Matroid Bounds on the Region of Entropic Vectors

Congduan Li, John MacLaren Walsh, Steven Weber
Drexel University, Dept. of ECE, Philadelphia, PA 19104, USA
congduan.li@drexel.edu, jwalsh@coe.drexel.edu, sweber@coe.drexel.edu

***Abstract*—Several properties of the inner bound on the region of entropic vectors obtained from representable matroids are derived. In particular, it is shown that: I) It suffices to check size 2 minors of an integer-valued vector to determine if it is a valid matroid rank; II) the subset of the extreme rays of the Shannon outer bound (the extremal polymatroids) that are matroidal are also the extreme rays of the cone of matroids; III) All matroid ranks are convex independent; and IV) the extreme rays of the conic hull of the binary/ternary/quaternary representable matroid ranks inner bound are a subset of the extreme rays of the conic hull of matroid ranks. These properties are shown to allow for substantial reduction in the complexity of calculating important rate regions in multiterminal information theory, including multiple source multicast network coding capacity regions.**

Keywords*—*entropic vectors; matroids; polymatroids; network coding.

I. Introduction

The region of entropic vectors is a fundamental region in information theory that both gives all possible information inequalities, as well as the rate regions for coded networks [13], [15], [14], [12] utilizing multiple source multicasts.

While it is known to be a convex cone, the exact characterization of the closure of the region of entropic vectors $\bar{\Gamma}^*_N$ is still an open problem for $N \geq 4$. However, one can use outer or inner bounds of $\bar{\Gamma}^*_N$ to replace it in the rate region expression in order to obtain inner bounds and outer bounds for the network coding capacity region. When these bounds match for the network in question, the rate region has been determined exactly. For example, in our previous work [4], [5], we presented algorithms combining inner bounds obtained from representable matroids, together with Shannon outer bound, to determine coding rate regions for multi-terminal coded networks. A merit of the method of multiple source multicast rate region computation presented there is that the representable matroid inner bound naturally corresponds to the use of linear codes over the specified field size, and these codes can be reconstructed from the rate region [4]. Our first rate region computation technique [5] worked with an inequality representation of the cone of binary representable matroids obtained from a theorem of Hassibi et al. [3] as an inner bound, however this later proved to have unbearable computational complexity for even small networks due to the requirement of calculating the convex cone of matroids. Improving upon this idea, the computational approach we presented in [4] utilized an extreme ray representation of the cone of $\mathbb{F}_q$ representable matroid inner bounds for $q \in \{2, 3, 4\}$ that is natural given the forbidden minor characterization for representability over these field sizes [10]. Namely, the extreme ray representation discussed there is obtained by 1) removing from a list of non-isomorphic matroids those having the forbidden minors, then 2) adding back their permutations and removing those that are not conically independent. The switch to working with the extreme ray representation of the region allowed the bounds to be calculated efficiently for small numbers of variables/ground set sizes, and thus enabled the capacity regions for a class of small networks to be calculated exactly.

However, the full lists of non-isomorphic matroid ranks are only available on ground set sizes $N \leq 9$ [8]. Furthermore, the method of removing from the list of non-isomorphic matroids those with forbidden minors for representability then adding their permutations and taking the conic hull is computationally intensive. Thus, this paper derives in §IV a series of theoretical results about the extremal representations for the inner bounds for the region of entropic vectors that allows us in §V to provide a method of listing them with substantially further reduced complexity. For the sake of completeness and to provide context, these novel theoretical results in §IV and the new algorithm in §V follow a brief review in §II and §III of how network coding capacity regions can be calculated from bounds on the region of entropic vectors, and the various bounds available for the region of entropic vectors, respectively.

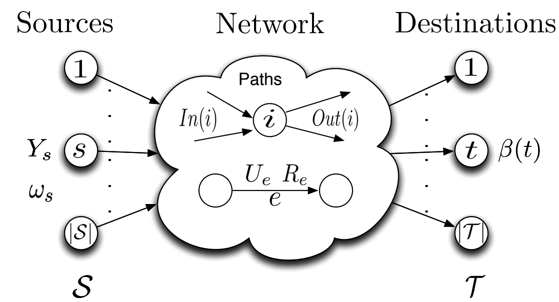

Figure 1. A general network model

II. Rate regions for coded networks

It is known that multiple important rate regions in multiterminal information theory can be directly expressed in terms of the region of entropic vectors [14], including those for distributed source coding [15], multi-level diversity coding systems [4], [5], and peer-to-peer networks [12]. Here we will review the expression for the capacity region for networks under multiple multicast network coding.

Suppose we have a network as shown in Figure 1. There are independent sources $\mathcal{S}$, communication links (edges) $\mathcal{E}$, sink nodes $\mathcal{T}$. For each $s \in \mathcal{S}$, the associated source variables is Y_s with source rate ω_s. For each edge $e \in \mathcal{E}$, the associated random variable is U_e with edge capacity R_e. For an intermediate node i, we denote its incoming edges as $\mathrm{In}(i)$ and outgoing edges as $\mathrm{Out}(i)$. For each $t \in \mathcal{T}$, the output is $\beta(t)$, a subset of source variables and $\beta(t)$ can vary across t. According to [14], the coding rate (capacity) region $\mathcal{R}$ can be expressed as follows. If we collect all $Y_s, s \in \mathcal{S}$ and $U_e, e \in \mathcal{E}$ as random variables and assume $|\{Y_s \cup U_e, s \in \mathcal{S}, e \in \mathcal{E}\}| = N$, then

$$\mathcal{R} \quad = \quad \text{Ex}(\text{proj}_{U_e}(\overline{\text{con}(\Gamma_N^* \cap \mathcal{L}_{234})} \cap \mathcal{L}_{15})), \qquad (1)$$

where Γ_N^* is the region of entropic vectors (discussed in §III), $\text{con}(\mathcal{B})$ is the convex hull of $\mathcal{B}$, $\text{proj}_{U_e}(\mathcal{B})$ is the projection of the set $\mathcal{B}$ on the coordinates $(h_{U_e}|e \in \mathcal{E})$, and $\text{Ex}(\mathcal{B}) = \{\mathbf{h} \in \mathbb{R}_+^{2^N-1} : \mathbf{h} \geq \mathbf{h}' \text{ for some } \mathbf{h}' \in \mathcal{B}\}$, for $\mathcal{B} \subset \mathbb{R}_+^{2^N-1}$. Further, $\mathcal{L}_i, i = 1, 2, \ldots 5$ are network constraints representing source rate constraints, source independency, source nodes coding, intermediate nodes coding, sink nodes decoding, respectively (listed below). Finally, $\mathcal{L}_{234} = \mathcal{L}_2 \cap \mathcal{L}_3 \cap \mathcal{L}_4$ and $\mathcal{L}_{15} = \mathcal{L}_1 \cap \mathcal{L}_5$. The network constraints naturally reflect the reproduction requirements and functional requirements of the network graph, namely:

$$\mathcal{L}_1 \quad = \quad \{\mathbf{h} \in \Gamma_N^* : h_{Y_s} \geq \omega_s\} \qquad (2)$$
$$\mathcal{L}_2 \quad = \quad \{\mathbf{h} \in \Gamma_N^* : h_{Y_\mathcal{S}} = \Sigma_{s \in \mathcal{S}} h_{Y_s}\} \qquad (3)$$
$$\mathcal{L}_3 \quad = \quad \{\mathbf{h} \in \Gamma_N^* : h_{X_{\text{Out}(k)}|Y_s} = 0\} \qquad (4)$$
$$\mathcal{L}_4 \quad = \quad \{\mathbf{h} \in \Gamma_N^* : h_{X_{\text{Out}(i)}|X_{\text{In}(i)}} = 0\} \qquad (5)$$
$$\mathcal{L}_5 \quad = \quad \{\mathbf{h} \in \Gamma_N^* : h_{Y_{\beta(t)}|U_{\text{In}(t)}} = 0\}. \qquad (6)$$

While this in principle calculates the capacity region of any network under network coding, as will be discussed in §III, Γ_N^* is unknown and is not even polyhedral for $N \geq 4$. Thus, the direct calculation of rate regions from equation (1) for a network with more than 4 variables is infeasible. However, replacing Γ_N^* with polyhedral inner and outer bounds transforms (1) into a polyhedron, which involves applying some constraints to a polyhedra and then projecting down onto some coordinates. This inspires us to substitute Γ_N^* with its closed polyhedral outer and inner bounds respectively, and get an outer $\mathcal{R}_{\text{out}}$ and inner bound $\mathcal{R}_{\text{in}}$ on the rate region. Several techniques for calculating these bounds are discussed in [4], [5]. If $\mathcal{R}_{\text{out}} = \mathcal{R}_{\text{in}}$, we know $\mathcal{R} = \mathcal{R}_{\text{out}}$. We pass now to discussing the bounds on the region on entropic vectors utilized in [4], [5], after which we will derive some new properties of the inner bounds that allows the complexity of calculating it to be further reduced from [4], [5].

III. Bounds for the Region of entropic vectors Γ_N^*

We would like to first review the region of entropic vectors and then discuss the bounds on it.

A. Region of entropic vectors Γ_N^*

Consider an arbitrary collection $\mathbf{X} = (X_1, \ldots, X_N)$ of N discrete random variables with joint probability mass function p_X. To each of the $2^N - 1$ non-empty subsets of the collection of random variables, $X_\mathcal{A} := (X_i | i \in \mathcal{A})$ with $\mathcal{A} \subseteq \{1, \ldots, N\} \equiv [[N]]$, there is associated a joint Shannon entropy $H(X_\mathcal{A})$. Stacking these subset entropies for different subsets into a $2^N - 1$ dimensional vector we form an entropy vector

$$\mathbf{h} = [H(X_\mathcal{A}) \,|\mathcal{A} \subseteq [[N]], \mathcal{A} \neq \emptyset]\,. \qquad (7)$$

By virtue of having been created in this manner, the vector $\mathbf{h}$ must live in some subset of $\mathbb{R}_+^{2^N-1}$, and is said to be *entropic* due to the existence of p_X. However, not every point in $\mathbb{R}_+^{2^N-1}$ is entropic since for many points, there does not exist an associated valid distribution p_X. The collection of all entropic vectors form a region denoted as Γ_N^*. It is known that the closure of the region of entropic vectors $\bar{\Gamma}_N^*$ is a convex cone [14].

B. Shannon outer bound Γ_N

Next observe that elementary properties of Shannon entropies indicates that $H(X_\mathcal{A})$ is a non-decreasing submodular function, so that $\forall \mathcal{A} \subseteq \mathcal{B} \subseteq [[N]], \forall \mathcal{C}, \mathcal{D} \subseteq [[N]]$

$$H(X_\mathcal{A}) \quad \leq \quad H(X_\mathcal{B}) \qquad (8)$$
$$H(X_{\mathcal{C}\cup\mathcal{D}}) + H(X_{\mathcal{C}\cap\mathcal{D}}) \quad \leq \quad H(X_\mathcal{C}) + H(X_\mathcal{D}). \qquad (9)$$

Since they are true for any collection of subset entropies, these linear inequalities (8), (9) can be viewed as supporting halfspaces for Γ_N^*.

Thus, the intersection of all such inequalities form a polyhedral outer bound Γ_N for Γ_N^* and $\bar{\Gamma}_N^*$, where $\forall \mathcal{A} \subseteq \mathcal{B} \subseteq [[N]]$ and $\forall \mathcal{C}, \mathcal{D} \subseteq [[N]]$

$$\Gamma_N := \left\{ \mathbf{h} \in \mathbb{R}^{2^N-1} \,\middle|\, \begin{array}{c} h_\mathcal{A} \leq h_\mathcal{B} \\ h_{\mathcal{C}\cup\mathcal{D}} + h_{\mathcal{C}\cap\mathcal{D}} \leq h_\mathcal{C} + h_\mathcal{D} \end{array} \right\}.$$

This outer bound Γ_N is known as the *Shannon outer bound*, as it can be thought of as the set of all inequalities resulting from the positivity of Shannon's information measures among the random variables. Fujishige observed in 1978 [2] that the entropy function for a collection of random variables $(X_i, i \in [[N]])$ viewed as a set function is a polymatroid rank function, where a set function $\rho : 2^S \to \mathbb{R}_+$ is a rank function of a polymatroid if it obeys the following axioms:

1) Normalization: $\rho(\emptyset) = 0$;
2) Monotonicity: if $A \subseteq B \subseteq S$ then $\rho(A) \leq \rho(B)$;
3) Submodularity: if $A, B \subseteq S$ then $\rho(A \cup B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

While $\Gamma_2 = \Gamma_2^*$ and $\Gamma_3 = \bar{\Gamma}_3^*$, $\bar{\Gamma}_N^* \subsetneq \Gamma_N$ for all $N \geq 4$ [14], and indeed it is known [1] that $\bar{\Gamma}_N^*$ is not even polyhedral for $N \geq 4$.

C. Matroid basics

Matroid theory [10] is an abstract generalization of the notion of independence in the context of linear algebra to the more general setting of set systems, i.e., collections of subsets of a ground set obeying certain axioms. The ground set of size N is without loss of generality $S = [[N]]$, and in our context each element of the ground set will correspond to a random variable. There are numerous equivalent definitions of matroids, we first present one commonly used in terms of independent sets.

Definition 1: [10] A matroid M is an ordered pair $(S, \mathcal{I})$ consisting of a finite set S (the ground set) and a collection $\mathcal{I}$ (called independent sets) of subsets of S obeying:

1) Normalization: $\emptyset \in \mathcal{I}$;
2) Heredity: If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$;
3) Independence augmentation: If $I_1 \in \mathcal{I}$ and $I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there is an element $e \in I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

Another definition of matroids utilizes *rank functions*. For a matroid $M = (S, \mathcal{I})$ with $|S| = N$ the rank function

$r : 2^S \to \{0, \dots, N\}$ is defined as the size of the largest independent set contained in each subset of S, i.e., $r(A) = \max_{B \subseteq A}\{|B| : B \in \mathcal{I}\}$. The rank of a matroid, r_M, is the rank of the ground set, $r_M = r(S)$. The rank function of a matroid can be shown to obey the following properties. In fact these properties may instead be viewed as an alternate definition of a matroid in that any set function obeying these axioms is the rank function of a matroid.

Definition 2: A set function $r : 2^S \to \{0, \dots, N\}$ is a rank function of a matroid if it obeys the following axioms:

1) Cardinality: $r(A) \leq |A|$;
2) Monotonicity: if $A \subseteq B \subseteq S$ then $r(A) \leq r(B)$;
3) Submodularity: if $A, B \subseteq S$ then $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

We denote the collection of all matroid ranks on N elements as $\mathbb{M}_N$. There are many operations on matroids, such as *contraction* and *deletion*. Details about these operations can be found in [10]. Next, we define the important concept of *minor* based on these two operations.

Definition 3: If M is a matroid on S and $T \subseteq S$, a matroid M' on T is called a *minor* of M if M' is obtained by any combination of deletion (\) and contraction (/) of M.

The operations of deletion and contraction mentioned above yield new matroids with new rank functions for the minors. Specifically, let M/T denote the matroid obtained by contraction of M on $T \subset S$, and let $M \setminus T$ denote the matroid obtained by deletion from M of $T \subset S$. Then, by [10] (3.1.5,7), $\forall X \subseteq S - T$

$$\begin{aligned} r_{M/T}(X) &= r_M(X \cup T) - r_M(T) \\ r_{M \setminus T}(X) &= r_M(X) \end{aligned} \tag{10}$$

To each set function $r_N : 2^{[[N]]} \to \mathbb{R}_{\geq 0}$ we will associate a vector $\mathbf{r}_N \in \mathbb{R}_{\geq 0}^{2^N - 1}$ formed by stacking the various values of the function r_N into a vector, e.g., in a manner associated with a binary counter:

$$\mathbf{r} = \begin{bmatrix} r(\{1\}) \\ r(\{2\}) \\ r(\{1,2\}) \\ r(\{3\}) \\ r(\{1,3\}) \\ r(\{2,3\}) \\ r(\{1,2,3\}) \\ r(\{4\}) \\ \vdots \end{bmatrix} \tag{11}$$

For any such function, r_N, and hence for any such vector $\mathbf{r}_N$, for any pair of sets $\mathcal{A}, \mathcal{B} \subseteq [[N]]$ we will define the *minor* associated with deleting $[[N]] \setminus (\mathcal{A} \cup \mathcal{B})$ and contracting on $\mathcal{A}$ as

$$r_{\mathcal{B}|\mathcal{A}}(\mathcal{C}) := r(\mathcal{C} \cup \mathcal{A}) - r(\mathcal{A}) \quad \forall \mathcal{C} \subseteq \mathcal{B} \tag{12}$$

and $\mathbf{r}_{\mathcal{B}|\mathcal{A}}$ will denote the associated vector, ordered again by a binary counter whose bit positions are created by enumerating again the elements of $\mathcal{B}$ (i.e., keeping the same order). If r is the rank function of a matroid, this definition is consistent with the definition of the matroid operations of taking a minor, deleting and contracting, although we will apply them to any real valued set function here.

Another important concept in matroid theory is that of connected matroids, which is similar to connected polymatroids.

Definition 4: A matroid M on S with rank function r is connected if $\forall A \subsetneq S, r(A) + r(S \setminus A) > r(S)$ where $A \neq \emptyset$ and $A \neq S$.

When M is disconnected, there exists $A \subsetneq S$ such that $r(A) + r(S \setminus A) = r(S)$. It is not hard to observe that there exist two other rank functions r_1, r_2 such that $r(X) = r_1(X) + r_2(X), \forall X \subseteq S$ where $r_1(X) = r(X \cap A)$ and $r_2(X) = r(X \cap (S \setminus A))$. Therefore, when a matroid is disconnected, its rank function can be expressed as sum of two other matroid ranks.

Though there are many classes of matroids, we are especially interested in one of them, *representable matroids*, because they can be related to linear codes to solve network coding problems as discussed in [4], [5].

D. Representable matroids

Representable matroids are an important class of matroids which connect the independent sets to the conventional notion of independence in a vector space.

Definition 5: A matroid M with ground set S of size $|S| = N$ and rank $r_M = r$ is representable over a field $\mathbb{F}$ if there exists a matrix $A \in \mathbb{F}^{r \times N}$ such that for each independent set $I \in \mathcal{I}$ the corresponding columns in A, viewed as vectors in $\mathbb{F}^r$, are linearly independent.

There has been significant effort towards characterizing the set of matroids that are representable over various field sizes, with a complete answer only available for fields of sizes two, three, and four. For example, the characterization of binary representable matroids, due to Tutte [11], is:

Theorem 1: (Tutte) A matroid M is binary representable (representable over a binary field) iff it does not have the matroid $U_{2,4}$ as a minor.

Here, $U_{k,N}$ is the *uniform* matroid on the ground set $S = [N]$ with independent sets $\mathcal{I}$ equal to all subsets of $[N]$ of size at most k. For example, $U_{2,4}$ has as its independent sets

$$\mathcal{I} = \{\emptyset, 1, 2, 3, 4, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}. \tag{13}$$

Another important observation is that all matroids are representable, at least in some field, for $N \leq 7$. The *Vámos* matroid is an example of a non-representable matroid on 8 elements [10].

E. Inner bounds from representable matroids

Suppose a matroid M with ground set $\mathcal{S}$ of size $|\mathcal{S}| = N$ and rank $r(\mathcal{S}) = k$ is representable over the finite field $\mathbb{F}_q$ of size q and the representing matrix is $\mathbf{A} \in \mathbb{F}_q^{k \times N}$ such that $\forall B \subseteq \mathcal{S}\ r(B) = \text{rank}(\mathbf{A}_{:,B})$, the matrix rank of the columns of $\mathbf{A}$ indexed by B. Let Γ_N^q be the conic hull of all rank functions of matroid with N elements and representable in $\mathbb{F}_q$. This provides an inner bound $\Gamma_N^q \subseteq \bar{\Gamma}_N^*$, because any extremal rank function r of Γ_N^q is by definition representable and hence is associated with a matrix representation $\mathbf{A} \in \mathbb{F}_q^{k\times N}$, from which we can create the random variables

$$(X_1, \dots, X_N) = \mathbf{u}\mathbf{A}, \quad \mathbf{u} \sim \mathcal{U}(\mathbb{F}_q^k). \tag{14}$$

whose elements are $h_A = r(A)\log_2 q, \forall A \subseteq \mathcal{S}$. Hence, all extreme rays of Γ_N^q are entropic, and $\Gamma_N^q \subseteq \bar{\Gamma}_N^*$, as discussed in [4], [5].

IV. Main results: properties of matroid bounds

This section shows the main results for this paper, while some long proofs are reserved in §VI.

We begin by noting that one can determine if a given integer valued vector of dimensions $2^N - 1$ is a rank vector of a matroid by checking all of its size 2 minors. While it is a simple observation that follows from the definition of a matroid, this result will help us prove several other more useful results.

Theorem 2: An integer valued set function is the rank function of a matroid if and only if all of its size 2 minors are matroids. Equivalently, for any $\mathbf{r}_N \in \mathbb{Z}_{\geq 0}^{2^N-1}, \mathbf{r}_N \in \mathbb{M}_N$ if and only if $\mathbf{r}_{\{i,j\}|\mathcal{A}} \in \mathbb{M}_2$ for every $\mathcal{A} \subseteq [[N]]\backslash\{i,j\}$ and every $\{i,j\} \subseteq [[N]]$.

The proof is in §VI.

Next, we present properties of the matroid bounds on $\bar{\Gamma}_N^*$. When examining properties of the bounds obtained from matroid ranks, we found that all matroid ranks are extremal in the convex hull of them, i.e., no rank can be expressed as a convex combination of some other ranks with non-zero coefficients.

Theorem 3: [Matroid Rank Vectors are Convex Independent] Any collection of matroid rank vectors $\mathcal{V} \subseteq \mathbb{M}_N$ are convex independent. Equivalently, the set of extreme points of the convex hull $\mathrm{convex}(\mathcal{V})$ is $\mathcal{V}$ itself. Equivalently, a matroid rank vector can not be expressed as a convex combination of any other matroid rank vectors other than itself.

The proof is in §VI. This property does not extend to the conic hull. Our next result is based on Theorem 3.

Theorem 4: [Conically Dependent Matroids are Simple Sums] Any matroid rank vector which is not an extreme ray of the conic hull $\mathrm{cone}(\mathbb{M}_N)$ is the simple sum of a collection of matroid rank vectors that are extreme rays. That is, the coefficients in the conic combination may all be taken to be one.

Proof: Suppose a rank vector $\mathbf{r}_N \notin \mathrm{Ext}(\mathrm{cone}(\mathbb{M}_N))$. Nguyen [9] proved that a matroid rank $\mathbf{r}'_N \in \mathrm{Ext}(\mathrm{cone}(\mathbb{M}_N)) \Leftrightarrow \mathbf{r}'_N$ is connected (which by definition of connectedness means $\mathbf{r}'_N$ can not be written as a sum of two or more other matroids). As such, $\mathbf{r}_N$ is not connected and can thus be written as the sum of two or more other matroids, i.e $\exists \mathcal{V} \subseteq \mathbb{M}_N \backslash \mathbf{r}_N$ such that $\mathbf{r}_N = \sum_{\mathbf{r}_N^i \in \mathcal{V}} \mathbf{r}_N^i$. If $\forall i, \mathbf{r}_N^i$ is connected, we are done. However, if $\exists i$ such that $\mathbf{r}_N^i$ is not connected, we can express $\mathbf{r}_N^i$ as the sum of other matroids. Continue applying the decomposition until only connected matroids remain. This process will finish, because $|\mathbb{M}_N| < \infty$ and each one can appear in the sum at most once, for otherwise they would be scaled by an integer number other than one. Such a scaling other than one is not allowed, for it will violate the cardinality requirement (e.g., on one of the singleton sets) for any matroid other than the trivial all zero rank function matroid. ■

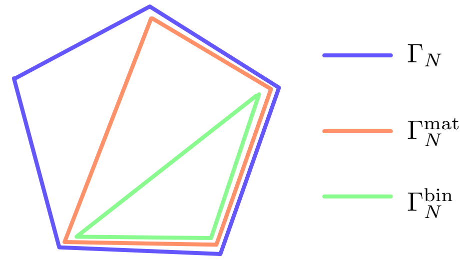

Figure 2. Extreme rays relationship: $\mathrm{Ext}(\Gamma_N^{\mathrm{bin}}) \subseteq \mathrm{Ext}(\Gamma_N^{\mathrm{mat}}) \subseteq \mathrm{Ext}(\Gamma_N)$

We will discuss the relationship between three sets related to $\bar{\Gamma}_N^*$: The Shannon outer bound Γ_N, the conic hull of matroids Γ_N^{mat} and the conic hull of $\mathbb{F}_q$-representable matroids Γ_N^q.

Since for $N \leq 7$, all matroids are representable, we know that $\Gamma_N^{\mathrm{mat}} \subseteq \bar{\Gamma}_N^*, N \leq 7$. In addition, we observed that, for $N = 4, 5, 6$, the extreme rays of Γ_N^{bin} are a subset of extreme rays of Γ_N^{mat}, which themselves are a subset of extreme rays of Γ_N, the Shannon outer bound. This paper aims to prove this relationship for all N.

Define $\mathcal{T}_N^{\mathrm{bin}} = \mathrm{cone}(\mathrm{Bin}(\mathrm{Ext}(\Gamma_N^{\mathrm{mat}})))$ and $\mathcal{T}_N^{\mathrm{mat}} = \mathrm{cone}(\mathrm{Mat}(\mathrm{Ext}(\Gamma_N)))$, where $\mathrm{Ext}(\cdot)$ is the function to get extreme rays, $\mathrm{Bin}(\cdot)$ is to choose binary representable ones, $\mathrm{Mat}(\cdot)$ is to choose valid matroidal ones, and $\mathrm{cone}(\cdot)$ is to get the conic hull of a set of rank vectors. We see that $\mathcal{T}_N^{\mathrm{bin}}$ is the conic hull of the binary representable extreme rays of Γ_N^{mat} and $\mathcal{T}_N^{\mathrm{mat}}$ is the conic hull of matroidal extreme rays of Γ_N. We found that $\mathrm{Ext}(\Gamma_N^{\mathrm{bin}}) \subseteq \mathrm{Ext}(\Gamma_N^{\mathrm{mat}}) \subseteq \mathrm{Ext}(\Gamma_N)$, as shown in Figure 2. Equivalently, we have the following theorem.

Theorem 5: [Extremal Matroids are Extremal Polymatroids] Every extreme ray of $\mathrm{cone}(\mathbb{M}_N)$ is an extreme ray of Γ_N. Equivalently, $\Gamma_N^{\mathrm{mat}} = \mathcal{T}_N^{\mathrm{mat}}$.

Proof: First note that an extreme ray $\mathbf{r}_N$ of $\mathrm{cone}(\mathbb{M}_N)$ must be connected. Otherwise, there exists a separator $A \subsetneq N$ such that $r(N) = r(A) + r(N \setminus A)$. Then there exist two other rank functions r_1, r_2 such that $r(X) = r_1(X) + r_2(X), \forall X \subseteq S$ where $r_1(X) = r(X \cap A)$ and $r_2(X) = r(X \cap (S \setminus A))$. Therefore, $r(N)$ can be expressed as sum of two other ranks and this contradicts the assumed extremality. In [9], Nguyen proved that a connected matroid rank is extremal in the polymatroid cone, i.e., is an extremal polymatroid. Together with the observation above, we complete the proof. ■

An alternate proof based on Theorem 2 is in §VI. Since any extremal polymatroid that is a matroid must be an extremal matroid (which follows from the fact that every matroid is a polymatroid), this shows that one can determine the list of extremal matroids by considering the matroidal extremal polymatroids.

Similarly, we can establish a relationship between the representable matroids inner bound and the general matroids bound.

Theorem 6: [Forbidden Minors and Extremality] Let $\mathcal{V}$ be a set of matroid rank vectors formed by removing from $\mathbb{M}_N$ (exclusively) those with a certain collection of connected forbidden minors. The extreme rays of $\text{cone}(\mathcal{V})$ are all extreme rays of $\text{cone}(\mathbb{M}_N)$.

The following lemma is useful for the proof of Theorem 6.

Lemma 1: A matroid that is not an extreme ray of $\text{cone}(\mathbb{M}_N)$ has a connected forbidden minor if and only if at least one of the extremal matroids that it can be represented as the sum of has the connected forbidden minor.

Proof: Suppose a rank vector $\mathbf{r}_N \notin \text{Ext}(\text{cone}(\mathbb{M}_N))$. According to Theorem 4, $\exists \mathcal{V} \subseteq \mathbb{M}_N \backslash \mathbf{r}_N$ such that $\mathbf{r}_N = \sum_{\mathbf{r}_N^i \in \mathcal{V}} \mathbf{r}_N^i$. Suppose the forbidden minor on $\mathcal{C} \subseteq S$ is obtained by contracting $\mathcal{A} \subseteq S \backslash \mathcal{C}$ and deleting $S \backslash (\mathcal{C} \cup \mathcal{A})$. For $\mathcal{B} \subseteq \mathcal{C}$,

$$\begin{aligned} r_{\mathcal{C}|\mathcal{A}}(\mathcal{B}) &= r_N(\mathcal{B} \cup \mathcal{A}) - r_N(\mathcal{A}) \\ &= \sum_{\mathbf{r}_N^i \in \mathcal{V}} r_N^i(\mathcal{B} \cup \mathcal{A}) - \sum_{\mathbf{r}_N^i \in \mathcal{V}} r_N^i(\mathcal{A}) \\ &= \sum_{\mathbf{r}_N^i \in \mathcal{V}} (r_N^i(\mathcal{B} \cup \mathcal{A}) - r_N^i(\mathcal{A})). \\ &= \sum_{\mathbf{r}_N^i \in \mathcal{V}} r_{\mathcal{C}|\mathcal{A}}^i(\mathcal{B}) \end{aligned}$$

We observe that the minor of $\mathbf{r}_N$ is the sum of minors of $\mathbf{r}_N^i$. By assumption, $r_{\mathcal{C}|\mathcal{A}}(\mathcal{B})$ is equal to the connected forbidden minor. However, since it is connected, all but one of the component minors need to be the trivial all-zero rank vector, for otherwise the minor would be the sums of non-trivial rank vectors, and the thus not be connected. That is to say, there exists an i such that $r_{\mathcal{C}|\mathcal{A}}^i(\mathcal{B}) = r_{\mathcal{C}|\mathcal{A}}(\mathcal{B})$. This shows that $\mathbf{r}_N^i$ must have the forbidden minor. ■

Now we give the proof of Theorem 6.

Proof: [**Proof of Theorem 6**] Suppose $\mathbf{r}_N \in \text{Ext}(\text{cone}(\mathcal{V}))$ but $\mathbf{r}_N \notin \text{Ext}(\text{cone}(\mathbb{M}_N))$. As such, $\mathbf{r}_N$ can not have the forbidden minors. From Lemma 1, $\mathbf{r}_N$ must be expressible as a sum of extremal matroid ranks, all of which do not have the forbidden minors. But this contradicts the extremality within $\text{cone}(\mathcal{V})$, for these other ranks must be in $\mathcal{V}$ as well (since they do not have the forbidden minors), and now a conic combination of them equals the supposed extreme ray $\mathbf{r}_N$. ■

Corollary 1: [Extremal $\mathbb{F}_q$ Linear Representable Matroids are Extremal Matroids for $q \in \{2, 3, 4\}$] Every extreme ray of $\text{cone}(\mathbb{M}_N^q)$ is an extreme ray of $\text{cone}(\mathbb{M}_N)$.

Proof: Follows from [10] showing the forbidden minor characterizations of these classes of matroids, together with Theorem 6. ■

V. Reduction on computation complexity

One potential benefit of the relationships between extreme rays of different bounds proven in the previous section is to reduce computation complexity in obtaining the extreme-ray representation of representable matroid inner bound.

Table I. Cardinality comparison of different sets for $N = 4, 5, 6$

	$N = 4$	$N = 5$	$N = 6$
$\lvert\text{Ext}(\Gamma_N)\rvert$	41	117984	N/A
$\lvert\text{Ext}(\Gamma_N^{\text{space}})\rvert^*$	35	7944	N/A
$\lvert\mathbb{M}_N\rvert$	68	406	3035
$\lvert\text{Ext}(\Gamma_N^{\text{mat}})\rvert$	27	154	1785
$\lvert\text{Ext}(\Gamma_N^{\text{bin}})\rvert$	26	127	1205

$^*\Gamma_N^{\text{space}}$ is the conic hull of linear space ranks

For instance, in [4], an extreme-ray representation of Γ_N^{bin} is obtained by excluding ranks containing $U_{2,4}$ as minor from the full list of matroid ranks, and then taking the conic hull. We observed that only a fraction of the ranks are extreme rays in the conic hull. For instance, for $N = 4, 5, 6$, as shown in Table I, only about 50% of them are extreme rays. Similar results for more general cases can be found in [7]. Although it is conjectured in [7] that asymptotically almost every matroid is connected and hence the fraction of all matroids that are connected (extremal) goes to 1 asymptotically, the ratio is around 0.5 for small ground set sizes, including those considered in this paper. Furthermore, [7] only successfully proves a result that asymptoticly the ratio is at least 0.5.

In Table I, the all-zero rank is included in the number of all ranks but not included in the extreme rays. Also, we know that $\text{Ext}(\Gamma_N^{\text{bin}}) \subseteq \text{Ext}(\Gamma_N^{\text{mat}})$, the method in [4] is a waste of computations because those ranks are not extreme rays. In fact, it suffices to check the $U_{2,4}$ containment in the list of $\text{Ext}(\Gamma_N^{\text{mat}})$, which can be obtained by checking the cardinality and integrality of $\text{Ext}(\Gamma_N)$.

However, it is easy to obtain inequalities representation for Γ_N but difficult to obtain extreme rays of Γ_N. The enumeration of all matroid ranks $\mathbb{M}_N$ reaches a computation wall for $N = 10$ [6]. Consider the tiny fraction of extremal representable matroid inner bound and extreme rays of Γ_N and Γ_N^{mat}; a more efficient way to obtain a representable matroid inner bound may be to directly enumerate connected (and thus extremal) matroids without particular forbidden minors. The results in this paper showing that it suffices to enumerate these direclty lay the foundation for our future work on this type of enumeration, which will allow us to obtain a representable matroid inner bound for $N \geq 10$.

In fact, some additional savings may be achieved by observing some additional properties regarding the matroid ranks after constraints have been added in network coding problems. Indeed, there are only $|\mathcal{S}|$ independent random variables in the networks because to all edge variables are functions of the sources. Thus, we only need to consider the representable matroid inner bounds obtained from matroids with ranks up to $|\mathcal{S}|$. For a network $|\mathcal{S}| < N$, this observation can further reduce the complexity of obtaining the desired inner bound to start the rate region computation from representable matroid inner bounds.

Finally, we observe that when vector codes are considered [4], linear space inner bound Γ_N^{space} (can be viewed as projection of representable matroids) is needed. Hence to obtain better inner bounds than the matroid bounds, projection of the representable matroid inner bounds will be necessary.

VI. Proofs

In this section, we give proofs of some theorems in §IV. At first, we would like to give a lemma that will be used in the later proofs.

Lemma 2: Suppose $\mathbf{r}, \mathbf{r}'$ are two ranks of matroids M_1, M_2 on S, respectively. $\mathbf{r} = \mathbf{r}'$ if and only if $\forall i, j \in S$, for every combination of deletion and contraction operations, the ranks $\mathbf{r}_{\{i,j\}}$ and $\mathbf{r}'_{\{i,j\}}$ of the obtained minors on $\{i, j\}$, are equal.

Proof: $\Rightarrow$: This is trivial since all minors of two equal ranks must be equal.
$\Leftarrow$: We will prove by induction that the entries of all subsets in the two rank functions are equal. First observe that entries of all size 1 and 2 subsets are equal, since $\forall i, j \in S$, we can obtain the size-2 minor on $\{i, j\}$ by deleting $S \setminus \{i, j\}$.

Now suppose the ranks of all size m subsets are equal, we will show that the entries of all size $m+1$ subsets are also equal. Let $\mathcal{C} \subseteq S$, with $|C| = m$ such that $\forall B \subseteq C$, $r(B) = r'(B)$. Consider the size-2 minor on $e_1 \in C, e_2 \in S \setminus C$ by contracting $C \cup e_2 \setminus e_1$. As assumed, $r_{e_1,e_2}(e_1, e_2) = r'_{e_1,e_2}(e_1, e_2)$, i.e, $r(C \cup e_2) - r(C \cup e_2 \setminus e_1) = r'(C \cup e_2) - r'(C \cup e_2 \setminus e_1)$. Since $|C \cup e_2 \setminus e_1| = m$, $r(C \cup e_2 \setminus e_1) = r'(C \cup e_2 \setminus e_1)$. Thus $r(C \cup e_2) = r'(C \cup e_2)$. So size $m+1$ subsets also have the same entries in $\mathbf{r}$ and $\mathbf{r}'$. ∎

Now we would like to prove Theorem 2.

Proof: [**Proof of Theorem 2**] $\Rightarrow$: This is trivial since the operations are taking minors and a minor of a matroid is also a matroid.
$\Leftarrow$: To prove one vector is a rank for matroid, we need to show that it satisfies the three conditions in Definition 2. We know that $\mathbf{r}_{\{i,j\}|\mathcal{A}}$ is a rank for a matroid, so it must also satisfy the three conditions.

Cardinality: we first let $\mathcal{A} = \emptyset$, then

$$\begin{aligned} 0 \leq r_{\{i,j\}|\mathcal{A}}(\mathcal{B}) &= r_N(\mathcal{A} \cup \mathcal{B}) - r_N(\mathcal{A}) \\ &= r_N(\mathcal{B}) \leq |\mathcal{B}|. \end{aligned}$$

This shows cardinality constraint holds for any subset $\mathcal{B}$ with $|\mathcal{B}| \leq 2$.

For a subset $\mathcal{C}$ with size of 3, if exists, there exists a one-element subset $\mathcal{A}$ and an 2-element subset $\mathcal{B}$ such that $\mathcal{C} = \mathcal{A} \cup \mathcal{B}$. Let the rank $\mathbf{r}_{\{i,j\}|\mathcal{A}}$ is obtained as $r_{\{i,j\}|\mathcal{A}}(\mathcal{B}) = r_N(\mathcal{A} \cup \mathcal{B}) - r_N(\mathcal{A})$, we have

$$\begin{aligned} r_{\{i,j\}|\mathcal{A}}(\mathcal{B}) &= r_N(\mathcal{A} \cup \mathcal{B}) - r_N(\mathcal{A}) \\ &= r_N(\mathcal{C}) - r_N(\mathcal{A}) \\ &\leq |\mathcal{B}| = 2. \end{aligned}$$

Since we know for any subset with size not greater than 2, it satisfies the cardinality requirement, we obtain

$$r_N(\mathcal{C}) \leq r_N(\mathcal{A}) + 2 \leq 3 = |\mathcal{C}|.$$

Similarly, suppose for a subset $\mathcal{B}$ of $[N]$ with size of m, we have $r_N(\mathcal{B}) \leq m$. For subset $\mathcal{C}$ with size of $m+1$, there exists one-element subset $\mathcal{A}$ such that $\mathcal{C} = \mathcal{A} \cup \mathcal{B}$. Let the rank $\mathbf{r}_{\mathcal{B}|\mathcal{A}}$ is obtained as $r_{\mathcal{B}|\mathcal{A}}(\mathcal{B}) = r_N(\mathcal{A} \cup \mathcal{B}) - r_N(\mathcal{A})$, we will have

$$r_{\mathcal{B}|\mathcal{A}}(\mathcal{B}) = r_N(\mathcal{C}) - r_N(\mathcal{A}) \leq |\mathcal{B}| = m.$$

So,

$$r_N(\mathcal{C}) \leq r_N(\mathcal{A}) + m \leq m + 1 = |\mathcal{C}|.$$

This shows that for any subset A of $[N]$, $0 \leq r_N(A) \leq |A|$.
Monotonicity: suppose $A \subseteq B \subseteq [N]$, if $|B - A| \leq 2$, there must exist $\{i, j\}$, $\mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \{i, j\}$ and $\mathcal{A} \subseteq [N] \setminus \{i, j\}$ such that $A = \mathcal{A} \cup \mathcal{B}_1$ and $B = \mathcal{A} \cup \mathcal{B}_2$. Let the rank obtained as $r_{\{i,j\}|\mathcal{A}}(\mathcal{B}) := r_N(\mathcal{A} \cup \mathcal{B}) - r_N(\mathcal{A})$, $\mathcal{B} \subseteq \{i, j\}$. Since $r_{\{i,j\}|\mathcal{A}}(\mathcal{B}_1) \leq r_{\{i,j\}|\mathcal{A}}(\mathcal{B}_2)$, we have

$$r_N(\mathcal{A} \cup \mathcal{B}_1) - r_N(\mathcal{A}) \leq r_N(\mathcal{A} \cup \mathcal{B}_2) - r_N(\mathcal{A})$$

which is equivalent to $r_N(A) \leq r_N(B)$.

If $|B - A| > 2$, there must exist positive number m subsets $A_1, \ldots A_m$ such that $A \subseteq A_1 \subseteq \cdots \subseteq A_m \subseteq B$ and cardinality of set difference between two adjacent sets are less than or equal to 2. Since equation (VI) holds for all sets with cardinality of set difference less than or equal to 2, we have

$$r_N(A) \leq r_N(A_1) \leq \cdots \leq r_N(A_m) \leq r_N(B).$$

Submodularity: suppose $A, B \subseteq [N]$, let $C = A \cap B$, if $|A \cup B - C| \leq 2$, i.e, cardinality of symmetric set difference is less than or equal to 2, there exists a set $\{i, j\}$ and $D, E \subseteq \{i, j\}$ such that $A = C \cup D$, $B = C \cup E$. We could let $\mathcal{A} = C$ and obtain the rank $r_{\{i,j\}|\mathcal{A}}(\mathcal{B}) = r_N(\mathcal{A} \cup \mathcal{B}) - r_N(\mathcal{A})$, $\mathcal{B} \subseteq \{i, j\}$. Since D, E as subsets of $\{i, j\}$ satisfy submodularity in the so called "contracted minor rank", we have

$$\begin{aligned} &r_{\{i,j\}|\mathcal{A}}(D \cup E) + r_{\{i,j\}|\mathcal{A}}(D \cap E) \\ &\quad \leq r_{\{i,j\}|\mathcal{A}}(D) + r_{\{i,j\}|\mathcal{A}}(E), \end{aligned}$$

i.e,

$$\begin{aligned} &r_N(D \cup E \cup C) - r_N(C) + r_N((D \cap E) \cup C) - r_N(C) \\ &\qquad \leq r_N(A) + r_N(B) - 2r_N(C) \end{aligned}$$

Due to $r_N(D \cup E \cup C) = r_N(A \cup B)$, $r_N((D \cap E) \cup C) = r_N(A \cap B)$, we get

$$r_N(A \cup B) + r_N(A \cap B) \leq r_N(A) + r_N(B).$$

Now suppose we have two subsets $A, B \subseteq [N]$, let $C = A \cap B$ and $|A \cup B - C| = m$, we would like to show that the cardinality of symmetric set difference increases by 1, it still obeys submodularity.

Without loss of generality, we assume that $B' = B \cup e$, where $e \notin A$ and $e \notin B$. So, we have $|A \cup B' - C| = m+1$. Then we have

$$\begin{aligned} & r_N(A \cup B') + r_N(A \cap B') \\ = \; & r_N(A \cup B \cup e) + r_N(A \cap (B \cup e)) \\ = \; & r_N(A \cup B \cup e) + r_N(A \cap B) \\ \leq \; & r_N(A \cup B \cup e) + r_N(A) + r_N(B) - r_N(A \cup B) \quad (15) \end{aligned}$$

We know that

$$r_N(B') = r_N(B \cup e) \leq r_N(B) + 1.$$

If $r_N(B') = r_N(B)$, we have

$$\begin{aligned} &r_N(A \cup B \cup e) + r_N(A) + r_N(B) - r_N(A \cup B) \\ &\quad = r_N(A) + r_N(B) = r_N(A) + r_N(B'). \end{aligned}$$

If $r_N(B') = r_N(B) + 1$, we have

$$\begin{aligned} &r_N(A \cup B \cup e) + r_N(A) + r_N(B) - r_N(A \cup B) \\ &\leq r_N(A \cup B) + 1 + r_N(A) + r_N(B) - r_N(A \cup B) \\ &\qquad = r_N(A) + r_N(B'). \end{aligned}$$

Therefore, we have

$$r_N(A \cup B') + r_N(A \cap B') \le r_N(A) + r_N(B')$$

holds for arbitrary subsets with symmetric set difference of $m+1$.

Satisfaction of the three conditions in Def. 2 indicates the vector is a valid rank for the matroid with ground set $[N]$. ∎

Next, we show that no rank can be expressed as a convex combination of some other ranks with non-zero coefficients.

Proof: [**Proof of Theorem 3**] Trivially, the all-zero vector cannot be a convex combination of other ranks.

To pursue a contradiction, we assume that there exists a convex combination $\mathbf{r}^i = \sum_{\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i} \alpha_j \mathbf{r}^j$ with $\sum_{\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i} \alpha_j = 1$ and $\mathbf{r}^j \neq \mathbf{r}^i, \forall \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i$. Note that every size 2 minor of $\mathbf{r}^i$ is also a valid rank function on a two-element set. We suppose a size 2 minor on $\{a,b\} \subseteq S$ is obtained by contracting $\mathcal{A} \subseteq S\backslash\{a,b\}$ and deleting $S\backslash(\{a,b\}\cup\mathcal{A})$.

Now we examine the rank of minor obtained from $\mathbf{r}^i$. For $\mathcal{B} \subseteq \{a,b\}$

$$\begin{aligned} r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) &= r^i(\mathcal{B}\cup\mathcal{A}) - r^i(\mathcal{A}) \\ &= \sum_{\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i} \alpha_j r^j(\mathcal{B}\cup\mathcal{A}) - \sum_{\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i} \alpha_j r^j(\mathcal{A}) \\ &= \sum_{\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i} \alpha_j (r^j(\mathcal{B}\cup\mathcal{A}) - r^j(\mathcal{A})). \\ &= \sum_{\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i} \alpha_j r^j_{\{a,b\}|\mathcal{A}}(\mathcal{B}). \end{aligned}$$

We see that every entry of $\mathbf{r}^i_{\{a,b\}|\mathcal{A}}$ is the same convex combination as $\mathbf{r}^j_{\{a,b\}|\mathcal{A}}$ of corresponding entries of ranks of minors obtained from $\mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i$.

First we let $\mathcal{B}$ be one-element subset of $\{a,b\}$ and examine $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B})$. Due to the cardinality constraints on matroid ranks, rank of all one-element subsets should be 0 or 1. For a fixed $\mathcal{B}$, we can partition the ranks of minors $R = \{\mathbf{r}^j, \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i\}$ into $R_{1,0}$ and $R_{1,1}$, where $R_{1,0}$ include those who have entry of 0 and $R_{1,1}$ include those who have entry of 1, at the coordinate corresponding to $\mathcal{B}$ in the minors. Similarly, the coefficients can be partitioned to θ_0 and θ_1 to match with $R_{1,0}$ and $R_{1,1}$. We still have $\sum_{k=1}^{|\theta_0|} \theta_{0,k} + \sum_{l=1}^{|\theta_1|} \theta_{1,l} = 1$ and $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = \sum_{k=1}^{|\theta_0|} \theta_{0,k} * 0 + \sum_{l=1}^{|\theta_1|} \theta_{1,l} * 1 = \sum_{l=1}^{|\theta_1|} \theta_{1,l}$. If $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 0$, we have $\sum_{l=1}^{|\theta_1|} \theta_{1,l} = 0$, which indicates $r^j_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 0, \forall \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i$. If $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 1$, $\sum_{l=1}^{|\theta_1|} \theta_{1,l} = 1$. Together with $\sum_{k=1}^{|\theta_0|} \theta_{0,i} + \sum_{l=1}^{|\theta_1|} \theta_{1,j} = 1$ we see that all ranks of minors obtained from the ranks involved in the combination have entry of 1 at coordinates mapped with a or b. So $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = r^j_{\{a,b\}|\mathcal{A}}(\mathcal{B}), \forall \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i, \mathcal{B} = a$ or b.

Now let $\mathcal{B}$ be $\{a,b\}$ and examine $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B})$. Due to cardinality constraints and the fact proved above, $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 1$ or 2. Similarly, we can partition R to $R_{2,1}$ and $R_{2,2}$ where $R_{2,1}$ include those who have entry of 1 and $R_{2,2}$ include those who have entry of 2, at the coordinate corresponding to $\mathcal{B}$ in the minors. Corresponding coefficients are partitioned to θ'_1 and θ'_2. We have $\sum_{k=1}^{|\theta'_1|} \theta'_{1,i} + \sum_{l=1}^{|\theta'_2|} \theta'_{2,j} = 1$ and $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = \sum_{k=1}^{|\theta'_1|} \theta'_{1,i} + 2\sum_{l=1}^{|\theta'_2|} \theta'_{2,j}$. Suppose $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 1$, we have $\theta'_2 = \emptyset$ which indicates $r^j_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 1$. If $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 2$, which makes θ'_1, and hence $R_{2,1}$ to be empty set and therefore $r^j_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = 2, \forall \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i$. So we have $r^i_{\{a,b\}|\mathcal{A}}(\mathcal{B}) = r^j_{\{a,b\}|\mathcal{A}}(\mathcal{B}), \forall \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i, \mathcal{B} = \{a,b\}$.

Together with Lemma 2 we see $\mathbf{r}^i = \mathbf{r}^j, \forall \mathbf{r}^j \in \mathcal{V}\backslash \mathbf{r}^i$, contradicted with the assumption. ∎

Finally, we give an alternate proof for the extreme rays relationship between Γ_N^{mat} and Γ_N.

Proof: [**Alternate Proof of Theorem 5**] Clearly, $\mathcal{T}_N^{\text{mat}} \subseteq \Gamma_N^{\text{mat}}$. For the other direction, we need to show that there does not exist an extreme ray of Γ_N^{mat} that lies outside of $\mathcal{T}_N^{\text{mat}}$, the conic hull of all matroidal extreme rays of Γ_N. Here we assume all extreme rays of Γ_N are scaled to their minimal integer representation. To pursue a contradiction, we assume that there exists an extreme ray $\mathbf{r}$ of Γ_N^{mat} which lies outside of $\mathcal{T}_N$, but still lies in Γ_N and is not an extreme ray of Γ_N.

Since all extreme rays of Γ_N^{mat} are ranks of matroids, $\mathbf{r}$ must be integer-valued and every size 2 minor obtained from every possible combination of deletion and contraction is also a valid rank vector of matroid. Note that $\mathbf{r}$ (or $\eta\mathbf{r}, \eta > 0$) lies outside of the conical hull of all matroidal extreme rays of Γ_N but still inside Γ_N, hence $\mathbf{r}$ can be expressed as a conical combination (or equivalently, $\mathbf{r}' = \epsilon\mathbf{r}, \epsilon > 0$ can be expressed as a convex combination) of some matroidal extreme rays and some (at least one) extreme rays that are not matroidal. Note that these extreme rays involved in the combination must be connected, otherwise, they can be expressed as sum of two other ranks and thus contradict with extremality.

Suppose

$$\mathbf{r}' = \epsilon\mathbf{r} = \sum_{i=1}^{m} \alpha_i \mathbf{r}_i^{\text{mat}} + \sum_{j=1}^{n} \beta_j \mathbf{r}_j^{\text{Shan}},$$

where $\alpha_i \in (0,1), i = 1,2,\dots m, \beta_j \in (0,1), j = 1,2,\dots n$ and $\sum_{i=1}^{m} \alpha_i + \sum_{j=1}^{n} \beta_j = 1$. Extreme rays $\mathbf{r}_i^{\text{mat}}$ are matroidal extreme rays and $\mathbf{r}_j^{\text{Shan}}$ are extreme rays of Γ_N that are not matroidal involved in the convex combination.

We pick one such $\mathbf{r}_j^{\text{Shan}}$ (since there exists at least one) and denote as $\mathbf{r}^{\text{Shan}}$. We know $\mathbf{r}^{\text{Shan}}$ is connected but not matroidal, therefore, there exists a way (mimic the way to get the minor of $\{a,b\}$ obtained by contracting $\mathcal{A} \subset \{1,2,\dots N\}\backslash\{a,b\}$ and deleting $\{1,2,\dots N\}\backslash(\{a,b\}\cup\mathcal{A})$) to obtain the corresponding vector $\mathbf{r}^{\text{Shann}}_{\{a,b\}|\mathcal{A}} = (r^{\text{Shann}}_{\{a,b\}|\mathcal{A}}(a), r^{\text{Shann}}_{\{a,b\}|\mathcal{A}}(b), r^{\text{Shann}}_{\{a,b\}|\mathcal{A}}(ab))$ which is not matroidal but is connected, since there exists dependence in $\mathbf{r}_j^{\text{Shan}}$.

Now we examine the rank of the minor obtained the same way from $\mathbf{r}'$. For $\mathcal{B} \subseteq \{a,b\}$

$$\begin{aligned} r'_{\{a.b|\mathcal{A}\}}(\mathcal{B}) &= r'(\mathcal{B}\cup\mathcal{A}) - r'(\mathcal{A}) \\ &= \sum_{i=1}^{m} \alpha_i (r_i^{\text{mat}}(\mathcal{B}\cup\mathcal{A}) - r_i^{\text{mat}}(\mathcal{A})) \\ &\quad + \sum_{j=1}^{n} \beta_j (r_j^{\text{Shan}}(\mathcal{B}\cup\mathcal{A}) - r_j^{\text{Shan}}(\mathcal{A})). \end{aligned}$$

We see that every entry of $\mathbf{r}'_{\{a.b|\mathcal{A}\}}$ is the same convex combination as $\mathbf{r}'$ of corresponding entries of ranks of minors obtained from $\mathbf{r}_i^{\text{mat}}, i = 1, 2, \dots m$ and $\mathbf{r}_j^{\text{Shan}}, j = 1, 2, \dots n$.

Since $\mathbf{r}^{\text{Shan}}$ is involved in the convex combination, the "minor" obtained here is not matroidal, since this is the way we originally selected the minor to take. Suppose $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(a) = 2$, and only $\mathbf{r}^{\text{Shan}}$ with coefficient β is involved in the convex combination.

Due to the cardinality constraints on matroid ranks, rank of all one-element subsets should be 0 or 1, so $r'_{\{a.b|\mathcal{A}\}}(a) = 0$ or ϵ. We can partition the ranks of minors $R = \{r^{\text{mat}}_{i,\{a,b|\mathcal{A}\}}, i = 1, 2, \dots m\}$ into $R_{a,0}$, and $R_{a,1}$ which include those "minors" who have entry of 0 and 1 respectively at the coordinate corresponding to a. Similarly, the coefficients can be partitioned to $\theta_{a,0}$ and $\theta_{a,1}$ to match with $R_{a,0}$ and $R_{a,1}$. We still have $\sum_{l=0}^{1}\sum_{k=1}^{|\theta_{\mathcal{B},l}|}\theta^k_{a,l,} + \beta = 1$ and $r'_{\{a.b|\mathcal{A}\}}(a) = \sum_{k=1}^{|\theta_{a,0}|}\theta^k_{a,0,} * 0 + \sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} * 1 + \beta = \sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} + 2\beta$. Clearly $r'_{\{a.b|\mathcal{A}\}}(a) \neq 0$ since $\beta > 0$. Therefore $r'_{\{a.b|\mathcal{A}\}}(a) = \sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} + 2\beta = \epsilon$.

Suppose $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(b) = r'_{\{a.b|\mathcal{A}\}}(b) = 0$, then $r^{\text{mat}}_{i,\{a,b|\mathcal{A}\}}(b) = 0$, and $r^{\text{mat}}_{i,\{a,b|\mathcal{A}\}}(ab) = r^{\text{mat}}_{i,\{a,b|\mathcal{A}\}}(a), i = 1, 2, \dots m$. Further, $r'_{\{a.b|\mathcal{A}\}}(ab) = \epsilon = r'_{\{a.b|\mathcal{A}\}}(a)$, which requires $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(ab) = 2 = r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(a)$. In this case, $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}} = (2, 0, 2) = 2 \cdot (1, 0, 1)$, contradicting with that $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}$ is not matroidal.

Suppose $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(b) = 1$,$r'_{\{a.b|\mathcal{A}\}}(b) = \epsilon = \sum_{l=1}^{|\theta_{b,1}|}\theta^l_{b,1} + \beta = \sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} + 2\beta$, we have $\sum_{l=1}^{|\theta_{b,1}|}\theta^l_{b,1} = \sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} + \beta$. Then $r'_{\{a.b|\mathcal{A}\}}(ab) = \sum_{l=1}^{|\theta_{ab,1}|}\theta^l_{ab,1} + 2\sum_{l=1}^{|\theta_{ab,2}|}\theta^l_{ab,2} + \beta \cdot r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(ab)$. First observe that $r'_{\{a.b|\mathcal{A}\}}(ab) > \epsilon$, since $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(ab) \geq r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(a) = 2$ and $R_{a,1} \subseteq R_{ab,1} \cup R_{ab,2}$. Further, $r'_{\{a.b|\mathcal{A}\}}(ab) \leq \sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} + \sum_{l=1}^{|\theta_{b,1}|}\theta^l_{b,1} + \beta \cdot r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(ab)$, where equality is obtained when $R_{ab,1} = \emptyset$. Due to the connectedness of $\mathbf{r}_j^{\text{Shan}}$, $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(ab) < r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(a) + r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(b) = 3$. Hence $r'_{\{a.b|\mathcal{A}\}}(ab) < 2\sum_{l=1}^{|\theta_{a,1}|}\theta^l_{a,1} + 3\beta = 2\epsilon - \beta < 2\epsilon$. Theorefore, the vector $(r_{\{a.b|\mathcal{A}\}}(a), r_{\{a.b|\mathcal{A}\}}(b), r_{\{a.b|\mathcal{A}\}}(ab) = \frac{1}{\epsilon} \cdot (r'_{\{a.b|\mathcal{A}\}}(a), r'_{\{a.b|\mathcal{A}\}}(b), r'_{\{a.b|\mathcal{A}\}}(ab)$ is not a valid two-element matroid rank. From theorem 2 we get that $\mathbf{r}$ is not a valid matroid rank, either. Contradiction.

Now, proceeding with the same argument in the previous three paragraphs, but with ranks $r^{\text{Shan}}_{\{a,b\}|\mathcal{A}}(a)$ even larger than 2, and with even more non-matroidal ranks involved in the convex combination, we observe that we will still have a contradiction stating that the originally supposed extremal matroid is in fact no longer a matroid.

Therefore, $\Gamma_N^{\text{mat}} \subseteq \mathcal{T}_N^{\text{mat}}$. ■

VII. Conclusion

This paper considers properties of inner bounds to the region of entropic vectors created from representable matroids. These inner bounds can be further used in multi-terminal network information theory to determine rate regions and associated linear codes. Some interesting properties of the matroid bounds were proven in this paper. The most significant result was that the extreme rays of binary representable matroid inner bound are a subset of extreme rays of matroid bound, which themselves are a subset of extreme rays of Shannon outer bound. In addition, this paper also showed that it suffices to check size 2 subsets to determine if an integer-valued vector is a valid matroid rank, and that matroid ranks are convex independent. Finally, it was noted that the properties of the bounds proven here enable computational methods for determining them with reduced complexity, the creation of the most efficient forms of which is a topic of ongoing investigation.

Acknowledgments

The authors gratefully acknowledge NSF support of this research through grants CCF-1016588 and CCF-1053702.

References

[1] F. Matúš. Infinitely Many Information Inequalities. In *IEEE International Symposium on Information Theory (ISIT)*, pages 41–44, June 2007.

[2] S. Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39:55–72, 1978.

[3] B. Hassibi, S. Shadbakht, and M. Thill. On optimal design of network codes. In *Information Theory and Applications Workshop (ITA)*, February 2010. (Conference Presentation).

[4] Congduan Li, J. Apte, J. M. Walsh, and S. Weber. A new computational approach for determining rate regions and optimal codes for coded networks. In *NetCod 2013*, pages 1 –6, Jun 2013.

[5] Congduan Li, J. M. Walsh, and S. Weber. Computational approaches for determining rate regions and codes using entropic vector bounds. In *50th Annual Allerton Conference on Communication, Control and Computing, 2012*, pages 1 –9, Oct 2012.

[6] Yoshitake Matsumoto, Sonoko Moriyama, Hiroshi Imai, and David Bremner. Matroid enumeration for incidence geometry. *Discrete and Computational Geometry*, 47(1):17–43, 2012.

[7] Dillon Mayhew, Mike Newman, Dominic Welsh, and Geoff Whittle. On the asymptotic proportion of connected matroids. *European Journal of Combinatorics*, 32(6):882–890, 2011.

[8] Dillon Mayhew and Gordon F. Royle. Matroids with nine elements. *Journal of Combinatorial Theory, Series B*, 98(2):415 – 431, 2008.

[9] H. Q. Nguyen. Semimodular functions and combinatorial geometries. *Transactions of the American mathematical society*, 238:355 – 383, Apr. 1978.

[10] J. G. Oxley. *Matroid Theory*. Oxford University, 2011.

[11] W. T. Tutte. A homotopy theorem for matroids. *Trans. Amer. Math. Soc.*, 88:144–174, 1958.

[12] S. Weber, C. Li, and J. M. Walsh. Rate region for a class of delay mitigating codes and p2p networks. *46th Annual Conference on Information Sciences and Systems*, March 2012.

[13] R. W. Yeung. Multilevel diversity coding with distortion. *IEEE Trans. Information Theory*, 41:412–422, 1995.

[14] R. W. Yeung. *Information Theory and Network Coding*. Springer, 2008.

[15] R. W. Yeung and Z. Zhang. Distributed source coding for satellite communications. *IEEE Trans. on Information Theory*, 45(4):1111–1120, 1999.