

## MIT Open Access Articles

*On the representability of integer polymatroids:  
Applications in linear code construction*

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

**Citation:** Salimi, Amir, Muriel Medard, and Shuguang Cui. "On the Representability of Integer Polymatroids: Applications in Linear Code Construction." 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton), 29 September - October 2, 2015, Monticello, Illinois, IEEE, 2016.

**As Published:** <http://dx.doi.org/10.1109/ALLERTON.2015.7447046>

**Publisher:** Institute of Electrical and Electronics Engineers (IEEE)

**Persistent URL:** <http://hdl.handle.net/1721.1/114894>

**Version:** Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

**Terms of use:** Creative Commons Attribution-Noncommercial-Share Alike



# On the Representability of Integer Polymatroids: Applications in Linear Code Construction

Amir Salimi, Muriel Médard, and Shuguang Cui

**Abstract**—It has been shown that there is a duality between the linear network coding solution and the entropic vectors induced by collection of subspaces in a vector space over a finite field (dubbed linearly constructed entropic vectors). The region of all linearly constructed vectors, coincides with the set of all representable polymatroids. For any integer polymatroid, there is an associated matroid, which uniquely identifies the polymatroid. We conjecture that the representability of the underlying matroid is a sufficient condition for integer polymatroids to be linearly representable. We prove that the conjecture holds for representation over real numbers. Furthermore, we show that any real-valued submodular function (such as Shannon entropy) can be approximated (arbitrarily close) by an integer polymatroid.

## I. INTRODUCTION

Let  $f : 2^{[n]} \rightarrow \mathbb{R}$  be a real valued set function, where  $[n] = \{1, 2, \dots, n\}$ . The function  $f$  is submodular if for every  $S, T \subseteq [n]$

$$f(S) + f(T) \geq f(S \cup T) + f(S \cap T), \quad (1)$$

Submodularity has a rich combinatorial structure. Submodular functions play a key role in many combinatorial optimization problems, and have many applications in economics and engineering. In information theory, many problems are directly related to submodular function analysis, since Shannon entropy of collection of random variables is known to be a submodular function. Specifically, for a collection of jointly distributed discrete random variables  $\{X_1, X_2, \dots, X_n\}$ , the joint entropy of a collection of random variables  $X_S := (X_i, i \in [n])$ , denoted by  $H(X_S, S \subseteq [n])$ , is submodular. For a particular joint distribution of  $(X_1, \dots, X_n)$ , the entropy of all subsets of these random variables can be expressed by a  $2^n - 1$  dimensional vector  $(H(X_S), S \subseteq [n])$ . The region of all such vectors known as the *entropy region* and denoted by  $\Gamma_n^*$ . It has been shown that the closure of this region  $\bar{\Gamma}^*$  is convex; however, characterization of this region for  $n > 3$  is one of the well-known open problems in network information theory [1], which is closely related to the capacity region of the general network coding problem.

This research was supported in part by DoD with grant HDTRA1-13-1-0029, by NSF with grants ECCS-1508051, CNS-1343155, ECCS-1305979, and CNS-1265227, by grant NSFC-61328102, and by the Air Force Office of Scientific Research (AFOSR) under award No. FA9550-14-1-043. A. Salimi, S. Cui are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA (email: {salimi,cui}@tamu.edu). S. Cui is also with King Abdulaziz University in Saudi Arabia as a Distinguished Adjunct Professor. M. Médard is with the Research Laboratory for Electronics (RLE), Massachusetts Institute of Technology, Room 36-512, 77 Massachusetts Avenue, Cambridge, MA 02139 USA (e-mail: medard@mit.edu).

Many network coding capacity regions and entropy region can be upper-bounded by exploiting just the submodularity of entropy function. These upper bounds are often termed as *polymatroidal upper bounds* [1]. It has been shown that these outer bounds are not tight when  $n > 3$ . Many techniques exist for constructing the corresponding lower bounds. One of the most important classes, which we term as *linear construction of entropy vector* or simply *linear network coding solution*, relies on building a subspace of a vector space over a finite field, and we denote this region by  $\Gamma_n^L$ . However, it has been shown that linear solutions are not sufficient to characterize the entire entropy region or achieve the network coding capacity. When  $n = 4$ , the region  $\Gamma_n^L$  can be characterized by the *Ingleton inequality* and Shannon inequalities [9], [10]. The exact characterization of this region for five random variables, is given by a set of inequalities known as DFZ, together with Shannon and Ingleton inequalities [7]. In general, exact characterization of  $\Gamma_n^L$  is equivalent to the space of all *linearly representable integer polymatroids* [11].

From a combinatorial point of view, integer polymatroids are closely related to matroids. In this paper, we ask the following question: Given an integer polymatroid, is it possible to infer its representability from that of a particular matroid? We conjecture that this is possible and in fact, we prove the statement for representation over  $\mathbb{R}$ . If the conjecture is true, the results concerning the representation of matroids, would be sufficient to analyze the representability of integer polymatroids. A necessary and sufficient condition for representability of integer polymatroids is given in Section III. Furthermore, we show that for any  $\epsilon > 0$ , any submodular function  $f$ , can be approximated by a rational-valued submodular function  $\hat{f}_Q$  such that for every set  $S$ , we have  $|f(S) - \hat{f}_Q(S)| < \epsilon$ ; we refer to this as  $\epsilon$ -approximation. Since any rational-valued submodular function can be considered as a properly scaled integer polymatroid, this approximation suggests that any submodular function can be approximated by an integer polymatroid. In Sections IV and V, we discuss the implication of these results in some network information theory problems.

## II. PRELIMINARIES

For a given submodular function  $f$ , we define the following distance between two arbitrary subsets of the ground set,  $S, T \subseteq E$

$$D_f(S, T) = f(S) + f(T) - f(T \cup S) - f(T \cap S). \quad (2)$$

By definition of submodularity,  $D_f(S, T) \geq 0$  for any submodular function and  $D_f(S, T) \leq 0$  for any supermodular function. This distance is not an interesting object by itself, since  $D_f(S, T) = 0$  for every  $S \subseteq T$  (or  $T \subseteq S$ ). However, if we take out these special subsets, the minimum value that  $D_f(S, T)$  can take, becomes informative and is defined as

$$\Delta_f = \min_{S \subseteq E} \min_{i, j \in E \setminus S} |D_f(S + i, S + j)| \quad (3)$$

**Remark 1.** It is easy to verify some of the properties of  $\Delta_f$ . For example, if  $f$  and  $g$  are both submodular functions, we have

$$\Delta_{f+g} \geq \Delta_f + \Delta_g, \quad (4)$$

and when  $f$  and  $g$  are both supermodular functions, we have

$$\Delta_{f+g} \leq \Delta_f + \Delta_g. \quad (5)$$

This particular property defines a special class of submodular functions as follows.

**Definition 1.** A submodular (supermodular) function  $f$ , defined on the ground set  $E$ , is called strictly submodular (supermodular) if  $\Delta_f > 0$ .

In the following we show an example of a strictly submodular function.

**Example 1.** The set function  $\log(1 + |S|)$  is strictly submodular. One way to prove this is by contradiction. Assume that it is not strictly submodular and, therefore, there exist  $T, S \neq \emptyset$  and  $T \not\subseteq S, S \not\subseteq T$  such that

$$\begin{aligned} 0 &= f(S) + f(T) - f(S \cup T) - f(S \cap T) \\ &= \log(1 + |S|) + \log(1 + |T|) - \log(1 + |S \cup T|) \\ &\quad - \log(1 + |S \cap T|) \\ &= \log(1 + |S||T| + |S| + |T|) \\ &\quad - \log(1 + |S \cup T||S \cap T| + |S \cup T| + |S \cap T|). \end{aligned}$$

Since  $|S| + |T| = |S \cup T| + |S \cap T|$ , this implies that

$$|S \cup T||S \cap T| = |S||T| \quad (6)$$

Assume  $|S| = |S \cup T| - x$  and  $|T| = |S \cap T| + x$ . Therefore, we have

$$\begin{aligned} |S||T| &= (|S \cup T| - x)(|S \cap T| + x) \\ &= |S \cap T||S \cup T| + x|S \cup T| - x|S \cap T| - x^2 \end{aligned}$$

which implies either  $x = 0$  or  $x = |S \cup T| - |S \cap T|$ . The former condition on  $x$  implies that  $T \subseteq S$  and the latter implies that  $S \subseteq T$ , which contradicts our assumption.

#### A. Integer polymatroids

A Polymatroid  $P$  is a pair  $(E, f)$ , where  $E$  is a non-empty ground set and  $f$  is a set function satisfying the following conditions:

- $f$  is submodular:  $f(S) + f(T) \geq f(S \cap T) + f(S \cup T)$ , for  $S, T \subseteq E$
- Nondecreasing:  $f(S) \geq f(T), S \supseteq T$

- Normalized:  $f(\emptyset) = 0$

When  $f$  is an integer-valued set function,  $P = (E, f)$  is called *integer polymatroid*.

In a way akin to representable matroids, we can define the representability of integer polymatroids as follows:

**Definition 2.** An integer polymatroid  $(E, f)$  on the ground set  $E$  is representable, if there exists a collection of subspaces  $V_e, e \in E$ , such that for every  $S \subseteq E$ , we have  $\text{rank}(\cup_{e \in S} V_e) = f(S)$ .

### III. MAIN RESULTS

#### A. Representability of Integer Polymatroids

Although integer polymatroids are interesting combinatorial objects by nature, they have a matroid structure. Moreover, it has been shown by Helgason [2], that every integer polymatroid can be constructed by a matroid. Therefore, all problems in integer polymatroids are matroid problems. More specifically, let  $f$  be an integer-valued, nondecreasing submodular set function on  $E$ , with  $f(\emptyset) = 0$ . For each element of ground set  $e \in E$ , we assign a set  $X_e$  with the size of  $f(\{e\})$ . Now the ground set for the new matroid that we construct will be  $X = \bigsqcup_{e \in S} X_e$ , where  $\bigsqcup$  denotes the disjoint union operation.

**Theorem 1.** Helgason [2]:  $\mathcal{M} = (X, r)$  is a matroid, where the rank function of a matroid is given by

$$r(U) = \min_{T \subseteq S} (|U \setminus \bigcup_{e \in T} X_e| + f(T)). \quad \forall U \subseteq X \quad (7)$$

It is easy to check that the rank function of the original integer polymatroid has not been changed. Namely,

$$f(T) = r(\bigsqcup_{e \in T} X_e). \quad (8)$$

The interesting observation here is that the integer polymatroid is defined on the ground set  $E$ , where the rank function of the matroid  $r(\cdot)$  is defined on a larger ground set than  $E$ , namely  $X = \bigsqcup_{e \in E} X_e$  with cardinality  $|X| = \sum_{e \in E} f(e)$ . The construction of an integer polymatroid from matroids is not unique. In the next section, we explain the notion of extending the ground set of a polymatroid and how using this extension, it is possible to construct a matroid.

#### B. Extending Integer Polymatroids

Lovász [6], showed that it is possible to extend the ground set of an integer polymatroid by “adding new element  $e'$  to the element  $e$  in the ground set”<sup>1</sup>. Specifically, “adding  $e'$  to  $e \in E$ ” means constructing a new integer polymatroid  $(E \cup \{e'\}, f)$ , where the value of  $f$  remains the same on the subsets of  $E$  and

$$f(T + e') = \begin{cases} f(T), & \text{if } f(T + e) = f(T) \\ f(T) + 1, & \text{if } f(T + e) > f(T). \end{cases} \quad (9)$$

<sup>1</sup>Lovász [6], gave this a geometric interpretation and called “adding a point  $x$  on an element of integer polymatroid  $y$  in general position”. Here we adopt his notation and for simplicity we refer to this as “adding  $x$  on an element  $y$  in the ground set of integer polymatroid”.

Similarly, we can continue adding elements and eventually construct an integer polymatroid  $(E \cup X, f)$ , where  $X = \bigcup_{e \in S} X_e$  and elements of  $X_e$  have been added to element  $e \in E$ . The following theorem, gives the explicit construction of a matroid.

**Theorem 2.** *Lovász [6]: Let  $(E \cup X, f)$  be the extended polymatroid defined above. Then  $\mathcal{M} = (X, r)$  is a matroid where  $r(U) = f(U)$ , for all  $U \subseteq E$ . Moreover,*

$$r(U) = \min_{T \in E} (|U \setminus \bigcup_{e \in T} X_e| + f(T)), \quad \forall U \subseteq X \quad (10)$$

which is identical to (7).

Through the paper, we will refer to this special construction of matroids as *expanding-construction*.

### C. Representation of Integer Polymatroid

The following theorem gives the necessary and sufficient condition for the representability of an integer polymatroid over real numbers  $\mathbb{R}$ .

**Theorem 3.** *An integer polymatroid is representable over  $\mathbb{R}$ , if and only if the underlying matroid using the expanding-construction, is representable over  $\mathbb{R}$ .*

*Proof.* Assume that  $(E, f)$  is an integer polymatroid and its associated matroid using the described expanding construction is  $(\bigcup_{e \in E} X_e, r)$ . One direction trivially holds: if the underlying matroid  $(\bigcup_{e \in E} X_e, r)$  is representable, one can take the subspace generated by the span of the vectors associated with each  $X_e$  and therefore, by definition, the integer matroid is, indeed, representable.

To verify the other direction, we assume that there exist a collection of vector spaces  $V_e$  for every  $e \in E$  and the goal is to show that the matroid derived using expanding-construction is representable. Assume that the subspaces for the integer polymatroid are given as  $S = \{S_1, S_2, \dots, S_{|E|}\}$  and define  $r_i := \text{rank}(S_i)$ .

The outline of the proof is as follows: Similarly to the expanding-construction, we start with the ground set  $S$ , and at each step, we “add a vector to subspace  $S_i \in S$ ”, where the definition will be made precise later. We continue adding elements and, for each  $S_i \in S$ , we add  $r_i$  vectors, which are denoted by  $\mathcal{V}_i = \{V_1^{(i)}, \dots, V_{r_i}^{(i)}\}$ . Eventually the ground set will be  $S \cup \bigcup_{i \in [|E|]} \mathcal{V}_i$  and we show that the rank function of any collection of these vectors satisfies (7). Therefore, we conclude that the vectors  $\bigcup_{i \in [|E|]} \mathcal{V}_i$  are a linear representation of the expanding-construction matroid.

In order to complete the proof, we need to explain how we add vector  $V_j^{(i)}$  to subspace  $S_i$ . Assume that we want to add a vector  $V_j^{(i)}$  for  $j \leq r_i$  to  $S_i$ . First, we define the following set

$$\mathcal{T}_{i,j}^* := S \cup \mathcal{V}_1 \cup \dots \cup \mathcal{V}_{i-1} \cup \{V_1^{(i)} \dots V_{j-1}^{(i)}\}. \quad (11)$$

It is easy to verify that  $|\mathcal{T}_{i,j}^*| = |E| + \sum_{k=1}^{i-1} r_k + (j-1)$ . We define

$$\mathcal{T}_{i,j} = \{T | T \subseteq \mathcal{T}_{i,j}^*, \text{rank}(T \cup S_i) > \text{rank}(T)\}. \quad (12)$$

To accomplish the construction of the linear matroid, we pick a vector  $V_j^{(i)}$  for  $j \leq r_i$  such that:

$$V_j^{(i)} \in S_i \setminus \bigcup_{T \in \mathcal{T}_{i,j}} \text{span}(T). \quad (13)$$

In order to choose the vector  $V_j^{(i)}$ , we need to make sure that  $S_i \setminus \bigcup_{T \in \mathcal{T}_{i,j}} \text{span}(T) \neq \emptyset$ .

**Claim 1.** *For all  $i \in [|E|]$ , we have  $S_i \setminus \bigcup_{T \in \mathcal{T}_{i,j}} \text{span}(T) \neq \emptyset$ .*

*Proof.* First, note that  $S_i \not\subseteq \text{span}(T)$  for all  $T \in \mathcal{T}_{i,j}$ ; otherwise  $\text{rank}(T \cup S_i) = \text{rank}(T)$ . This implies that  $T \notin \mathcal{T}_{i,j}$ ; however, this contradicts our assumption that we started with  $T \in \mathcal{T}_{i,j}$ . The only possibility is  $S_i \supset \bigcup_{T \in \mathcal{T}_{i,j}} \text{span}(T)$ . However, since we assumed that all subspaces are in  $\mathbb{R}$ , we know that it is not possible to write a subspace in  $\mathbb{R}$  as countable union of subspaces that do not include it.  $\square$

With this choice of vectors, once we add a new vector  $V_j^{(i)}$  to the ground set of the integer polymatroid, since the chosen vector is not in the  $\bigcup_{T \in \mathcal{T}_{i,j}} \text{span}(T)$ , we have

$$\text{rank}(T + V_j^{(i)}) = \begin{cases} \text{rank}(T), & \text{if } T \notin \mathcal{T}_{i,j} \\ \text{rank}(T) + 1, & \text{if } T \in \mathcal{T}_{i,j}. \end{cases} \quad (14)$$

Without loss of generality, we continue this construction in  $|E|$  steps, starting from  $S_1$  up to  $S_{|E|}$ , and at each step  $i$ , we add  $r_i$  new vectors to the ground set. On the other hand, the rank function given in (14) is identical to (9), and therefore, this proves that the collection of vectors  $\mathcal{V} = \bigcup_{i=1}^{|E|} \mathcal{V}_i$  is a vector matroid, isomorphic to the matroid that we obtain from an expanding-construction; and this completes the proof.  $\square$

This proof cannot be directly generalized to finite fields since we used a unique property of the vector spaces in  $\mathbb{R}$ . Namely, a vector space over  $\mathbb{R}$  cannot be decomposed into a countable union of proper subspaces. However, we posit the following conjecture, suggested by our results,

**Conjecture 1.** *The integer polymatroid is representable, if and only if the underlying matroid using the expanding-construction, is representable.*

### D. Approximation of Submodular Function With Rank Function of a Matroid

Recall that the rank function of an integer polymatroid is submodular; Therefore, it might seem redundant to approximate a submodular function with another submodular function. However, as we discussed in the previous sections, any scaled integer polymatroids can be constructed by matroids. Observe that when a submodular function takes rational values, it can be considered as an integer-valued submodular function with proper scaling, which is the lowest common denominator of all the function values. On the other hand, when the submodular function takes real values, this construction is impossible. However, in this case, we can approximate any submodular function (with proper scaling) by a matroid. This approximation is not only just of mathematical interest, but also useful in certain information theoretic problems.

**Theorem 4.** Suppose that  $f : 2^E \rightarrow \mathbb{R}$  is a real-valued submodular function over the ground set  $E$ . For every  $\epsilon > 0$ , there exist a polymatroid  $(E, f_Q)$  where  $f_Q : 2^E \rightarrow \mathbb{Q}$ , satisfying

$$0 < f(T) - f_Q(T) < \epsilon \quad (15)$$

for all  $T \subseteq E$ .

*Proof.* We consider two cases; For the first case, we assume that the function is strictly submodular ( $\Delta_f > 0$ ). For the second case, we argue that, when  $\Delta_f = 0$ , we can construct a strictly submodular function  $\tilde{f}$ , which is properly close to the original function  $f$ , namely  $f(T) - \tilde{f}(T) \leq \epsilon$ , for any  $T \subseteq E$ .

**Case 1:** We consider that  $f(\cdot)$  is strictly submodular, namely  $\Delta_f > 0$ , and define  $\epsilon^* := \min(\epsilon, \frac{\Delta_f}{2})$ . Then we are guaranteed to find a rational number  $f_Q(T)$  such that  $f_Q(T) \in [f(T) - \epsilon^*, f(T)]$ . Assume

$$f(T) - \epsilon^* \leq f_Q(T) = f(T) - \epsilon_T \leq f(T). \quad (16)$$

**Lemma 1.** The set function  $f_Q$  defined on the ground set  $E$  is submodular.

*Proof.* First, observe that, by our assumption  $\Delta_f > 0$  and  $\epsilon_T \leq \epsilon^*$  for every  $T \subseteq E$ , we have

$$\begin{aligned} \Delta_{f_Q} &= \min_{S \subseteq E} \min_{i, j \in E \setminus S} f_Q(S+i) + f_Q(S+j) \\ &\quad - f_Q(S) - f_Q(S+i+j) \\ &\geq \min_{S \subseteq E} \min_{i, j \in E \setminus S} f(S+i) + f(S+j) \\ &\quad - f(S) - f(S+i+j) \\ &\quad + \min_{S \subseteq E} \min_{i, j \in E \setminus S} \epsilon_{S+i} + \epsilon_{S+j} - \epsilon_S - \epsilon_{S+i+j} \\ &\stackrel{a}{=} \Delta_f + \epsilon_{S^*+i^*} + \epsilon_{S^*+j^*} - \epsilon_{S^*} - \epsilon_{S^*+i^*+j^*} \\ &\geq \Delta_f - \epsilon_{S^*} - \epsilon_{S^*+i^*+j^*} \\ &\geq \Delta_f - 2\frac{\Delta_f}{2} \\ &\geq 0 \end{aligned}$$

where  $S^*, i^*$  and  $j^*$  in (a) are the optimal solutions for the second minimization.  $\square$

**Case 2:** Consider that  $\Delta_f = 0$ ; then we can construct a strictly submodular function as follows

$$\tilde{f}(T) = f(T) - \gamma g(T), \quad (17)$$

where  $\gamma$  is small enough and  $g(T)$  is a strictly supermodular function. We have the following two facts.

**Fact 1.** The set function  $\tilde{f}(T)$  defined over ground set  $E$  is strictly submodular.

**Fact 2.** We have  $\Delta_{\tilde{f}} \geq \Delta_f + \gamma \Delta_g = \gamma \Delta_g$ .

Both are the immediate consequence of (4). We can choose  $\gamma$  to be arbitrary small, such that  $\epsilon^* = \frac{\gamma \Delta_g}{2} < \epsilon$ . Now with this choice of  $\tilde{f}$ , we have a strictly submodular function and similarly to the previous case and (16), with  $\tilde{f}(\cdot)$  and  $\epsilon^*$ , we are guaranteed to find rational-valued submodular function,

which is an  $\epsilon$ -approximation of  $f$ . This completes the proof.  $\square$

Similarly we can approximate any submodular function from above.

**Corollary 2.** Suppose that  $f : 2^E \rightarrow \mathbb{R}$  is a real-valued submodular function over the ground set  $E$ . For every  $\epsilon > 0$ , there exists a polymatroid  $(E, f_Q)$  where  $f_Q : 2^E \rightarrow \mathbb{Q}$ , satisfying

$$0 < f_Q(T) - f(T) < \epsilon \quad (18)$$

for all  $T \subseteq E$ .

*Proof.* The proof is similar to Theorem 4, except that we need  $g(T)$  to be a non-negative strictly submodular function.  $\square$

#### IV. IMPLICATION IN INFORMATION THEORY: FRACTIONAL NETWORK CODING SOLUTION

We consider a network with the underlying topology as a capacitated directed acyclic graph (DAG)  $((\mathcal{V}, \mathcal{A}), (C_a : a \in \mathcal{A}))$ . Here,  $\mathcal{V}$  and  $\mathcal{A}$  are the node and the arc sets of the graph with unit edge capacities. A set of distinct nodes  $S \subset \mathcal{V}$  called source nodes, which have the access to a subset of message set  $\mathcal{W} = \{w_1, \dots, w_m\}$ . There is also, a distinct subset of nodes  $\mathcal{T} \subset \mathcal{V}$  called sink nodes. Associated with each sink node there is a subset of message set  $\mathcal{W}$  as demand.

We assume that a vector of  $k_i$  symbols of message  $w_i$  for every  $i \in [m]$  at a source node are encoded and a code  $(n, \{x_a : a \in \mathcal{A}\})$  with block length  $n$  is transmitted over the arc  $a$ .

**Definition 3.** A network has  $(k_1, \dots, k_m, n)$  fractional linear solution if there exists a set of linear encoding and decoding operations at each node of the network and decoders at sink nodes, such that each sink node can perfectly decode its demanded messages.

When  $k = n = 1$ , the linear network coding solution is called a scalar-linear solution. It has been shown that every scalar linear solvable network is a matroidal network. For the special case where  $k = n$ , the solution is called a vector linear solution. From the definition above, the following lemma is immediate [3].

**Lemma 3.** If a network has a  $(k_1, \dots, k_m, n)$  fractional network coding solution over  $\Sigma$ , with independent messages uniformly distributed over  $\Sigma$ , the following hold:

- 1) For any collection of source messages  $H(\cup_{i \in I} w_i) = \sum_{i \in I} k_i$ , where  $I \subseteq [m]$ .
- 2)  $H(X_a) \leq n$  for every  $a \in \mathcal{A}$
- 3)  $H(\cup_{a \in In(v)} X_a) = H(\cup_{a \in In(v)} X_a, \cup_{a \in Out(v)} X_a)$

In the work by Dougherty et. al. [3], it has been shown that, if the network has a scalar linear solution over finite field  $\Sigma$ , with messages  $w_1, \dots, w_m$  and the links that carry the symbols  $\{x_a : a \in \mathcal{A}\}$ , finding a scalar linear solution is equivalent to finding a mapping  $T : \mathcal{W} \cup_{a \in \mathcal{A}} X_a \rightarrow E$  where  $E$  is the ground set of a representable matroid  $\mathcal{M} =$

$(E, r)$ , such that the three conditions in Lemma 3 are satisfied with  $H(\cdot) = r(\cdot)$ . The converse was established by Médard and Kim [8]. Similarly, we can have the following result for fractional linear solutions.

**Lemma 4.** *Assume that the network has a  $(k_1, \dots, k_m, n)$  fractional linear solution over finite field  $\Sigma$ , with messages  $w_1, \dots, w_m$  and the links that carry the symbols  $\{x_a : a \in \mathcal{A}\}$ . Then finding a fractional linear solution is equivalent to finding a mapping  $T : \mathcal{W} \cup_{a \in \mathcal{A}} X_a \rightarrow E$ , where  $E$  is the ground set of a representable integer polymatroid  $(E, f)$ , such that the three conditions in Lemma 3 are satisfied with  $H(\cdot) = f(\cdot)$ .*

The proof is similar to the proof of Lemma 3. A similar statement has been proved in (Theorem. 3, [4]), where they introduced the notion of *discrete polymatroidal network*, and showed that the network has a fractional linear solution if and only if it is discrete polymatroidal with respect to a representable discrete polymatroid.

#### V. IMPLICATION IN INFORMATION THEORY: CONSTRUCTING ENTROPIC VECTORS

Assume that we are given an integer vector (or rational <sup>2</sup>) in  $\Gamma_n$ . Naturally, this vector defines an integer polymatroid since entropy is a submodular function. Therefore, if it is representable over some finite field  $\mathbb{F}$ , we can conclude that the vector is indeed entropic and it can be constructed using linear mappings. The main problem here is that checking whether an integer polymatroid is representable, is not an easy task. However, if our conjecture is true, we can construct the associated expanded-matroid and check its representability. Therefore, one can use the extensive literature on representability of matroids. Moreover, if we conclude that the underlying matroid is not representable, we can claim that nonlinear transformation (or nonlinear code in the case of network coding) is inevitable.

Furthermore, if the given vector is not integral (or rational), then using Theorem 4, we are guaranteed to find an integer polymatroid, which is arbitrarily close to the desired vector. We should then be able to study the approximated integer polymatroid to see whether it is representable or not.

#### VI. CONCLUSION

In this paper, we studied the representability of polymatroids. We showed that the representability of an integer polymatroid is a necessary and sufficient condition for the representability of the underlying expanding-construction matroid over reals. Moreover, we showed that it is always possible to approximate a polymatroid with an integer polymatroid.

#### ACKNOWLEDGEMENT

We would like to acknowledge Profs. Tie Liu and Michel Goemans for fruitful discussions, and Ali Makhdoumi and Ahmad Beirami for their comments on the results.

<sup>2</sup>A rational vector can be transformed to an integer vector with a proper scaling.

#### REFERENCES

- [1] R. W. Yeung, *Information Theory and Network Coding*. Springer, 2008.
- [2] T. Helgason, "Aspects of the theory of hypermatroids", *Hypergraph Seminar*, Springer Lecture Notes 411, Springer, Berlin, 191-214.
- [3] R. Dougherty, C. Freiling, and K. Zeger, "Matroids, networks, and non-Shannon information inequalities", *IEEE Trans. Inf. Theory*, vol. 53, no. 6, Jun. 2007.
- [4] V. T. Muralidharan and B. S. Rajan, "Linear Network Coding, Linear index coding and representable discrete polymatroids", Available on ArXiv at <http://arxiv.org/abs/1306.1157>.
- [5] M. Médard, M. Effros, T. Ho and D. R. Karger "On coding for non-multicast networks", Proc. 41st Annu. Allerton Conf. Communication, Control, and Computing, Monticello, IL, Oct. 2003.
- [6] L. Lovász, "Flats in matroids and geometric graphs", in *Combinatorial Surveys, Proc. 6th British Comb. Conf.*, Academic Press (1977), 45-86.
- [7] R. Dougherty, C. Freiling, and K. Zeger, "Linear rank inequalities on five or more variables", arXiv cs.IT/0910.0284v3, 2009.
- [8] A. Kim, M. Médard, "Scalar-linear solvability of matroidal networks associated with representable matroids", in *Proc. Int. Symp. Turbo Codes and Iterative Information Processing*, Brest, Sept. 2010, pp. 452-456
- [9] D. Hammer, A.E. Romashchenko, A. Shen, and N.K. Vereshchagin, "Inequalities for Shannon entropy and Kolmogorov complexity", *Journal of Computer and Systems Sciences*, vol. 60, pp. 442-464, 2000.
- [10] A. W. Ingleton, "Representation of matroids", in *Combinatorial Mathematics and its Applications*, D. J. A. Welsh, ed., pp. 149-167, Academic Press, London, 1971.
- [11] Chan, Terence, Alex Grant, and Doris Pflger. "Truncation technique for characterizing linear polymatroids." *IEEE Trans. Inf. Theory* vol. 57, no. 10, Oct. 2011, pp. 6364-6378.