbb{F}}$, $\mathcal{M}^{\mathrm{pare}}_{d}$ and $\mathcal{M}^{\mathrm{aent}}$, respectively. Let further

$$\begin{aligned}
\mathcal{M}^{\mathrm{lin}}_{\mathbb{F}} &\triangleq \mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},1}\,, & \mathcal{M}^{\mathrm{lin}} &\triangleq \textstyle\bigcup_{\mathbb{F}} \mathcal{M}^{\mathrm{lin}}_{\mathbb{F}}\,,\\
\mathcal{M}^{\mathrm{mlin}}_{\delta} &\triangleq \textstyle\bigcup_{\mathbb{F}} \mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},\delta}\,, & \mathcal{M}^{\mathrm{mlin}} &\triangleq \textstyle\bigcup_{\delta\geqslant 1} \mathcal{M}^{\mathrm{mlin}}_{\delta}\,,\\
\mathcal{M}^{\mathrm{alg}} &\triangleq \textstyle\bigcup_{\mathbb{F}} \mathcal{M}^{\mathrm{alg}}_{\mathbb{F}}\,, & \mathcal{M}^{\mathrm{pare}} &\triangleq \textstyle\bigcup_{d\geqslant 2} \mathcal{M}^{\mathrm{pare}}_{d}\,.
\end{aligned}$$

The unions over $\mathbb{F}$ in the definitions $\mathcal{M}^{\mathrm{lin}}$ and $\mathcal{M}^{\mathrm{mlin}}_{\delta}$ can equivalently run over the finite fields, by [33, Proposition 6.8.2 and 6.8.11]. Also the union in $\mathcal{M}^{\mathrm{alg}}$ does not change when restricted to the fields with the nonzero characteristic, by [33, Propositions 6.7.11, 6.8.2 and 6.7.10].

The following assertions summarize selected applications of Theorem 1.

Theorem 2. *Let $\mathcal{M}$ be any of the following classes of matroids: $\mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},\delta}$ for any infinite field $\mathbb{F}$ and $\delta \geqslant 1$, $\mathcal{M}^{\mathrm{mlin}}_{\delta}$ for $\delta \geqslant 1$, $\mathcal{M}^{\mathrm{mlin}}$, $\mathcal{M}^{\mathrm{alg}}_{\mathbb{F}}$ for any $\mathbb{F}$, $\mathcal{M}^{\mathrm{alg}}$ and $\mathcal{M}^{\mathrm{aent}}$. Every matroid in $\mathcal{M}$ is a minor of a matroid that is an excluded minor for $\mathcal{M}$.*

The assertions of Theorem 2 are new up to the class $\mathcal{M}^{\mathrm{lin}}_{\mathbb{F}}$ over any infinite field $\mathbb{F}$ which is [31, Theorem 1.1], conjectured earlier in [10].

Corollary 1. *Each of the classes in Theorem 2 has infinitely many excluded minors. They can have an arbitrarily large rank.*

The case $\mathcal{M}^{\mathrm{lin}}_{\mathbb{F}}$ over the field of real numbers goes back to [18]. For the classes $\mathcal{M}^{\mathrm{alg}}_{\mathbb{F}}$ and $\mathcal{M}^{\mathrm{alg}}$ the assertions of Corollary 1 appeared in [21]. Otherwise, it is new.

As a consequence of Corollary 1, the classes have infinitely many excluded minors which has been partially known, even much earlier. A sequence of matroids L_n that have rank three and the ground set of cardinality $2n+3$ was introduced in [7, p. 108], see also the figures in [11, p. 67] and [33, p. 218]. For n non-prime, L_n is an excluded minor for the linear representability and algebraic representability over any field by [11, Theorem 2]

and [20], respectively. The consequence for the three multilinear classes seems to be new. The matroid L_n with n non-prime is also an excluded minor for partition representability of any degree, by [27, Proposition 4.3], that classifies the partition representations of L_n up to isotopies. The existence of infinitely many excluded minors for $\mathcal{M}^{\text{aent}}$ was open.

The classes $\mathcal{M}^{\text{mlin}}_{\mathbb{F},\delta}$ with $\mathbb{F}$ finite and $\delta \geqslant 1$, and $\mathcal{M}^{\text{pare}}_{d}$, $d \geqslant 2$, do not feature in Theorem 2 because they are not closed under principal extensions. Actually, Rota's conjecture [35] states that $\mathcal{M}^{\text{lin}}_{\mathbb{F}}$ has finitely many excluded minors for $\mathbb{F}$ finite; for recent progress see [12].

Conjecture 1. *The class $\mathcal{M}^{\text{pare}}_{d}$, $d \geqslant 2$, has finitely many excluded minors.*

The cases $d = 2, 3$ reduce to the binary and ternary matroids [4, 26], respectively.

Figure 1 depicts inclusions among the classes $\mathcal{M}^{\text{lin}}$, $\mathcal{M}^{\text{mlin}}$, $\mathcal{M}^{\text{alg}}$, $\mathcal{M}^{\text{pare}}$ and $\mathcal{M}^{\text{aent}}$. For $\mathcal{M}^{\text{lin}}_{\mathbb{F}} \subseteq \mathcal{M}^{\text{alg}}_{\mathbb{F}}$ see [33, Proposition 6.7.10].

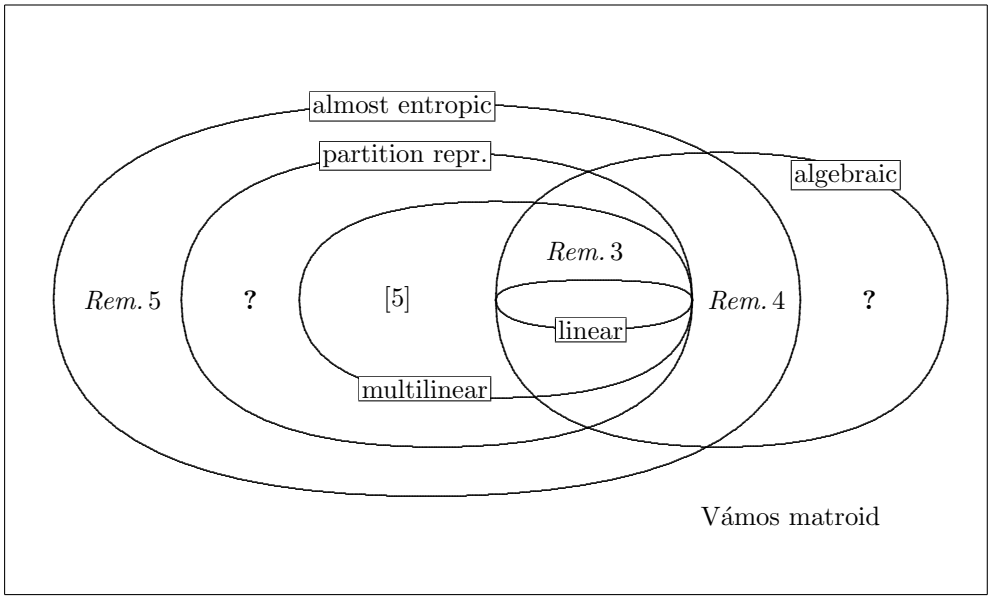

FIGURE 1. Classes of matroids.

Remark 1. The class of partition representable matroids contains the multilinear matroids. In fact, let M have a multilinear representation of the degree δ by subspaces E_i, $i \in N$, of a space of the dimension $\delta \cdot r(N)$ over a finite field $\mathbb{F}$. The dual of the space can play the role of Ω. The annihilator of E_I in Ω has the dimension $\delta[r(N)-r(I)]$ and $\mathbb{F}^{\,\delta \cdot r(I)}$ cosets, $I \subseteq N$. They are the blocks of a meet-partition π_I of Ω. Then, M is partition representable by π_i, $i \in N$, with $d = |\mathbb{F}|^{\delta}$. Thus, $\mathcal{M}^{\text{mlin}}_{\mathbb{F},\delta} \subseteq \mathcal{M}^{\text{pare}}_{d}$ and $\mathcal{M}^{\text{mlin}} \subseteq \mathcal{M}^{\text{pare}}$.

Remark 2. In a partition representation π_i, $i \in N$, of M, if Ω is endowed with the uniform probability measure and π_i are interpreted as factor mappings then they turn into random

variables ξ_i. The variables give rise to the entropic polymatroid $(N, r\cdot\ln d)$. For a converse see [26, Theorem]. The inclusion $\mathcal{M}^{\text{pare}} \subseteq \mathcal{M}^{\text{aent}}$ follows from the fact that the closure of the entropic region is a convex cone [41, Theorem 1].

Figure 1 shows also references to examples of matroids that have or do not have some representations simultaneously, and indicates two open problems.

Remark 3. The non-Pappus matroid is not linear but it is multilinear of the degree $\delta = 2$ over the field $\mathbb{F}$ whose cardinality is a power of 3 [37, 27]. It is algebraic over any field [19].

Remark 4. The direct sum of Fano and non-Fano matroids is algebraic, [14], [33, p. 216]. It is not partition representable by [27, Proposition 4.1] but it is almost entropic because the entropy region is closed under sums. The direct sum can be truncated to a connected matroid with the same properties. In fact, the truncation is expressible as a principal extension followed by a contraction [30, Lemma 4], so the class $\mathcal{M}^{\text{alg}}_{\mathbb{F}}$ is closed under truncations by Lemma 13. The class $\mathcal{M}^{\text{aent}}$ admits the truncations by [28, Theorem 2].

Remark 5. A nontrivial multilinear matroid that is not algebraic was constructed recently in [5], answering a question from [27, 5.5]. The direct sum of Fano matroid, non-Fano matroid and the matroid from [5] is almost entropic but neither partition representable nor algebraic. Truncations apply.

Since the appearance of [37] it has been an open problem, especially in a cryptographic disguise, whether the inclusion $\mathcal{M}^{\text{mlin}} \subseteq \mathcal{M}^{\text{pare}}$ is strict. This is indicated in Figure 1 by the question mark on the left. The question mark on the right expresses the following.

Conjecture 2. *The algebraic matroids are almost entropic.*

Vámos matroid is not linear [14], violating Ingleton inequality. It is not algebraic [15]. It was proved independently in [36] and [26, Section 7] that it is not partition representable. The most natural argument that Vámos matroid belongs to none of the classes considered here is that it violates even the Zhang-Yeung inequality. In fact, this inequality is valid for the entropic polymatroids, and therefore in $\mathcal{M}^{\text{aent}}$ by limiting. It holds in $\mathcal{M}^{\text{alg}}$ by Corollary 2.

Finally, a miscellany of the related literature is presented below.

For the linear representability see the chapters in [39, 7, 33]. Recent developments extend to the spaces over division or skew partial fields [34, 38]. Multilinear matroids feature in network coding [8] and cryptography [25, 2, 3].

Though the notion of algebraic matroids dates back to the very beginnings of the matroid theory it has been less studied for periods. Older reviews are in [22, 23]. Recent activities are related to algebraic geometry [16].

Partition representability can be defined equivalently via generalized quasigroup equations [27, Proposition 2.4]. The distribution of the random variables ξ_i, $i \in N$, representing a matroid is uniform on a set that corresponds to the almost affine code and

the matroid is then also called *almost affine* [37]. Partition representable matroids admit interpretation as the ideal secret sharing schemes which motivated the cryptographic community to call them *secret-sharing* [6]. The strict inclusion in $\mathcal{M}^{\rm mlin} \subseteq \mathcal{M}^{\rm pare}$ would imply existence of an ideal secret sharing scheme which is not multilinear. These equivalent approaches are discussed in [28, Discussion B,D][‡].

The rank functions of the entropic polymatroids need not satisfy the Ingleton inequality [13, 14], a well-known necessary condition for the multilinear representability, but they enjoy a weaker Zhang-Yeung inequality [42, Theorems 3 and 5], and a profusion of others [30]. The class $\mathcal{M}^{\rm aent}$ induces dense subsets of the entropy regions [28, Theorem 5].

The above notions have turned out to have motivation and relevance in many problems of the information theory, statistics, network coding, cryptography, game theory, group theory and elsewhere.

3. Preliminaries

This section reviews the principal extensions of polymatroids and Zhang-Yeung inequality. Three auxilliary lemmas are worked out for later purposes.

The principal extension [24, p. 245] of a polymatroid (N, f) by a single element $0 \notin N$ is constructed by a convolution and parallel extension. The *convolution* $f * g$ of f with a polymatroidal rank function g is defined by

$$f * g\,(I) = \min_{J \subseteq I} \big[\, f(J) + g(I \setminus J) \,\big]\,, \qquad I \subseteq N\,.$$

For $L \subseteq N$ the polymatroid $(N \cup 0, h)$ given by

$$h(J) = f(J) \text{ and } h(J \cup 0) = f(J \cup L)\,, \qquad J \subseteq N\,,$$

is called the *extension of* (N, f) *by* 0 *parallel to* L.

For a matroid $\mathsf{M} = (N, r)$, the *principal extension* $(N \cup 0, \bar{r})$ *of* M *by* 0 *at* L is obtained by convolving the extension of M by 0 parallel to L and the free matroid $(N \cup 0, |\cdot|)$. Thus, the rank function $\bar{r}$ is given by $\bar{r}(I) = r(I)$ and

$$\bar{r}(I \cup 0) = \min_{J \subseteq I} \min\big\{ r(J \cup L) + |(I \cup 0) \setminus (J \cup 0)|, r(J) + |I \cup 0 \setminus J| \big\}\,, \qquad I \subseteq N\,.$$

This extension is a matroid [24, Theorem 2.5]. By submodularity, the minimum over J is attained at $J = I$ whence

$$\bar{r}(I \cup 0) = \min\big\{ r(I \cup L), r(I) + 1 \big\}\,, \qquad I \subseteq N\,. \tag{1}$$

When L is a singleton the principal extension coincides with the parallel one. The rank $\bar{r}(I \cup 0)$ depends on I only through the closure of L in M and equals $r(I \cup L)$ if and only if L is contained in the closure of I in M. Thus, the principal extension at L coincides with that at the closure of L. If L is a flat of M the element 0 is interpreted as being freely

[‡]We decided to coin the term *partition representable* because of the succinct definition that seems to be amenable to broadest mathematical audience.

added to L, see [33, p. 270]. Principal extensions for polymatroids can be introduced analogously. Convolving with modular polymatroids, even an individual value at 0 can be adjusted but that generality does not occur here.

Extending a matroid principally two or more times is commutative [24, Proposition 2.8]. In the sequel, an explicit formula for the rank functions of multiple extensions is needed.

Let $\mathsf{M} = (N, r)$ be a matroid to be extended by elements of a finite set M that is disjoint with N. For $m \in M$ let $L_m \subseteq N$ be a set specifying parallelism. The *principal extension of* M *adding each* $m \in M$ *at* L_m is the matroid $(N \cup M, \bar{r})$ whose rank function is given by

$$\bar{r}(I \cup K) = \min_{D \subseteq K} \left[r\big(I \cup \textstyle\bigcup_{d \in D} L_d\big) + |K \setminus D| \right], \qquad I \subseteq N\,,\ K \subseteq M\,. \tag{2}$$

The formula is obtained by convolving the extension of M by each $m \in M$ in parallel at L_m and $(N \cup M, |\cdot|)$. If all L_m equal a single set $L \subseteq N$ then (2) reduces to

$$\bar{r}(I \cup K) = \min \big\{ r\big(I \cup L\big), r(I) + |K| \big\}, \qquad I \subseteq N\,,\ K \subseteq M\,. \tag{3}$$

Given a set N and disjoint copy N', let i' be the copy of $i \in N$ and $J' = \{j' \colon j \in J\}$, $J \subseteq N$. A second copy N'' is disjoint with $N \cup N'$, copying i to i'' and J to J''.

Any matroid $\mathsf{M} = (N, r)$ can be extended to $N \cup N'$ so that the elements of N' become coloops of the extension. This is referred to as *addition of coloops*. This extension is further principally extended to $\widetilde{\mathsf{M}} = (N \cup N' \cup N'', \tilde{r})$ by adding i'' at $i \cup i'$ for every $i \in N$.

Lemma 6. *The mappings $i \mapsto i''$ and $i \mapsto i'$ are isomorphisms of the matroid M onto the minors $\widetilde{\mathsf{M}} \setminus N / N'$ and $\widetilde{\mathsf{M}} \setminus N / N''$, respectively.*

Proof. The assertions are consequences of

$$\tilde{r}(I \cup J' \cup K'') = r(I \cup (J \cap K)) + |J \cup K|\,, \qquad I, J, K \subseteq N\,. \tag{4}$$

In fact, $\tilde{r}(N' \cup K'') = r(K) + |N|$, $K \subseteq N$, and $\tilde{r}(J' \cup N'') = r(J) + |N|$, $J \subseteq N$.

Eqs. (4) follow from (2) with $M = N''$

$$\tilde{r}(I \cup J' \cup K'') = \min_{D \subseteq K} \left[r(I \cup D) + |J' \cup D'| + |K'' \setminus D''| \right]$$

where the two cardinalities sum to $|(J \cap K) \setminus D| + |J \cup K|$. Then

$$\tilde{r}(I \cup J' \cup K'') = \min_{D \subseteq J \cap K} \left[r(I \cup D) + |(J \cap K) \setminus D| \right] + |J \cup K|\,.$$

The minimization can be further restricted to the sets D containing $I \cap J \cap K$. By submodularity, the minimum is then attained at $D = J \cap K$ whence eqs. (4) hold. □

Having a base B of M let $B' \subseteq N'$ and $B'' \subseteq N''$ be the copies of B, and D' and D'' be another disjoint copies not intersecting $N' \cup N''$. The matroid obtained from $\widetilde{\mathsf{M}} \setminus N$ by extending each element of $B' \cup B''$ by a parallel one in $D' \cup D''$ is denoted by $\widetilde{\widetilde{\mathsf{M}}}$.

Lemma 7. *The matroid $\widetilde{\widetilde{\mathsf{M}}}$ has a minor isomorphic to M and the ground set partitioned into the bases $N' \cup D''$ and $N'' \cup D'$.*

Proof. The first assertion follows from Lemma 6. By (4), $\tilde r(N'\cup B'')$ and $\tilde r(B'\cup N'')$ equal $r(B)+|N|$. It suffices to replace here B' by D' and B'' by D'', and recall that $r(N)+|N|$ is the rank of $\tilde{\tilde M}$. □

By [31, Lemma 2.2], a matroid that is linear over an infinite field is a minor of a linear matroid whose ground set partitions into two bases. This follows from Lemma 7 and the observation that the constructions used to arrive at $\tilde{\tilde M}$ preserve linearity.

Lemma 8. *The direct sum of a matroid with a uniform one can be constructed by adding coloops and by principal extensions.*

Proof. Let a uniform matroid sit on $L\cup M$ where L is a base and M the complement of L. A given matroid with a disjoint ground set J is extended to $(J\cup L, r)$ such that L becomes a set of its coloops. Then, the principal extensions adding each $m\in M$ at L are performed. By (3) with $N=J\cup L$, the resulting matroid $(J\cup L\cup M,\bar r)$ has

$$\bar r(I\cup K)=\min\big\{r(I\cap J)+|L|, r(I\cap J)+|I\cap L|+|K|\big\}\,,\qquad I\subseteq J\cup L\,,\ K\subseteq M\,.$$

It follows that its restriction to $L\cup M$ is the uniform matroid, its restriction to J is the given matroid and $\bar r(J\cup L\cup M)=r(J)+|L|$, giving the direct sum. □

The Zhang-Yeung inequality [42, Theorem 3]

$$\begin{aligned}\big[I(\xi_3;\xi_4|\xi_1)+I(\xi_3;\xi_4|\xi_2)+I(\xi_1;\xi_2)-I(\xi_3;\xi_4)\big]\\ +I(\xi_1;\xi_3|\xi_4)+I(\xi_1;\xi_4|\xi_3)+I(\xi_3;\xi_4|\xi_1)\geqslant 0\end{aligned}\tag{5}$$

holds for four random variables ξ_1,ξ_2,ξ_3,ξ_4 taking finite number of values. Every term of (5) is a conditional mutual information [40]. For example, $I(\xi_3;\xi_4|\xi_1)$ rewrites via Shannon entropies to $H(\xi_1,\xi_3)+H(\xi_1,\xi_4)-H(\xi_1,\xi_3,\xi_4)-H(\xi_1)$.

Having a polymatroid (N,h) and $I,J,K,L\subseteq N$, the mutual information $I(\xi_3;\xi_4|\xi_1)$ corresponds to $h(I\cup K)+h(I\cup L)-h(I\cup K\cup L)-h(I)$ and the bracket in (5) to

$$\begin{aligned}&\big[h(I\cup K)+h(I\cup L)+h(J\cup K)+h(J\cup L)+h(K\cup L)\big]\\ &\qquad-\big[h(I\cup J)+h(K)+h(L)+h(I\cup K\cup L)+h(J\cup K\cup L)\big]\,.\end{aligned}$$

Ingleton inequality [13, 14] claims nonnegativity of the above difference for the linear (poly)matroids. The Zhang-Yeung inequality is used later in the form

$$\begin{aligned}&3\big[h(I\cup K)+h(I\cup L)+h(K\cup L)\big]+h(J\cup K)+h(J\cup L)\\ &\qquad\geqslant\ h(I)+2\big[h(K)+h(L)\big]+h(I\cup J)+4h(I\cup K\cup L)+h(J\cup K\cup L)\,.\end{aligned}\tag{6}$$

This is valid for the almost entropic polymatroids by limiting, but fails for Vámos matroid. The Zhang-Yeung inequality is weaker than Ingleton one, by submodularity.

4. Encompassing matroid

Let $\mathsf{M} = (N, r)$ be a matroid of the rank $r(N) = s \geqslant 1$. In this section it is assumed that N is a disjoint union of two bases A and B. Let $\{\mathsf{1}, \mathsf{2}, \mathsf{3}, \mathsf{4}\}$ support the uniform matroid $\mathsf{U}_{3,4}$, $N' = A' \cup B'$ be a copy of N, I be a set with $s+1$ elements and J with two elements. All the sets in the union

$$N_{\text{enc}} = A \cup B \cup \{\mathsf{1}, \mathsf{2}, \mathsf{3}, \mathsf{4}\} \cup A' \cup B' \cup I \cup J$$

are assumed to be pairwise disjoint. Let $K = \mathsf{3} \cup A'$ and $L = \mathsf{4} \cup B'$.

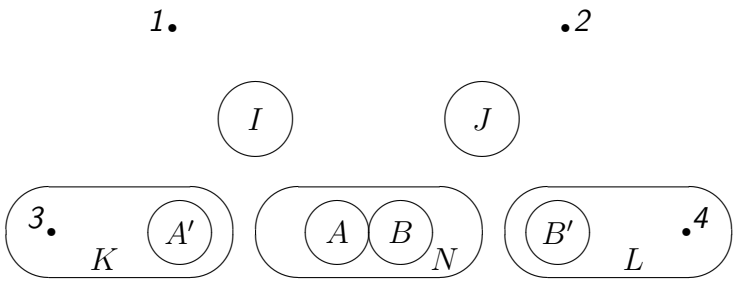

Figure 2. The encompassing matroid $\mathsf{M}_{\text{enc}} = (N_{\text{enc}}, \rho)$.

The *encompassing* matroid M_{enc} is constructed on the ground set N_{enc} from the direct sum $\mathsf{M} \oplus \mathsf{U}_{3,4}$ by principal extensions in the following four steps:

1. if $a \in A$ then $a' \in A'$ is added by the extension at $\mathsf{3} \cup a$,
2. if $b \in B$ then $b' \in B'$ is added by the extension at $\mathsf{4} \cup b$,
3. each element of I is added by extending at $\mathsf{1} \cup N$,
4. each element of J is added by extending at $\mathsf{2} \cup N$.

The rank function of M_{enc} is denoted by ρ. The rank is $s+3$.

The following three lemmas rely on eqs. (2) and their variants.

Lemma 9. *The matroid M is isomorphic to $\mathsf{M}_{\text{enc}} \setminus (N \cup \{\mathsf{1}, \mathsf{2}\} \cup I \cup J)/\{3, 4\}$.*

Proof. The minor sits on N' and the isomorphism is $i \mapsto i'$. The latter is a consequence of

$$\rho(C' \cup \{\mathsf{3}, \mathsf{4}\}) = \rho(C \cup C' \cup \{\mathsf{3}, \mathsf{4}\}) = \rho(C \cup \{\mathsf{3}, \mathsf{4}\}) = r(C) + 2\,, \qquad C \subseteq N\,, \tag{7}$$

using that the restrictions of M_{enc} to $\mathsf{3} \cup a \cup a'$, $a \in A$, and to $\mathsf{4} \cup b \cup b'$, $b \in B$, are isomorphic to $\mathsf{U}_{2,3}$, see Steps 1, 2 and (1). □

Eqs. (2) for the matroid $\mathsf{M}_{\text{enc}} \setminus (I \cup J)$ extended to M_{enc} in Steps 3 and 4 imply

$$\begin{aligned} \rho(M_1 \cup M_2) = \min\big\{\, &\rho(M_1 \cup N \cup \{\mathsf{1}, \mathsf{2}\})\,,\ \rho(M_1 \cup N) + 1 + |M_2 \cap I|\,,\\ &\rho(M_1 \cup N) + 1 + |M_2 \cap J|\,,\ \rho(M_1) + |M_2|\,\big\}\,,\\ &M_1 \subseteq K \cup L \cup N \text{ and } M_2 \subseteq I \cup J. \end{aligned} \tag{8}$$

In fact, the sets I and K in (2) correspond to M_1 and M_2 in (8), respectively. The minimization over D in (2) reduces in (8) to the cases M_2, $M_2 \cap J$, $M_2 \cap I$ and $\emptyset$, providing the four terms in the minimum.

Lemma 10. *In $\mathsf{M}_{\mathrm{enc}}$, $I \cup J$ is a circuit of rank $s+2$ and $N \cup \{\mathsf{1},\mathsf{2}\} \cup I \cup J$ a hyperplane.*

Proof. The first part follows from (8) with $M_1 = \emptyset$, giving

$$\rho(M_2) = \min\left\{ s+2\,,\, s+1+|M_2 \cap I|\,,\, s+1+|M_2 \cap J|\,,\, |M_2| \right\}, \quad M_2 \subseteq I \cup J\,. \tag{9}$$

Thus, $\rho(M_2) = \min\{s+2\,,\,|M_2|\}$ using the assumption $s \geqslant 1$.

By Steps 3 and 4, $\rho(N \cup \{\mathsf{1},\mathsf{2}\} \cup I \cup J) = s+2$. Further, $\rho(N \cup \{\mathsf{1},\mathsf{2},\mathsf{3}\})$ and $\rho(N \cup \{\mathsf{1},\mathsf{2},\mathsf{4}\})$ equal $s+3$. By Steps 1 or 2, $\rho(N \cup \{\mathsf{1},\mathsf{2},i'\}) = s+3$, $i \in N$. □

Lemma 11. *In $\mathsf{M}_{\mathrm{enc}}$, the instance of Zhang-Yeung inequality with I, J, K and L is tight.*

Proof. The tightness in (6) is summarized, correspondingly to the involved ranks, as

$$11(s+2) = (s+1) + 2[(s+1)+(s+1)] + (s+2) + 4(s+3) + (s+3)\,.$$

In fact, $\rho(K \cup L) = s+2$ by (7) and the remaining terms on the left-hand side of (6) equal $s+2$ by (8). On the right-hand side of (6), $\rho(I) = s+1$ by (3), $\rho(K) = \rho(L) = s+1$ since $\mathsf{3} \cup a \cup a'$, $a \in A$, and $\mathsf{4} \cup b \cup b'$, $b \in B$, are isomorphic to $\mathsf{U}_{2,3}$, $\rho(I \cup J) = s+2$ by Lemma 10, and $\rho(I \cup K \cup L) = \rho(J \cup K \cup L) = s+3$ by (8). □

The above argumentation implies also that the corresponding instance of Ingleton inequality is tight as well.

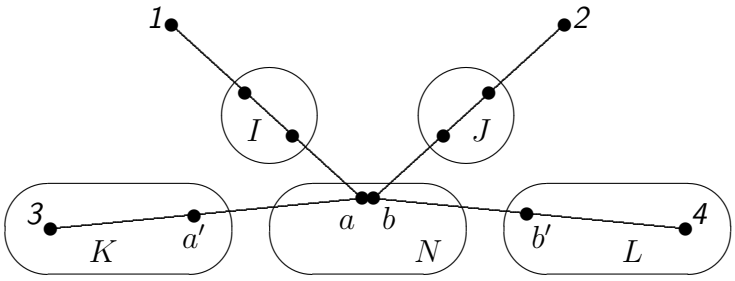

FIGURE 3. The encompassing matroid for $\mathsf{M} = \mathsf{U}_{1,2}$.

Example 1. Let $\mathsf{M} = \mathsf{U}_{1,2}$ have the ground set partitioned into singletons a and b. Then $\mathsf{M}_{\mathrm{enc}}$ has twelve points in N_{enc} and the rank four. It is linear. A geometric representation is depicted in Figure 3 where the four segments meet in one point.

5. The construction of M° and proof of Theorem 1

In the previous section, the encompassing matroid $M_{\rm enc} = (N_{\rm enc}, \rho)$ is constructed from any matroid M of the rank $s \geqslant 1$ whose ground set is a disjoint union of two bases. Let $M_{\rm res}$ denote the restriction of $M_{\rm enc}$ to $I \cup J \cup K \cup L$. By Lemma 10, $I \cup J$ is a circuit-hyperplane of $M_{\rm res}$. Let $M^\circ = (I \cup J \cup K \cup L, \rho^\circ)$ be the matroid obtained from $M_{\rm res}$ by the relaxation at $I \cup J$ [33, p. 39]. The only difference between the two matroids is that $\rho^\circ(I \cup J) = s + 3$ while $\rho(I \cup J) = s + 2$. If the construction starts with $M = U_{1,2}$ then M° is Vámos matroid, see Example 1 and Figure 3.

Proof of Theorem 1. Let $M = (N, r)$ be a matroid in $\mathcal{M}$ of the rank $s \geqslant 0$. By Lemma 7, M is a minor of $\tilde{\tilde{M}}$ whose ground set is partitioned into two bases. The latter matroid is constructed from the former by adding coloops, principal extensions, deletion and parallel extensions. Hence, $\tilde{\tilde{M}} \in \mathcal{M}$. It can happen that the rank of $\tilde{\tilde{M}}$ is zero but only if $N = \emptyset$. In this case, M is a minor of $U_{1,2}$ which belongs to $\mathcal{M}$ by Lemma 8. If the assertion of Theorem 1 holds for $\tilde{\tilde{M}}$, or for $U_{1,2}$ in the special case, then it does for M.

It follows that there is no loss of generality in assuming that M itself has the ground set N partitioned into two bases A and B and $s \geqslant 1$. By Lemma 8, $M \oplus U_{3,4} \in \mathcal{M}$. The encompassing matroid $M_{\rm enc}$ is constructed from M and its two distinguished bases by principal extensions. Therefore, $M_{\rm enc}$ and the restriction $M_{\rm res}$ belong to the class $\mathcal{M}$.

It remains to verify *(i)*, *(ii)* and *(iii)* for the relaxation M° constructed above.

(i) By Lemma 9, the minor $M_{\rm res} \setminus (I \cup J)/\{3, 4\}$ is isomorphic to M. The deletions of $I \cup J$ from M° and $M_{\rm res}$ coincide. Hence, M is isomorphic to a proper minor of M°.

(ii) The goal here is to prove that the contraction by and deletion of any element from M° belong to the class $\mathcal{M}$. Four cases are distinguished.

Case 1. "If $i \in I \cup J$ then $M^\circ \setminus i \in \mathcal{M}$." This follows from $M^\circ \setminus i = M_{\rm res} \setminus i \in \mathcal{M}$.

Case 2. "If $i \in I \cup J$ then $M^\circ / i \in \mathcal{M}$." For a demonstration, only $i \in I$ is considered since otherwise symmetry applies. On $N_{\rm enc} \setminus i$ a modified encompassing matroid $\hat{M}_{\rm enc}$ is constructed from $M \oplus U_{3,4}$ by the same extensions as in Steps 1 and 2, and

$\hat{3}$. each element of $I \setminus i$ is added by extending at N,
$\hat{4}$. each element of J is added by extending at $N \cup \{3, 4\}$.

Let $\hat{\rho}$ denote the rank function of $\hat{M}_{\rm enc}$ and $\hat{M}_{\rm res}$ its restriction to $(I \setminus i) \cup J \cup K \cup L$. It suffices to prove that M° / i coincides with $\hat{M}_{\rm res}$, belonging to the class $\mathcal{M}$ by construction. This is equivalent to

$$\rho^\circ(M_1 \cup M_2 \cup i) - \rho^\circ(i) = \hat{\rho}(M_1 \cup M_2)\,, \qquad M_1 \subseteq K \cup L \text{ and } M_2 \subseteq (I \setminus i) \cup J. \tag{10}$$

Eqs. (2) for $\hat{M}_{\rm enc} \setminus (K \cup L \cup N)$ extended to $\hat{M}_{\rm enc}$ in Steps $\hat{3}$ and $\hat{4}$ imply

$$\hat{\rho}(M_1 \cup M_2) = \min\left\{ \rho(M_1 \cup N \cup \{3, 4\})\,,\, \rho(M_1 \cup N) + |M_2 \cap J|\,,\, \rho(M_1) + |M_2| \right\}.$$

In minimization, only M_2, $M_2 \cap I$ and $\emptyset$ were relevant, giving the three terms on the right, respectively. In particular,

$$\hat{\rho}(M_2) = \min\big\{\, s+2\,,\, s+|M_2 \cap J|\,,\, |M_2|\,\big\} = |M_2|\,, \qquad M_2 \subseteq (I \setminus i) \cup J.$$

By the relaxation, $I \cup J$ is a base of M°. It follows that (10) holds if $M_1 = \emptyset$.

If $M_1 \neq \emptyset$ the left-hand side of (10) is $\rho(M_1 \cup M_2 \cup i) - 1$ where

$$\begin{aligned}\rho(M_1 \cup M_2 \cup i) &= \min\big\{\, \rho(M_1 \cup N \cup \{\mathit{1},\mathit{2}\})\,,\, \rho(M_1 \cup N) + 1 + |M_2 \cap I| + 1\,,\\ &\qquad\qquad \rho(M_1 \cup N) + 1 + |M_2 \cap J|\,,\, \rho(M_1) + |M_2| + 1\,\big\}\\ &= \min\big\{\, s+3\,,\, \rho(M_1 \cup N) + |M_2 \cap J| + 1\,,\, \rho(M_1) + |M_2| + 1\,\big\}\\ &= \hat{\rho}(M_1 \cup M_2) + 1\,,\end{aligned}$$

using (8). Hence, (10) holds.

Case 3. "If $k \in K \cup L$ then $\mathsf{M}^\circ / k \in \mathcal{M}$". This follows from $\mathsf{M}^\circ / k = \mathsf{M}_{\rm res} / k \in \mathcal{M}$.

Case 4. "If $k \in K \cup L$ then $\mathsf{M}^\circ \setminus k \in \mathcal{M}$". The proof is presented for $k \in K$ because arguments are symmetric for $k \in L$. Another modification $\check{\mathsf{M}}_{\rm enc}$ of the encompassing matroid constructed as follows. First, $\mathsf{M} \oplus \mathsf{U}_{3,4}$ is extended as in Steps 1 and 2. Second, disjoint sets U and V of the cardinality s are chosen to be disjoint from the ground set of $\mathsf{M}_{\rm enc}$, and

- $\check{3}$. each element of U is added by extending at $(K \setminus k) \cup N$,
- $\check{4}$. each element of V is added by extending at $L \cup N$.

Finally,

- $\check{5}$. each element of I is added by extending at $\mathit{1} \cup U$,
- $\check{6}$. each element of J is added by extending at $\mathit{2} \cup V$.

The ground set of $\check{\mathsf{M}}_{\rm enc}$ is $I \cup J \cup K \cup L \cup N \cup \{\mathit{1},\mathit{2}\} \cup U \cup V$ and the rank function is denoted by $\check{\rho}$. By construction, $\mathcal{M}$ contains the restriction of $\check{\mathsf{M}}_{\rm enc}$ to $I \cup J \cup (K \setminus k) \cup L$, denoted by $\check{\mathsf{M}}_{\rm res}$. It suffices to prove that $\mathsf{M}^\circ \setminus k = \check{\mathsf{M}}_{\rm res}$, thus

$$(11) \qquad \rho^\circ(M_1 \cup M_2) = \check{\rho}(M_1 \cup M_2)\,, \qquad M_1 \subseteq (K \setminus k) \cup L \ \text{ and } \ M_2 \subseteq I \cup J.$$

Eqs. (2) are applied to the extensions in Steps $\check{3}$ and $\check{4}$, giving for $M_3 \subseteq (K \setminus k) \cup L \cup \{\mathit{1},\mathit{2}\}$ and $M_4 \subseteq U \cup V$

$$\begin{aligned}\check{\rho}(M_3 \cup M_4) = \min\big\{\, &\rho(M_3 \cup (K \setminus k) \cup L \cup N)\,,\\ &\rho(M_3 \cup (K \setminus k) \cup N) + |M_4 \cap V|\,,\, \rho(M_3 \cup L \cup N) + |M_4 \cap U|\,,\, \rho(M_3) + |M_4|\,\big\}\end{aligned}$$

In particular,

$$\begin{aligned}&\check{\rho}(M_1 \cup \{\mathit{1},\mathit{2}\} \cup U \cup V) = \min\big\{\, s+3, s+3+|V|, s+3+|U|, \rho(M_1 \cup \{\mathit{1},\mathit{2}\}) + 2s\,\big\}\,,\\ &\check{\rho}(M_1 \cup \mathit{1} \cup U) = \min\big\{\, s+3\,,\, \rho(M_1 \cup (K \setminus k) \cup N) + 1\,,\, \rho(M_1) + 1 + |U|\,\big\}\,,\\ &\check{\rho}(M_1 \cup \mathit{2} \cup V) = \min\big\{\, s+3\,,\, \rho(M_1 \cup L \cup N) + 1\,,\, \rho(M_1) + 1 + |V|\,\big\}\,.\end{aligned}$$

Thus, $\check{\rho}(M_1 \cup \{\mathit{1},\mathit{2}\} \cup U \cup V) = s+3$ and in the last two lines $s+3$ in the minimization can be omitted. By (2) applied to the extensions in Steps $\check{5}$ and $\check{6}$,

$$\begin{aligned}\check{\rho}(M_3 \cup M_4 \cup M_2) = \min\big\{\, &\check{\rho}(M_3 \cup M_4 \cup \{\mathit{1},\mathit{2}\} \cup U \cup V)\,,\\ &\check{\rho}(M_3 \cup M_4 \cup \mathit{1} \cup U) + |M_2 \cap J|)\,,\\ &\check{\rho}(M_3 \cup M_4 \cup \mathit{2} \cup V) + |M_2 \cap I|\,,\ \check{\rho}(M_3 \cup M_4) + |M_2|\,\big\}.\end{aligned} \tag{12}$$

When $M_2 = I \cup J$ and $M_3 = M_4 = \emptyset$ it follows that

$$\check{\rho}(I \cup J) = \min\big\{\, \check{\rho}(\{\mathit{1},\mathit{2}\} \cup U \cup V)\,,\ \check{\rho}(\mathit{1} \cup U) + 2\,,\ \check{\rho}(\mathit{2} \cup V) + s + 1\,,\ s+3\,\big\} = s+3\,.$$

Hence, $I \cup J$ is a base of $\check{\mathsf{M}}_{\mathrm{res}}$. It is also a base of M° by relaxation. Thus, eqs. (11) hold for $M_1 = \emptyset$.

Eq. (12), takes for $M_1 \neq \emptyset$ in the role of M_3 and $M_4 = \emptyset$ the form

$$\begin{aligned}\check{\rho}(M_1 \cup M_2) = \min\big\{\, &s+3\,,\ \check{\rho}(M_1 \cup \mathit{1} \cup U) + |M_2 \cap J|)\,,\\ &\check{\rho}(M_1 \cup \mathit{2} \cup V) + |M_2 \cap I|\,,\ \rho(M_1) + |M_2|\,\big\}\end{aligned}$$

while (8) reduces to

$$\begin{aligned}\rho(M_1 \cup M_2) = \min\big\{\, &s+3\,,\ \rho(M_1 \cup N) + 1 + |M_2 \cap J|)\,,\\ &\rho(M_1 \cup N) + 1 + |M_2 \cap I|\,,\ \rho(M_1) + |M_2|\,\big\}\,.\end{aligned}$$

Hence, when M_1 intersects both $K \setminus k$ and L then

$$\check{\rho}(M_1 \cup M_2) = \rho(M_1 \cup M_2) = \min\big\{\, s+3\,,\ \rho(M_1) + |M_2|\,\big\}$$

and when M_1 intersects only one of $K \setminus k$ and L then

$$\check{\rho}(M_1 \cup M_2) = \rho(M_1 \cup M_2) = \min\big\{\, s+3\,,\ s+2+|M_2 \cap J|\,,\ s+2+|M_2 \cap I|\,,\ \rho(M_1)+|M_2|\,\big\}\,.$$

It follows that eqs. (11) hold.

(iii) By Lemma 11, Zhang-Yeung inequality is tight in $\mathsf{M}_{\mathrm{res}}$ for the sets I, J, K, L. This instance of the inequality fails in M° because its right-hand side is greater by one due to the relaxation. □

The presented proof of Theorem 1 is partially inspired by that of [31, Theorem 1.1]. Both are constructive and mimic the construction of Vámos matroid to violate Ingleton or Zhang-Yeung inequalities. Several subtle arguments based previously on reasoning in projective geometries had to be avoided and replaced here. This necessitated to maintain the encompassing matroid during the whole proof and to introduce its variants. The approach via rank functions was preferred because it bypasses intuitive arguments on freeness in projective spaces and leads to mere computations with minima. The most difficult Case 4 needed new arguments since modularity was not available, as in projective geometries.

6. Proof of Theorem 2

This section contains the proof of Theorem 2. First, three lemmas are worked out.

It is assumed throughout that $\mathsf{M} = (N, r)$ is a matroid and $\bar{\mathsf{M}} = (N \cup 0, \bar{r})$ its principal extension by 0 at $L \subseteq N$.

Lemma 12. *If M is multilinear of the degree $\delta \geqslant 1$ over a finite field $\mathbb{F}$ then $\bar{\mathsf{M}}$ is multilinear of the same degree δ over a finite field extending $\mathbb{F}$.*

Proof. Let M be multilinear of the degree δ over $\mathbb{F}$ and be represented by subspaces E_i, $i \in N$, of a linear space over $\mathbb{F}$. Thus, $\delta \cdot r(I) = \dim E_I$, $I \subseteq N$, where E_I abbreviates the sum $\bigoplus_{i \in I} E_i$. Then, the above holds in a linear space over any field extension $\mathbb{E}$ of $\mathbb{F}$.

An extension $\mathbb{E}$ is chosen to have the cardinality q that is greater than the number ℓ of hyperplanes of M. Let $\mathcal{H}_L$ denote the family of the hyperplanes that do not contain $\mathsf{cl}(L)$. Thus, $H \in \mathcal{H}_L$ if and only if $r(H \cup L) = r(N)$. Then, $\delta + \dim E_H \cap E_L \leqslant \dim E_L$. The union of $E_H \cap E_L$ over $H \in \mathcal{H}_L$ contains at most $\ell \cdot q^{\delta \cdot r(L) - \delta}$ vectors. This is less than $q^{\delta \cdot r(L)}$, the number of vectors in E_L. Therefore, there exists $v_1 \in E_L$ outside of each hyperplane from $\mathcal{H}_L$. If $\delta = 1$ then let E_0 be the span of v_1. Otherwise, the argument is repeated with $(E_H \cap E_L) \oplus v_1$ in the role of $E_H \cap E_L$. By finite induction, there exist independent vectors $v_1, \ldots, v_\delta$ in E_L whose span intersects each $E_H \cap E_L$, $H \in \mathcal{H}_L$, in the zero vector. Let E_0 be the span of these vectors. By construction, $\dim E_0 = \delta$, and E_H and E_0 sum directly to E_N once $H \in \mathcal{H}_L$.

The remaining part of the proof shows that E_i, $i \in N$, and E_0 represent $\bar{\mathsf{M}}$ multilinearly with the degree δ over $\mathbb{E}$. To this end, it suffices to prove

$$\delta \cdot \bar{r}(I \cup 0) = \dim E_I \oplus E_0 \,, \qquad I \subseteq N \,. \tag{13}$$

If $r(I \cup L) = r(I)$ then $E_0 \subseteq E_L \subseteq E_{I \cup L} = E_I$. Since $\bar{r}(I \cup 0) = r(I)$ eq. (13) rewrites to $\delta \cdot r(I) = \dim E_I$ which holds because E_i, $i \in N$, represent M. If $r(I \cup L) > r(I)$ then a hyperplane H from $\mathcal{H}_L$ contains I. Then, eq. (13) holds because $\bar{r}(I \cup 0) = r(I) + 1$, and $E_H \oplus E_0 = E_N$ implies $\dim E_I \oplus E_0 = \delta \cdot r(I) + \delta$. □

For the field extension theory the reader is referred to [17]. Let a matroid M with the ground set $\{1, \ldots, n\}$ have an algebraic representation over a field $\mathbb{F}$ by elements $e_1, \ldots, e_n$ of an extension field $\mathbb{E}$. The tower of fields $\mathbb{F}_0 \subseteq \ldots \subseteq \mathbb{F}_n$ is constructed from $\mathbb{F}_0 = \mathbb{F}$ inductively by $\mathbb{F}_i = \mathbb{F}_{i-1}(i)$, $1 \leqslant i \leqslant n$, where $\mathbb{F}_{i-1}(i)$ is the smallest subfield of $\mathbb{E}$ that contains $\mathbb{F}_{i-1}$ and e_i. If e_i is transcendental over $\mathbb{F}_{i-1}$ then $\mathbb{F}_i$ is isomorphic to the quotient field $\mathbb{F}_{i-1}(x)$ of an indeterminate x. Otherwise, e_i is algebraic and $\mathbb{F}_i$ is isomorphic to the quotient ring $\mathbb{F}_{i-1}[x]/p_i$ where p_i is an irreducible polynomial in x with coefficients in $\mathbb{F}_{i-1}$. There is no loss of generality in assuming that $\mathbb{E} = \mathbb{F}_n$. As well known, for $I \subseteq N$ the transcendence dimension $\dim_{\mathrm{tr}} \mathbb{F}(I)$ of $\mathbb{F}(I)$ over $\mathbb{F}$ equals the number of transcendental extensions $\mathbb{F}_{i-1}(i)$, $i \in I$, in the tower construction. The dimension does not depend on the construction of the tower when $e_1, \ldots, e_n$ are permuted.

Lemma 13. *The principal extensions of the algebraic matroids over a field are algebraic over the same field.*

Proof. Let M be represented by $e_1, \dots, e_n$ as above. It suffices to consider the principal extension $\bar{\mathsf{M}}$ at $L \subseteq N$ such that $\{1, \dots, m\}$ is a maximal independent subset of L for some $0 \leqslant m \leqslant n$. Thus, $e_1, \dots, e_m$ are algebraically independent transcendentals over $\mathbb{F}$. If $e_{n+i} = e_1\, e_2^i \cdots e_m^{i^m}$, $i \geqslant 1$, then $e_1, \dots, e_m, e_{n+1}, \dots, e_{n+i}$ represent algebraically a uniform matroid $\mathsf{U}_{m,m+i}$ over $\mathbb{F}$ [33, Example 6.7.8].

Let $I \subseteq N$. If $r(I \cup L) > r(I)$ then $\mathsf{cl}(I)$ does not contain L whence it does not cover $\{1, \dots, m\}$. Hence, $\mathbb{F}(I)$ does not contain some of $e_1, \dots, e_m$. In turn, it contains less than m elements of the sequence e_{n+i}, $i \geqslant 1$. It follows that for i sufficiently large none of the sets I satisfying $r(I \cup L) > r(I)$ contains e_{n+i}. Let $e_0 = e_{n+i}$ for that i. Extending $\mathbb{F}(I)$ by e_0 the transcendence dimension jumps up by one. This is not the case when $r(I \cup L) = r(I)$ by the construction of the sequence. Comparing with (1), it follows that the principal extension $\bar{\mathsf{M}}$ is represented by $e_0, \dots, e_n$. □

Let $\pi\colon N \to \pi(N)$ be a bijection fixing the points of $N \cap \pi(N)$. A matroid $\mathsf{M} = (N, r)$ is *selfadhesive* at $N \cap \pi(N)$ if it extends to a matroid $(N \cup \pi(N), r_\pi)$ such that π becomes a matroid monomorphism and $r(N) + r_\pi(\pi(N)) = r_\pi(N \cup \pi(N)) + r(N \cap \pi(N))$. The equality expresses the adhesivity. A matroid is selfadhesive if it is selfadhesive at each of its subsets.

Lemma 14. *The algebraic matroids are selfadhesive.*

Proof. Let M be algebraically represented by $e_1, \dots, e_n$ as above. It is assumed that for some $0 \leqslant m \leqslant n$ the bijection $\pi\colon N \to \pi(N)$ is given by $\pi(i) = i$, $1 \leqslant i \leqslant m$, and $\pi(i) = i + n - m$, $m < i \leqslant n$. The field $\mathbb{E} = \mathbb{F}_n$, closing the tower construction, is further extended by prolonging the tower $\mathbb{F}_0 \subseteq \ldots \subseteq \mathbb{F}_n$ to $\mathbb{F}_{n+1} \subseteq \ldots \subseteq \mathbb{F}_{2n-m}$. Here, if $n < i \leqslant 2n - m$ then $\mathbb{F}_i = \mathbb{F}_{i-1}(x)$ whenever e_{i-n+m} is transcendental over $\mathbb{F}_{i-n+m-1}$ and $\mathbb{F}_i = \mathbb{F}_{i-1}[x]/p_i$ otherwise. In each extension x is successively renamed to e_i.

The elements e_i, $1 \leqslant i \in 2n - m$, represent a matroid on $N \cup \pi(N)$ that extends M. The restriction of the matroid to $\pi(N)$ is the isomorphic copy of M by π. The adhesivity condition follows by the construction of the prolonged tower. □

Corollary 2. *The rank functions of the algebraic matroids enjoy Zhang-Yeung inequality.*

Proof. It suffices to combine Lemma 14 with the fact that the selfadhesive polymatroids satisfy Zhang-Yeung inequality, see [29, Corollary 1][§]. □

Proof of Theorem 2. To apply Theorem 1, the assumptions that each of the classes is closed under minors, addition of coloops and principal extensions are verified. The addition of coloops is by elementary constructions and is not commented below.

[§]The reverse implication holds when $|N| = 4$ [29, Theorem 3].

It follows from elements of the basic theory of the linear matroids that every class $\mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},d}$ is closed under minors. The matroids from $\mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},d}$ have the principal extensions representable if $\mathbb{F}$ is infinite, see [24, p. 246]. Representability of the extensions in the case $\mathcal{M}^{\mathrm{mlin}}_{\delta}$ is covered by Lemma 12. It is inherited to $\mathcal{M}^{\mathrm{mlin}}$. This implies the assumptions in the first three cases.

The class $\mathcal{M}^{\mathrm{alg}}_{\mathbb{F}}$ is closed under minors by [33, Cor. 6.7.14]. Lemma 13 asserts that it is closed under principal extensions. The two properties inherit to $\mathcal{M}^{\mathrm{alg}}$.

The class $\mathcal{M}^{\mathrm{aent}}$ is closed under minors by [30, Lemma 1]. It is closed under parallel extensions and convolutions [28, Theorem 2] whence also to the principal extensions.

To apply Theorem 1 to one of the classes, it remains to verify that Zhang-Yeung inequality is valid. In $\mathcal{M}^{\mathrm{alg}}$ the inequality holds by Corollary 2. In $\mathcal{M}^{\mathrm{aent}}$ it holds by limiting in [42, Theorems 3 and 5]. Then, it suffices to invoke Figure 1 and the inclusions explained in Remarks 1 and 2. □

It is left open whether $\mathcal{M}^{\mathrm{mlin}}_{\mathbb{F}} \triangleq \bigcup_{\delta\geqslant 1} \mathcal{M}^{\mathrm{mlin}}_{\mathbb{F},\delta}$ and $\mathcal{M}^{\mathrm{pare}}$ are closed under principal extensions. A positive answer would enable to include these two classes to Theorem 2.

Acknowledgement

This is to appreciate hospitality of the Banff International Research Station during the workshop "Applications of Matroid Theory and Combinatorial Optimization to Information and Coding Theory", August 2–7, 2009, that ignited this work.

References

[1] M. Aigner (1979) *Combinatorial Theory.* Springer-Verlag, Berlin.
[2] A. Beimel (2011) Secret-sharing schemes: a survey. *Coding and Cryptology, Lecture Notes in Comp. Science* **6639** Springer-Verlag, Berlin, 11–46.
[3] A. Beimel, A.M. Ben-Efraim, C. Padró and I. Tomkin (2014) Multi-linear secret sharing schemes. *Theory of Cryptography, Lecture Notes in Comp. Science* **8349** Springer-Verlag, Berlin, 394–418.
[4] A. Beimel and B. Chor (1994) Universally ideal secret-sharing schemes. *IEEE Trans. Inf. Theory* **40** 786–794.
[5] A. Ben-Efraim (2016) Secret-sharing matroids need not be algebraic. *Disc. Math.* **339** 2136-2145.
[6] E.F. Brickell and D.M. Davenport (1991) On the classification of ideal secret sharing schemes. *J. Cryptology* **4** 123–134.
[7] T. Brylawski and D. Kelly (1980) *Matroids and Combinatorial Geometries.* Carolina Lecture Series, Department of Mathematics, Univ. of North Carolina at Chapel Hill.
[8] R. Dougherty, Ch. Freiling and K. Zeger (2007) Networks, matroids, and non-Shannon information inequalities. *IEEE Trans. Inf. Theory* **53** 1949–1969.
[9] S. Fujishige (1978) Polymatroidal dependence structure of a set of random variables. *Information and Control* **39** 55–72.
[10] J. Geelen (2008) Some open problems on excluding a uniform matroid. *Adv. Appl. Math.* **41** 628–637.
[11] G. Gordon (1988) Algebraic characteristic sets of matroids. *J. Comb. Th. B* **44** 64–74.
[12] J. Geelen, B. Gerards and G. Whittle (2014) Solving Rotas conjecture. *Notices AMS* **61** 736-743.
[13] A.W. Ingleton (1971) Conditions for representability and transversality of matroids. *Proc. Fr. Br. Conf. 1970*, Springer Lecture Notes **211**, Springer-Verlag, Berlin, 62–67.

[14] A.W. Ingleton (1971) Representation of matroids. *Combinatorial Mathematics and its Applications* (D.J.A. Welsh, ed.), Academic Press, London, 149–167.

[15] A.W. Ingleton and R.A. Main (1975) Non-algebraic matroids exist. *Bull. London Math. Soc.* **7** 144–146.

[16] E. Katz (2014) Matroid theory for algebraic geometers. (arXiv:1409.3503)

[17] S. Lang (2002) *Algebra.* Oxford University Press, Oxford.

[18] T. Lazarson (1968) The representation problem for independence functions. *J. London Math. Soc.* **33** 21-25.

[19] B. Lindström (1983) The non-Pappus matroid is algebraic. *Ars Combin.* **16** 95-96.

[20] B. Lindström (1987) A class of non-algebraic matroids of rank three. *Geometriae Dedic.* **32** 255–258.

[21] B. Lindström (1988) A generalization of the Ingleton-Main lemma and a class of non-algebraic matroids. *Combinatorica* **8** 87–90.

[22] B. Lindström (1988) Matroids, algebraic and non-algebraic. In: *Algebraic, Extremal and Metric Combinatorics.* (M-M. Deza, P. Frankl and I.G. Rosenberg, eds.) Cambridge University Press, Cambridge, New York.

[23] B. Lindström (1993) On algebraic matroids. *Discrete Math.* **111** 357–359.

[24] L. Lovász (1982) Submodular functions and convexity. In: *Mathematical Programming – The State of the Art* (A. Bachem, M. Grötchel and B. Korte, eds.) Springer-Verlag, Berlin, 234–257.

[25] J. Martí-Farré and C. Padró (2010) On secret sharing schemes, matroids and polymatroids *J. of Mathematical Cryptology* **4** 95–120.

[26] F. Matúš (1994) Probabilistic conditional independence structures and matroid theory: background. *Int. J. of General Systems* **22** 185–196.

[27] F. Matúš (1999) Matroid representations by partitions. *Discrete Math.* **203** 169–194.

[28] F. Matúš (2007) Two constructions on limits of entropy functions. *IEEE Trans. Inf. Th.* **53** 320–330.

[29] F. Matúš (2007) Adhesivity of polymatroids. *Discrete Math.* **307** 2464–2477.

[30] F. Matúš and L. Csirmaz (2016) Entropy region and convolution. *IEEE Trans. Inform. Theory* **62** 6007–6018.

[31] D. Mayhew, M. Newman and G. Whittle (2009) On excluded minors for real-representativity. *J. Comb. Th. B* **99** 685–689.

[32] H. Narayan (1997) *Submodular Functions and Electrical Networks.* Elsevier, Amsterdam.

[33] J.G. Oxley (2011) *Matroid Theory.* (Second Edition) Oxford Graduate Texts in Mathematics **21** Oxford University Press, Oxford.

[34] R.A. Pendavingh and S.H.M. van Zwam (2013) Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. *Advances in Applied Mathematics* **50** 201–227.

[35] G.-C. Rota (1971) Combinatorial theory, old and new. In: *Proc. Internat. Cong. Math.* Gauthier-Villars, Paris, 229–233.

[36] P.D. Seymour (1992) On secret-sharing matroids. *J. Comb. Theory B* **56** 69–73.

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

[38] D. Vertigan (2015) Dowling geometries representable over rings. *Annals of Comb.* **19** 225-233.

[39] D.J.A. Welsh (1976) *Matroid Theory.* Academic Press, London.

[40] R.W. Yeung (2002) *A First Course in Information Theory.* Kluwer Publishers, New York.

[41] Z. Zhang and R.W. Yeung (1997) A non-Shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory* **43** 1982–1986.

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