

# Constrained Linear Representability of Polymatroids and Algorithms for Computing Achievability Proofs in Network Coding

Jayant Apte, *Member, IEEE*, John MacLaren Walsh, *Member, IEEE*

## Abstract

The constrained linear representability problem (CLRP) for polymatroids determines whether there exists a polymatroid that is linear over a specified field while satisfying a collection of constraints on the rank function. Using a computer to test whether a certain rate vector is achievable with vector linear network codes for a multi-source network coding instance and whether there exists a multi-linear secret sharing scheme achieving a specified information ratio for a given secret sharing instance are shown to be special cases of CLRP. Methods for solving CLRP built from group theoretic techniques for combinatorial generation are developed and described. These techniques form the core of an information theoretic achievability prover, an implementation accompanies the article, and several computational experiments with interesting instances of network coding and secret sharing demonstrating the utility of the method are provided.

## Index Terms

network coding, secret sharing, polymatroids, entropy function, computer assisted achievability proofs

## I. INTRODUCTION

For many important multiterminal information theory problems, including those arising in network coding, distributed storage, and secret sharing, using a computer to perform an arbitrary achievability proof requires one to know an algorithm to determine if there exists an almost entropic polymatroid satisfying certain constraints on its rank function. Finding such an algorithm is a fundamental open problem in information theory, also known as the problem of characterization of the closure of the region of entropic vectors ( $\overline{\Gamma}_N^*$ ). We consider a special case of this very difficult problem, which we call the Constrained Linear Representability Problem (CLRP) for polymatroids. We show that the ability to solve CLRP can automate the achievability proofs that one encounters while determining the performance of linear codes in multi-source multi-sink network coding over directed acyclic hypergraphs and in secret sharing and while proving new linear rank inequalities.

Traditionally, the achievability constructions in proofs for these problems are performed manually, which makes them tedious and time consuming. A computer program to solve CLRP, at least for small and moderate instances, enables one, in turn, to pursue a computational agenda for approaching problems like network coding and secret sharing, which have proven difficult to solve in general. This involves solving small instances of these problems to build large and exhaustive databases of solved instances which can then be analyzed to find patterns and structure that allow one to make much more general statements about these problems [12], [15], [16]. All of these tasks would be impossible without the use of a computer due to sheer number of man hours required.

This article develops and describes a method for solving constrained linear representability problems built from group theoretic techniques for combinatorial generation. More precisely, in section II, after reviewing the definition of the region of entropic vectors and its linear polymatroid inner bound, we define two variants of CLRP, one existential and one enumerative. Then, Section III shows in detail how the problems of calculating achievability proofs for fundamental limits for network coding rate regions and secret sharing can be viewed as instances of these CLRPs. Section IV then defines key concepts

Support under National Science Foundation awards CCF-1016588 and CCF-1421828 is gratefully acknowledged. Jayant Apte and John MacLaren Walsh are with the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA, USA (email: jsa46@drexel.edu, and jwalsh@coe.drexel.edu). Preliminary ideas related to this work were presented at ISIT 2014 [3].

and terminology which enable techniques developed for combinatorial generation to be applied to CLRP, explaining along the way key decisions enabling CLRP to be solved in an efficient manner that can exploit problem symmetry and handle isomorphism. Building upon these ideas, section V presents the developed algorithm for solving CLRP, which is also implemented as a GAP package the Information Theoretic Achievability Prover– ITAP, the first of its kind, accompanying the article. Finally, Section VI describes several quantities playing a key role in the complexity of the developed method, then provides a series of examples of achievability problems solved with ITAP.

## II. ENTROPY, POLYMATROIDS, AND CONSTRAINED LINEAR REPRESENTABILITY PROBLEMS

In this section, we introduce basic terminology and review several key existential problems related to the region of entropic vectors in §II-A. We also state the existential and enumerative variants of the constrained linear representability problem (CLRP), which is the main subject of this paper. The relevance of the two variants of CLRP stated in this section to network coding and secret sharing will be discussed in §III, along with a review of prior work for solving these existential questions. For the basic terminology related to matroid theory and coding theory, we refer to the books by Oxley [43] and Betten et al. [8] respectively. The commonly used symbols and notation are described in table I.

Consider a collection of  $N$  discrete random variables  $\mathbf{X}_N = (X_1, \dots, X_N)$ . The associated *entropy vector* is a  $2^N - 1$ -dimensional vector obtained by stacking the entropies of subsets  $\mathbf{X}_A \triangleq (X_n | n \in A)$  of  $\mathbf{X}_N$  into a vector  $\mathbf{h} \triangleq (h(\mathbf{X}_A) | A \subseteq [N])$ . By convention,  $h(\emptyset) = 0$ . Let  $\mathcal{D}_N$  be the set of all joint probability mass functions for  $N$  discrete random variables. Then the *entropy function* is the map  $\mathbf{h} : \mathcal{D}_N \rightarrow \mathbb{R}^{2^N - 1}$  mapping a joint probability mass function to its entropy vector. Now consider the following problem:

- (E1) Given a vector  $\mathbf{h}' \in \mathbb{R}^{2^N - 1}$ , determine whether  $\mathbf{h}' = \mathbf{h}(p)$  for some  $p \in \mathcal{D}_N$ .

If the answer to E1 is 'yes', then there exists a joint probability mass function  $p$  s.t.  $\mathbf{h}' = \mathbf{h}(p)$ , and  $\mathbf{h}'$  is said to be *entropic*. We can now define the region of entropic vectors  $\Gamma_N^*$  as

$$\Gamma_N^* \triangleq \{\mathbf{h} \in \mathbb{R}^{2^N - 1} \mid \mathbf{h} \text{ is entropic} \} \quad (1)$$

Based on above definition, problem (E1) can be seen to be equivalent to testing membership in  $\Gamma_N^*$ . The closure of  $\Gamma_N^*$  is a convex cone. Characterization of  $\Gamma_N^*$  and  $\overline{\Gamma_N^*}$  is of central importance in network information theory as they determine all fundamental information inequalities [62], limits for secret sharing systems [5], and the capacity regions of all networks under network coding [16], [61].

Table I: Notation

$\setminus$	Set difference or polymatroid deletion
$\leq$	Subgroup relationship or inequality
$\mathbf{X}_N$	Set of $N$ discrete RVs
$[N]$	The set $1, \dots, N$ for $N \in \mathbb{N}$
$\mathcal{A}, \mathcal{B}, \mathcal{C}$	Generic sets or multisets
$\mathcal{D}, \mathcal{I}, \mathcal{J}$	
$E$	Ground set of a polymatroid (usually same as $[N]$ )
$\mathbf{X}_A$	Subset of $\mathbf{X}_N$
$\mathbf{h}$	A vector in $\mathbb{R}^{2^N - 1}$ or the entropy function, depending on context
$\mathbf{h}_{\mathcal{S}}$	Entry in vector $\mathbf{h}$ corresponding to subset $\mathcal{S}$ or entropy of a subset $\mathcal{S}$ of $\mathbf{X}_N$
$\Gamma_N^*$	Set of entropic vectors
$\overline{\Gamma_N^*}$	Closure of set of entropic vectors
$\mathcal{D}_N$	Set of all joint distributions on $\mathbf{X}_N$
$\text{rk}, f$	set functions
$2^{\mathcal{S}}$	Power set of the set $\mathcal{S}$
$c$	A constant

$P$	A polymatroid, i.e. 2-tuple consisting a set and a set function
$P^c$	Polymatroid $P$ with rank function scaled by $c$
$\mathbb{K}$	An arbitrary field
$q$	A prime power
$\mathbb{F}_q$	The $q$ -element finite field
$\Gamma_N^{\text{space}}$	Subspace inner bound
$\beta$	demands of sink nodes
$e, \mathcal{E}$	a (hyper)edge or an encoder, set of all (hyper)edges or encoders
$\mathcal{F}$	head nodes of a hyperedge
$g, \mathcal{G}$	an intermediate node, set of intermediate nodes
$s, \mathcal{S}$	a source node, set of source nodes
$t, \mathcal{T}$	a sink node, set of sink nodes
$\mathcal{I}$	A collection of constraints on the polymatroid rank function
$\mathfrak{P}$	A list of polymatroids
$\text{rep}(i)$	Bases of vector space associated with ground set element $i$
$p$ -map	An partial map from ground set of a polymatroid to $\mathbf{X}_N$
$\phi$	An isomorphism or a $p$ -map
$V_i, W_i$	Subspace associated with ground set element $i$ , presented as a matrix with $\text{rep}(i)$ as columns
$\equiv$	An arbitrary equivalence relation on a set of polymatroids or their representations
$\cong$	Strong isomorphism relation between polymatroids or their representations
$\stackrel{w}{\equiv}$	Weak isomorphism relation between polymatroids or their representations
$U_j^i$	Uniform matroid of rank $i$ and ground set size $j$
$\mathbf{u}, \mathbf{v}$	arbitrary vectors
$\text{Gr}_q(r, k)$	Set of all $k$ dimensional subspaces of $\mathbb{F}_q^r$
$\text{Gr}_q(r, K)$	Union of several $\text{Gr}_q(r, k)$ , $k \in K$
$GL(r, q)$	General linear group associated with $\mathbb{F}_q^r$
$\text{Gal}(\mathbb{q})$	Galois group of $\mathbb{F}_q$ which is the group of all automorphisms of $\mathbb{F}_q$
$\Gamma L(r, q)$	General semilinear group associated with $\mathbb{F}_q^r$
$PGL(r, q)$	Projective general linear group associated with $\mathbb{F}_q^r$
$P\Gamma L(r, q)$	Projective semilinear group associated with $\mathbb{F}_q^r$
$\mathcal{Z}_r$	Group formed by scaled versions of $\mathbb{I}_r$ over $\mathbb{F}_q$
$\langle \mathbf{v}_1, \dots, \mathbf{v}_N \rangle$	Vector subspace generated by vectors $\mathbf{v}_1, \dots, \mathbf{v}_N$
$K_P$	Set of distinct singleton ranks associated with polymatroid $P$
$\mathcal{S}_{N,r,K}$	Set of all representations of simple polymatroids of rank $r$ , size $N$ with singleton ranks from set $K$
$\mathcal{P}^q(\mathbf{c})$	A class of linear codes defined by the class tuple $\mathbf{c}$
$\mathcal{P}^q(\mathbf{c}, A)$	Linear network codes for HMSNC instance $A$ from class $\mathcal{P}^q(\mathbf{c})$
$\mathcal{R}^*$	The exact rate region of a HMSNC instance
$\mathcal{R}_{\text{out}}$	An outer bound on the exact rate region of a HMSNC instance
$\mathcal{R}_{\text{in}}$	An inner bound on the exact rate region of a HMSNC instance

Fujishige [29] observed that a vector  $\mathbf{h} \in \Gamma_N^*$  must satisfy the polymatroidal axioms (P1)-(P3) in the definition below.

**Definition 1.** A polymatroid  $(E, f)$  consists of a set  $E$ , called the ground set, and a set function  $f : 2^E \rightarrow \mathbb{R}$ , called the rank function, which satisfies the following properties:

- [(P1)]  $f(\emptyset) = 0$  (normalized)
- [(P2)]  $f(\mathcal{A}) \geq f(\mathcal{B}), \forall \mathcal{B} \subseteq \mathcal{A} \subseteq E$  (monotone)
- [(P3)]  $f(\mathcal{C}) + f(\mathcal{D}) \geq f(\mathcal{C} \cup \mathcal{D}) + f(\mathcal{C} \cap \mathcal{D}), \forall \mathcal{C}, \mathcal{D} \subseteq E$  (submodular)

Note that a polymatroid  $(E, f)$  is a matroid if it is integer valued,  $f : 2^E \rightarrow \mathbb{Z}_{\geq 0}$ , and  $f(i) \leq 1$  for each  $i \in E$ . (P1)-(P3) generate all Shannon type inequalities [62]. Unfortunately, Shannon type inequalities are only necessary conditions for determining whether or not a candidate vector is entropic. Inequalities not implied by (P1)-(P3) that are satisfied by all entropic vectors exist and are called non-Shannon type inequalities. The first such inequality was found by Zhang and Yeung [66]. Hundreds of linear non-Shannon type inequalities have been found since the Zhang-Yeung inequality [20], [24]. Furthermore, Matús [28] has shown that for  $N \geq 4$ , an infinite number of linear information inequalities is necessary to determine  $\bar{\Gamma}_N^*$ .

### A. Constrained Linear Representability Problems for polymatroids

The *representable* polymatroids are a sub-class of entropic polymatroids that arise from subspace arrangements.

**Definition 2.** A subspace arrangement in a  $k$ -dimensional vector space  $V = \mathbb{K}^k$  over some field  $\mathbb{K}$  is a multiset of  $N$  subspaces  $\mathcal{S} = \{V_1, V_2, \dots, V_N\}$  with  $V_n \subseteq V \forall n \in [N]$ . All vector spaces considered in this work are assumed to be finite dimensional. The rank function of the subspace arrangement is  $rk : 2^{[N]} \rightarrow \mathbb{Z}$  defined as

$$rk(\mathcal{S}) \triangleq \dim \sum_{i \in \mathcal{S}} V_i, \quad \forall \mathcal{S} \subseteq [N] \quad (2)$$

Note that in (2) the sum is understood to be the direct sum of subspaces of a vector space. As  $([N], rk)$  satisfies (P1)-(P3), it is a valid polymatroid. However, the converse does not necessarily hold true. This motivates the notion of representable polymatroids.

**Definition 3.** A polymatroid  $P = (E, f)$  is said to be *representable* if there exists a subspace arrangement  $\mathcal{S} = \{V_1, \dots, V_{|E|}\}$  over some field  $\mathbb{K}$  and a bijection  $m : E \rightarrow [E]$  s.t.  $f(\mathcal{S}) = rk(m(\mathcal{S}))$ ,  $\forall \mathcal{S} \subseteq E$ .

A theorem of Rado [49] which states that a polymatroid is representable over an infinite field then it is also representable over some finite field, allows us to restrict attention to fields  $\mathbb{K}$  with only a finite number of elements when considering representability of polymatroids. In the above definition, if  $\mathbb{K}$  is a finite field with  $q$  elements (i.e.  $q$  is a prime power), then we say that the polymatroid is  $\mathbb{F}_q$ -representable. Note that it is possible for  $P = (E, f)$  to not be  $\mathbb{F}_q$ -representable while a scaled version of  $P$  i.e.  $P^c = (E, cf)$ ,  $c > 0$  is. We emphasize this distinction, so as to avoid confusion later. One fact that makes representable polymatroids interesting is stated below.

**Lemma 1.** ([32], Thm. 2) *Every representable polymatroid is proportional to an entropic polymatroid.*

To see why the above statement is true, and to fix some notation, consider a representable polymatroid  $P = ([N], f)$  and let  $\{V_1, \dots, V_N\}$  be the associated subspace arrangement over finite field  $\mathbb{F}_q$  with  $q$  elements. Let the bijection mentioned in def. 3 be the identity map from  $[N]$  to itself. We assume that each subspace  $V_i, i \in [N]$  is presented as a set  $\text{rep}(i)$  of  $f(i)$  vectors in  $\mathbb{F}_q^{f([N])}$  forming a basis of the subspace  $V_i$ . Let  $\mathbb{M}(\mathcal{S})$  be the matrix  $[\text{rep}(i)|i \in \mathcal{S}]$  for each  $\mathcal{S} \subseteq [N]$  (i.e. collect together the columns in  $\text{rep}(i)$  for each  $i \in \mathcal{S}$ ). Consider a random row vector  $\mathbf{u} \sim \mathcal{U}(\mathbb{F}_q^{f([N])})$  uniformly distributed over  $\mathbb{F}_q^{f([N])}$ , and create a collection of random variables  $\mathbf{X}_N = \{X_1, \dots, X_N\}$  such that  $X_i = \mathbf{u}\mathbb{M}(i)$  is a random variable taking values in  $\mathbb{F}_q^{f(i)}$ . The entropy function maps  $\mathbf{X}_N$  to a vector  $\mathbf{h}$  such that for each  $\mathcal{A} \subseteq [N]$ , the entropy  $\mathbf{h}_{\mathcal{A}} = f(\mathcal{A}) \log_2 q = rk(\mathbb{M}(\mathcal{A})) \log_2 q$ . The polymatroid  $P^{\log_2 q} = ([N], (\log_2 q)f)$  is then entropic by construction, thus completing the proof.

We now state the representability problem for integer polymatroids.

- [E2] Given an integer polymatroid  $P = (E, f)$ , determine if there exists a representation of  $P^\alpha$  over a finite field  $\mathbb{F}_q$  for some  $\alpha \in \mathbb{N}$ .

Lemma 1, along with the fact that  $\bar{\Gamma}_N^*$  is a convex cone allow us to construct an inner bound  $\Gamma_N^{\text{space}}$  on  $\bar{\Gamma}_N^*$ , that we call the *subspace inner bound*, which is the conic hull of all representable polymatroids. Problem (E2) is equivalent to testing membership of an integer polymatroid within an inner bound to

$\Gamma_N^{\text{space}}$  formed by taking the conic hull of all polymatroids representable over a particular finite field.  $\Gamma_N^{\text{space}}$  is polyhedral for  $N \leq 5$  [26], while for  $N \geq 6$ , it remains unknown whether this set is polyhedral. The linear inequalities that are true for all points in  $\Gamma_N^{\text{space}}$  are called *rank inequalities*. For  $N \leq 3$ , the minimal (conic independent) set of rank inequalities is same as the minimal set of Shannon-type inequalities, while for  $N = 4$ , the minimal set of rank inequalities is the minimal set of Shannon-type inequalities and all 6 permutations of Ingleton's inequality [32], [33]. For  $N = 5$ , there are 24 new linear rank inequalities that, together with the Shannon-type and Ingleton inequalities, form the minimal set of inequalities [26]. One way to approach [E2] computationally, is to solve a restriction of [E2] for specific  $\alpha$  and size of finite field  $q$ , iteratively for increasing values of  $\alpha$  and  $q$  until we find a representation. This leads us to the following problem:

- [E2<sub>q</sub>] Given a polymatroid  $P = (E, f)$ , determine if there exists a representation of  $P$  over the finite field  $\mathbb{F}_q$  with  $q$  elements.

A special case of [E2<sub>q</sub>] that is well-studied is the situation where  $P$  is restricted to be a matroid. A famous conjecture of Rota [50], recently declared proven [31], states that for every finite field  $\mathbb{F}_q$ , there are only a finite number of forbidden minors, a series of smaller matroids obtained through contraction and deletion, for a matroid to be representable over that field.

We now define the notion of representation of a representable polymatroid.

**Definition 4.** A representation of a  $\mathbb{F}_q$ -representable polymatroid  $([N], f)$  associated with a multiset  $\mathcal{S} = \{V_1, \dots, V_n\}$  of subspaces is a multiset of matrices  $\{\mathbb{M}(i), i \in [N]\}$  where each subspace  $V_i$  is represented as a  $f([N]) \times f(i)$  matrix  $\mathbb{M}(i)$  whose columns are from the set  $\text{rep}(i)$  for all  $i \in [N]$ .

In the context of the definition above, two representations of the same polymatroid are considered distinct if they correspond to different multisets of subspaces. We will consider two other notions of distinctness via isomorphism later in the manuscript. Note that each subspace in such a multiset may be represented by several different bases. For the sake of simplicity, we do not distinguish between two representations that differ only in this sense. For the special case of matroids of ground set size  $N$ , we will assume that a representation is a multiset of vectors  $\{\mathbf{v}_1, \dots, \mathbf{v}_N\}$ , each of which generates a subspace of dimension at most 1. Let  $\text{Gr}_q(r, k), 0 \leq k \leq N$  be the set of all  $k$ -dimensional subspaces of  $\mathbb{F}_q^r$ . The set  $\text{Gr}_q(r, k)$  is also known as the Grassmannian. The size of  $\text{Gr}_q(r, k)$  is given by the  $q$ -ary Gaussian binomial coefficient:

$$|\text{Gr}_q(r, k)| = \binom{r}{k}_q \triangleq \frac{(q^r - 1)(q^{r-1} - 1) \dots (q^{r-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)} \quad (3)$$

For a set  $K \subseteq [r]$ , define  $\text{Gr}_q(r, K) \triangleq \bigcup_{k \in K} \text{Gr}_q(r, k)$ . We can associate with a polymatroid  $P = ([N], f)$ , a set  $K_P$  of distinct singleton ranks i.e.  $K_P \triangleq \{f(i) \mid i \in [N]\}$ . In the spirit of compactness, it is also important to consider *simple* polymatroids. A matroid is said to be simple if it has no parallel elements or loops [43], and likewise we have the following definition for a simple polymatroid

**Definition 5.** A polymatroid  $(E, f)$  is said to be simple if it satisfies following conditions:

- 1)  $\nexists e_1, e_2 \in E$  s.t.  $f(\{e_1, e_2\}) = f(e_1) = f(e_2)$
- 2) For every  $e \in E$ ,  $f(e) > 0$

If there exist elements  $e_1, e_2$  satisfying condition 1 of definition 5 above, they are said to be *parallel* with respect to each other. In fact, there can exist multiple such elements forming a parallel class.

**Definition 6.** For a polymatroid  $(E, f)$ ,  $S \subseteq E$  is said to form a parallel class if

$$f(S) = f(s) \forall s \in S \quad (4)$$

In this case,  $|S|$  is said to be the degree of the parallel class.

If there exists an element violating condition 2 of definition 5, then it is called a *loop*. The number of ground set elements that are loops is called the loop degree of the polymatroid. Given a polymatroid  $P = (E', f')$  with an order on the ground set  $E'$ , we can associate it with a simple polymatroid  $(E, f)$ , s.t.

$E \subseteq E'$  and  $f(S) = f'(S), \forall S \subseteq E$  where  $E$  is obtained by deleting all loops and all but one element of each parallel class from  $E'$ . Furthermore, we can decide to keep the smallest member of each parallel class under the aforementioned order on  $E'$ . We call  $(E, f)$  obtained in this manner the *unique simple polymatroid* associated with  $(E', f')$ , denoted as  $\text{us}(P)$ , and define, via an abuse of notation,  $|\text{us}(P)| = |E|$ . Having defined the parameters  $K_P$  and  $\text{us}(P)$  we can define the set  $\mathcal{P}^q(N, r, K, s)$  as the set of representations of polymatroids with ground set size  $N$ , containing subspaces of  $\mathbb{F}_q^r$  s.t.  $K_P \subseteq K$  and  $|\text{us}(P)| = s$  over  $\mathbb{F}_q$ . Finally, we define the set  $\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u))$  of polymatroid representations as

$$\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u)) \triangleq \bigcup_{\substack{r_l \leq r \leq r_u \\ s_l \leq s \leq s_u}} \mathcal{P}^q(N, r, K, s) \quad (5)$$

Henceforth, we shall refer to the tuple  $\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$  as the *class tuple* and abbreviate  $\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u))$  to  $\mathcal{P}^q(\mathbf{c})$ . This leads us to state precisely what we mean by a class of linear codes for the purpose of this work.

**Definition 7.** A class of linear codes is any set  $\mathcal{P}^q(\mathbf{c})$  where  $\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$  is the class tuple satisfying  $r_l \leq r_u \leq N \cdot \max K, s_l \leq s_u \leq N$  where  $K$  is a finite set containing non-negative integers.

We are now ready to define the central problem addressed in this work. In several problems of practical interest, which will be described in the next section, rather than testing representability for a polymatroid specified by its rank function, it is of interest to determine whether there exists a polymatroid representable over  $\mathbb{F}_q$  satisfying a specified collection of linear constraints on its rank function, and belonging to a particular class of linear codes. We will name this problem the constrained linear representability problem (CLRP) for polymatroids. More formally, let  $\mathcal{I}$  be a collection of linear constraints on the rank function of a polymatroid with ground set  $[N]$  and  $\mathbf{c}$  be any valid class tuple. Then, the existential variant of CLRP can be stated as follows:

- [CLRP<sub>q</sub>-EX] Given a system  $\mathcal{I}$  of constraints on the rank function of a polymatroid with ground set  $[N]$ , determine if there exists a polymatroid that satisfies  $\mathcal{I}$  in  $\mathcal{P}^q(\mathbf{c})$ .

Note that [E2<sub>q</sub>] is a special case of [CLRP<sub>q</sub>], as a pre-specified rank function  $f$  of a polymatroid  $(E, f)$  can be interpreted as a collection of  $2^N$  linear constraints on the rank function with  $N = |E|$ . As we shall discuss in next section, it is sometimes of interest to find *all* polymatroids satisfying  $\mathcal{I}$  and belonging to  $\mathcal{P}^q(\mathbf{c})$ . We now state CLRP<sub>q</sub>-EN to be the problem of constructing the members of  $\mathcal{P}(N, (r_l, r_u), K, (s_l, s_u))$  up to some notion of equivalence  $\equiv$ .

- [CLRP<sub>q</sub>-EN] Given a system  $\mathcal{I}$  of constraints on the rank function of a polymatroid with ground set  $[N]$ , list a representative from each equivalence class, under  $\equiv$ , of polymatroids in  $\mathcal{P}(N, (r_l, r_u), K, (s_l, s_u))$  representable over  $\mathbb{F}_q$ , that satisfy  $\mathcal{I}$ .

An algorithm to solve CLRP<sub>q</sub>-EN can also solve CLRP<sub>q</sub>-EX, by halting as soon as it finds one (the first) such polymatroid representation. The design of finite-terminating algorithms to solve CLRP<sub>q</sub>-EN is the subject of much of this paper. The approach we use is that of using combinatorial generation techniques which are able to construct combinatorial objects satisfying certain desired properties systematically, exhaustively, and efficiently.

### III. NETWORK CODING, SECRET SHARING AND CLRP

We now review the basic terminology related to network coding and secret sharing, showing that creating computer assisted achievability proofs and rate regions in network coding and secret sharing with finite length linear codes can be posed as variants of CLRP.

### A. Network coding as CLRP

Multisource multisink network coding over directed acyclic graphs (MSNC) was studied by Yan et. al. [61], where the authors give an implicit characterization of the rate regions in terms of  $\Gamma_N^*$ . The version of network coding problem considered here is *multisource multisink network coding over directed acyclic hypergraphs* (HMSNC), which was studied recently by Li et. al. [16]. HMSNC is a general model that includes as special case the MSNC problem, the Independent Distributed Source Coding (IDSC) problem, and the index coding (IC) problem [16].

A HMSNC instance is completely described by the tuple  $A = (\mathcal{S}, \mathcal{G}, \mathcal{T}, \mathcal{E}, \beta)$ . It consists of a directed acyclic hypergraph  $(\mathcal{V}, \mathcal{E})$  where the nodes  $\mathcal{V} = \mathcal{S} \cup \mathcal{T} \cup \mathcal{G}$  can be partitioned into the set of source nodes  $\mathcal{S}$ , the set of sink nodes  $\mathcal{T}$  and the set of intermediate nodes  $\mathcal{G}$ .  $\mathcal{E}$  is the set of directed hyperedges of the form  $(v, \mathcal{A})$  where  $v \in \mathcal{V}$ ,  $\mathcal{A} \subseteq \mathcal{V} \setminus \{v\}$ . The source nodes in  $\mathcal{S}$  have no incoming edges and exactly one outgoing edge carrying the source message, the sink nodes  $\mathcal{T}$  have no outgoing edges, and the intermediate nodes  $\mathcal{G}$  have both incoming and outgoing edges. Any hyperedge  $e \in \mathcal{E}$  then connects a source or an intermediate node to a subset of non-source nodes, i.e.,  $e = (i, \mathcal{F})$ , where  $i \in \mathcal{S} \cup \mathcal{G}$  and  $\mathcal{F} \subseteq (\mathcal{G} \cup \mathcal{T}) \setminus \{i\}$ . The number of source nodes will be denoted by  $|\mathcal{S}| = k$ , with a source message associated with each node. For convenience, we shall label the source messages on the outgoing hyperedges of source nodes as  $1, \dots, k$ . The remaining messages, carried on the rest of the hyperedges, are labeled  $k+1, \dots, |\mathcal{E}|$ . Thus, we have a total of  $N = |\mathcal{E}|$  messages. The demand function  $\beta : \mathcal{T} \rightarrow 2^{[k]}$  associates with each sink node a subset of source messages that it desires. Each message  $i \in [N]$  will be associated with a discrete random variable  $X_i$ , giving us the set  $\mathbf{X}_N$  of message random variables.

In network coding, it is assumed that the random variables  $\{X_i \mid i \in [k]\}$  associated with source messages are independent. Recalling that we are casting network coding rate region problems into the light of CLRPs, the source independence gives rise to the first constraint on the entropy function,

$$\mathbf{h}_{[k]} = \sum_{i \in [k]} \mathbf{h}_k. \quad (6)$$

For notational convenience, we form the set  $\mathcal{L}_1$  containing only the above constraint. For any  $v \in \mathcal{G} \cup \mathcal{T}$  define  $\text{In}(v)$  to be the set of its incoming messages, and for each  $g \in \mathcal{G}$ , define  $\text{Out}(g)$  to be the set of its outgoing messages. Every non-source message  $i \in [N] \setminus [k]$ , originates at some intermediate node  $g \in \mathcal{G}$ , and the associated random variable  $X_i = f_i(\{X_j, j \in \text{In}(g)\})$  is a function of all the input random variables of node  $g$ . This gives rise to constraints of the following type

$$\mathbf{h}_{\text{In}(g) \cup \text{Out}(g)} = \mathbf{h}_{\text{In}(g)}, \quad \forall g \in \mathcal{G}. \quad (7)$$

We collect the above constraints into a set  $\mathcal{L}_2$ . Finally, the demand function requires that each node  $t \in \mathcal{T}$  be able to reconstruct those source messages with indices in  $\beta(t)$ , which naturally gives rise to the decoding constraints

$$\mathbf{h}_{\text{In}(t) \cup \beta(t)} = \mathbf{h}_{\text{In}(t)}, \quad \forall t \in \mathcal{T}. \quad (8)$$

The decoding constraints are collected in a set  $\mathcal{L}_3$ . We shall denote the collected constraints on the entropy function associated with this network coding problem  $A$  as  $\mathcal{I}_A = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$ .

**Definition 8.** A network code for a HMSNC instance  $A$  is a collection of  $N$  discrete random variables  $\mathbf{X}_N$  with joint entropies satisfying the constraints  $\mathcal{I}_A$ .

Equivalently, a network code is an entropic polymatroid satisfying the constraints  $\mathcal{I}_A$  on its rank function. From the standpoint of the rate region of a network coding problem, all that matters, given the knowledge that the joint entropies satisfy the constraints of the network, is the singleton entropies. Thus, we will say that a network code  $\mathbf{X}_N$  achieves a rate vector  $\mathbf{r} = (r_1, \dots, r_N)$ ,  $r_i \in \mathbb{Z}_{\geq 0}$  if  $\mathbf{h}_i = r_i$ ,  $\forall i \in [N]$ .

Let  $\mathbb{R}^M$  be the space with subset entropies and rates as co-ordinates, i.e.  $M = 2^N - 1 + N$ . Aforementioned notion of achieving a rate vector  $\mathbf{r}$  follows directly from a result of Yan, Yeung, and Zhang [61], which can be easily generalized to provide the (closure of) the set of all rate vectors achievable

for a given network coding problem instance  $A$  [16], thereby yielding the capacity region of the network as

$$\mathcal{R}^* = \text{proj}_{\mathbf{r}}(\overline{\text{con}(\Gamma_N^* \cap \mathcal{L})} \cap \mathcal{L}') \quad (9)$$

where  $\text{con}(\mathcal{B})$  is the conic hull of set of vectors  $\mathcal{B}$ ,  $\text{proj}_{\mathbf{r}}(\mathcal{B})$  is the projection onto coordinates  $\mathbf{r}$  and where

$$\mathcal{L} \triangleq \{(\mathbf{h}, \mathbf{r}) \in \mathbb{R}^M \mid \mathbf{h} \text{ satisfies } \mathcal{L}_1 \cup \mathcal{L}_2\} \quad (10)$$

$$\mathcal{L}' \triangleq \{(\mathbf{h}, \mathbf{r}) \in \mathbb{R}^M \mid (\mathbf{h} \text{ satisfies } \mathcal{L}_3) \wedge (r_i \geq \mathbf{h}_i, \text{ for each } i \in [N] \setminus [k]) \wedge (r_i \leq \mathbf{h}_i, \text{ for each } i \in [k])\}$$

Under this formulation, the rate region for the network is a convex cone, described by a series of inequalities linking the rates of the sources  $r_i, i \in [k]$ , with the capacities of the links  $r_i, i \in [N] \setminus [k]$ . As  $\Gamma_N^*$  is not yet fully characterized for  $N \geq 4$ , most of the HMSNC rate region characterizations known so far have been found using the method of *sandwich bounds* [16], [25], which is based on substituting polyhedral inner and outer bounds in place of  $\Gamma_N^*$  in (9). This yields inner and outer bounds  $\mathcal{R}_{\text{in}}$  and  $\mathcal{R}_{\text{out}}$  on  $\mathcal{R}^*$ ,

$$\mathcal{R}_{\mathbf{x}} = \text{proj}_{\mathbf{r}}(\Gamma_{\mathbf{x}} \cap \mathcal{L} \cap \mathcal{L}'), \mathbf{x} \in \{\text{in}, \text{out}\} \quad (11)$$

Once we compute  $\mathcal{R}_{\text{in}}$  and  $\mathcal{R}_{\text{out}}$ , if  $\mathcal{R}_{\text{in}} = \mathcal{R}_{\text{out}}$ , we know that  $\mathcal{R}^* = \mathcal{R}_{\text{in}} = \mathcal{R}_{\text{out}}$ . In the context of this paper, we are particularly interested in rate vectors that are achievable with *linear* network codes. Given a class  $\mathcal{P}^q(\mathbf{c})$  of linear codes, one can consider the following inner bound on  $\Gamma_N^*$ :

$$\Gamma_N^{\mathcal{P}^q(\mathbf{c})} = \text{con}(\{\mathbf{h} \in \mathbb{R}^{2^N-1} \mid \mathbf{h} \in \mathcal{P}^q(\mathbf{c})\}) \quad (12)$$

yielding the inner bound  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})} = \text{proj}_{\mathbf{r}}(\Gamma_{\mathcal{P}^q(\mathbf{c})} \cap \mathcal{L} \cap \mathcal{L}')$  to the rate region  $\mathcal{R}^*$ .

A linear network code is a representable polymatroid that satisfies constraints  $\mathcal{I}_A$  on its rank function. As an aside, note that a linear network code is said to be *scalar* if the associated polymatroid is in fact a matroid. From the perspective of achievability proofs for network coding rate regions, and the inner bounds associated with linear codes  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$ , there are two variants of the constrained linear representability problem that are of interest, an existential one building from  $\text{CLRP}_q\text{-EX}$  and an enumerative one building from  $\text{CLRP}_q\text{-EN}$ . The existential variant takes a specified rate vector  $\mathbf{r}$  and asks whether there is a code over  $\mathbb{F}_q$  which achieves it.

- [E3<sub>q</sub>-EX] Given a HMSNC instance  $A$ , determine if there exists polymatroid of size  $N$  representable over  $\mathbb{F}_q$  satisfying  $\mathcal{I}_A$  achieving a rate vector  $\mathbf{r}$ .

Note that E3<sub>q</sub>-EX is a special case of  $\text{CLRP}_q\text{-EX}$ , as we can interpret the requirement to achieve a rate vector  $\mathbf{r}$  as additional linear constraints  $\mathcal{I}_{\mathbf{r}} = \{\{\mathbf{h}_i = r_i\}, i \in [N]\}$ . Hence, it is an instance of  $\text{CLRP}_q\text{-EX}$  with constraints  $\mathcal{I} = \mathcal{I}_A \cup \mathcal{I}_{\mathbf{r}}$  and class tuple  $\mathbf{c} = (N, (\sum_i r_i, \sum_i r_i), \text{unique}(\mathbf{r}), (k, N))$ , where  $\text{unique}(\mathbf{r})$  is the set of unique values in vector  $\mathbf{r}$ .

The enumerative variant associated with achievability proofs in network coding rate regions aims instead to find, up to isomorphism  $\equiv$ , all linear codes in a given class that satisfy the constraints of the network.

- [E3<sub>q</sub>-EN] Given a class tuple  $\mathbf{c}$  and a HMSNC instance  $A$ , list a representative from equivalence class of codes (under  $\equiv$ ) yielding joint entropy vectors  $\mathbf{h} \in \mathcal{P}^q(\mathbf{c})$  s.t.  $\mathbf{h}$  satisfies  $\mathcal{L}_1, \mathcal{L}_2$  and  $\mathcal{L}_3$  associated with  $A$ .

Observe that E3<sub>q</sub>-EN is likewise a special case of  $\text{CLRP}_q\text{-EN}$  associated with the same code class  $\mathbf{c}$ , where again the system of constraints is given by the constraints  $\mathcal{L}$  built from the network coding problem  $A$ .

Having defined the two problem classes, some comparison and historical discussion is in order. The existing computation based information theory achievability proofs literature, while thin, is focussed on the former of these two problems E3<sub>q</sub>-EX. This matches the situation with the computer aided converse proof literature, which, with the notable exception from our own previous work [1], [4], [13]–[16], aims to provide proofs verifying a putative given inequality [48], [56], [63] (i.e. membership testing in the polar  $\mathcal{R}_{\text{out}}^\circ$ ), rather than generating that inequality as part of a full description of an outer bound  $\mathcal{R}_{\text{out}}$  in the first place. The seminal network coding paper of Koetter and Medard [35] provided an algebraic



formulation of a slight variation of  $E3_q$ -EX which replaces  $\mathbb{F}_q$  with its algebraic closure  $\mathbb{F}_q^*$ . Under this Koetter and Medard formulation, one can construct a system of polynomial equations with coefficients in  $\mathbb{F}_q$  s.t. non-emptiness of the associated algebraic variety implies the existence of a polymatroid satisfying  $\mathcal{I}$  that is representable over the algebraic closure of  $\mathbb{F}_q$  and vice versa. The problem of determining the emptiness of the algebraic variety associated with these polynomial equations can be solved by computing the Gröbner basis [18] of the ideal generated by them in  $\mathbb{F}_q[\mathbf{x}]$ . Shifting back to  $E3_q$ -EX, i.e. if one is interested in existence of solution over a specific finite field (and not the algebraic closure of it), one can instead compute the Gröbner basis in the quotient ring  $\mathbb{F}_q[\mathbf{x}] \setminus \langle x_i^q = x_i \mid i \in [n] \rangle$ . An important subsequent work of Subramanian and Thangaraj [55] refined the algebraic formulation of Koetter and Medard to switch to using path gain variables instead of variables that represent local coding coefficients. The benefit of this path gain formulation is that the polynomials contain monomials of degree at most 2, which can have substantial complexity benefits over the original Koetter and Medard formulation in the Gröbner basis calculation. The details of how to adapt this method of Subramanian and Thangaraj to solve  $E3_q$ -EX are provided in algorithm 2 in the appendix. As we will show via computational experiments in §VI, the new methods for solving  $E3_q$ -EX that we will provide in this work, which, in fact, are built from enumerative methods best suited to solving  $E3_q$ -EN, in some problems enable substantial reduction of runtime relative to the Subramanian and Thangaraj Gröbner basis based formulation. The reduction in runtime appears to be most pronounced when the rate vectors  $\mathbf{r}$  being tested contain integers greater than one.

More broadly, when one has computed a polyhedral outer bound  $\mathcal{R}_{\text{out}}$  to  $\mathcal{R}^*$ , e.g. through polyhedral projection with the convex hull method [36], [59] as described in our previous work [1], [4], one can utilize a series of  $E3_q$ -EX problems to determine if  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})} = \mathcal{R}_{\text{out}}$  as follows. For each extreme ray  $\mathbf{r}$  of  $\mathcal{R}_{\text{out}}$ , one uses  $E3_q$ -EX to determine if  $\mathbf{r}$  is achievable with linear codes in the associated class  $\mathbf{c}$ . If the answer is yes for each of the extreme rays of  $\mathcal{R}_{\text{out}}$ , then  $\mathcal{R}^* = \mathcal{R}_{\text{out}} = \mathcal{R}^* = \mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$ . However, if the answer to  $E3_q$ -EX is no for one or more of the extreme rays  $\mathcal{R}_{\text{out}}$ , then it can be of interest to determine the region  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$  achievable with this class of codes.

This more difficult problem of determining the inequality description of the polyhedral cone  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$  can be solved with an algorithm providing a solution to  $E3_q$ -EN. Indeed, denoting the set of vectors forming the solution to  $E3_q$ -EN as  $\mathcal{P}^q(\mathbf{c}, A)$ , one can determine  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$  with e.g. the following remaining steps:

- 1) Delete all co-ordinates of  $\mathbf{h} \in \mathcal{P}^q(\mathbf{c}, A)$  other than singletons
- 2) Append the resulting list of vectors with  $-\mathbf{e}_i, i \in [k]$  and  $\mathbf{e}_i, i \in [N] \setminus [k]$ , where  $\mathbf{e}_i$  is the  $i$ th column of the identity matrix of dimension  $N$
- 3) Compute the inequality description of the conic hull of the resulting set of  $N$  dimensional vectors

The resulting inequalities are the system of inequalities defining the polyhedral cone  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$ , and the resulting extreme rays of the conic hull form the optimal codes which can be time-shared to achieve any point in  $\mathcal{R}_{\mathcal{P}^q(\mathbf{c})}$  arbitrarily closely [15], [16]. For the rest of the paper, rate regions will be specified as inequalities amongst source rate variables  $\omega_i, i \in [k]$  and edge rate variables  $R_j, j \in [N] \setminus [k]$ , whereas the rate vectors will be specified as  $(\boldsymbol{\omega}, \mathbf{r})$ , where  $\boldsymbol{\omega}$  and  $\mathbf{r}$  are source and edge rate vectors of size  $k$  and  $N - k$  respectively, to enhance readability.

## B. Secret sharing as CLRP

The next application where the ability to solve CLRP-EX is useful is secret sharing. Secret sharing [5], [53] is concerned with the sharing of a secret among a collection of people or entities such that only certain subsets of them can recover the secret. Let  $\Delta$  be the set of participants. We assume that  $|\Delta| = N$ , with participants labeled by  $[N]$ . The secret sharer is called the dealer, and has label 1 while the rest of the participants, called parties have labels in  $\{2, \dots, N\}$ . The dealer bears a secret, and gives each party a chunk of information, called a *share*. The subsets of  $\Delta \setminus \{1\}$  that are allowed to reconstruct the secret are called the authorized sets. The set of all authorized subsets, called an *access structure*, and denoted by  $\Gamma$  is a monotone collection of sets i.e.  $\mathcal{A} \in \Gamma \implies \mathcal{B} \in \Gamma, \forall \mathcal{B} \supset \mathcal{A}$ . We associate a random variable  $X_1$

with the dealer and random variables  $X_2, \dots, X_N$  with the parties. Given an access structure  $\Gamma$  containing authorized subsets of  $\{2, \dots, N\}$ , every authorized set of participants must be able to recover the secret, imposing the following constraints on the entropy function.

$$\mathbf{h}_{\mathcal{S} \cup \{1\}} = \mathbf{h}_{\mathcal{S}}, \forall \mathcal{S} \in \Gamma \quad (13)$$

Moreover, an un-authorized set must not be able to gain any information about the secret, imposing the following constraints on the entropy function.

$$\mathbf{h}_1 + \mathbf{h}_{\mathcal{S}} = \mathbf{h}_{\mathcal{S} \cup \{1\}}, \forall \mathcal{S} \notin \Gamma \quad (14)$$

We denote the collection of constraints specified by (13) and (14) as  $\mathcal{I}_\Gamma$ .

**Definition 9.** A secret sharing scheme (SSS) for a access structure  $\Gamma \subseteq 2^{\{2, \dots, N\}}$  is a collection of  $N$  random variables whose joint entropies satisfy the constraints  $\mathcal{I}_\Gamma$ .

A SSS is linear if it is associated with a representable matroid with ground set size  $N$  satisfying  $\mathcal{I}_\Gamma$ . A SSS is said to be multi-linear if it is associated with a representable polymatroid satisfying  $\mathcal{I}_\Gamma$ . We can now formulate the achievability problem for secret sharing as follows.

- [E5<sub>q</sub>] Given an access structure  $\Gamma$ , determine if there exists a polymatroid of size  $N$  representable over  $\mathbb{F}_q$  satisfying  $\mathcal{I}_\Gamma$  with secret size  $r_1$  and share sizes  $(r_2, \dots, r_N)$ .

Again, [E5<sub>q</sub>] can be seen as special case of CLRP<sub>q</sub> respectively, by interpreting the requirement to have specific secret and share sizes as a collection of constraints  $\mathcal{I}_\mathbf{r} = \{\{h_i = r_i\}, i \in [N]\}$ , where  $\mathbf{r} = (r_1, \dots, r_N)$ . The class of codes  $\mathcal{P}^q(\mathbf{c})$  is specified by the class tuple  $\mathbf{c} = (N, (\max_i r_i, \sum_i r_i - 1), \text{unique}(\mathbf{r}), (2, N))$

Secret sharing schemes can be classified into two types: those constructed by putting together other secret sharing schemes (decomposition constructions) and those that are constructed from scratch without using existing schemes (basic constructions). Decomposition constructions of secret sharing schemes have been proposed by Blundo et al. [10], Stinson [54], van Dijk et al. [22], [58]. Basic constructions of linear schemes were proposed by Bertilsson et al. [7] and van Dijk [57]. In [57], van Dijk refers to a secret sharing scheme associated with a representable polymatroid as the generalized vector space construction. He also proposes a backtracking algorithm for determining whether a certain worst case information rate (in context of problem [E5<sub>q</sub>],  $\frac{\max_{i \in \{2, \dots, N\}} r_i}{r_1}$  is the worst case information rate) can be achieved in a given access structure by means of the generalized vector space construction, thus providing an algorithm to solve a variant of (E5<sub>q</sub>). Secure network coding (SNC) [11] is a generalization of secret sharing. Again, one can form a variant of CLRP in the context of SNC.

#### IV. POLYMATROID ISOMORPHISM, PARTIAL $\mathcal{I}$ -FEASIBILITY, AND EXTENSION

Algorithms for generating various types of combinatorial objects that are special-cases of polymatroids: graphs, linear codes, matroids and  $k$ -polymatroids, up to some equivalence relation  $\equiv$ , have been studied in the literature, see e.g. [8], [9], [39], [41], [51]. A common theme in these algorithms is that of "orderly generation". Here, each combinatorial object  $X$  has an associated non-negative number "order"  $o(X)$  which is the size of the object. This could be the number of edges for graphs, block length for linear codes or the ground set size for matroids/polymatroids. The aim of these algorithms is to list inequivalent objects of order up to some  $N \geq 1$ . The name orderly generation follows from the fact that these algorithms proceed in an orderly fashion, by constructing inequivalent objects of size  $i \leq N$  from the list of inequivalent objects of size  $i - 1$ , recursively in  $i$ . The key tool used for constructing an object of size  $i$  from an object of size  $i - 1$  is the notion of *augmentation*. For matroids or polymatroids, an example of such operation is extension, which augments a polymatroid with ground set size  $i - 1$  by adding a new element to the ground set, thereby constructing a polymatroid with ground set size  $i$ . In order to apply this orderly generation technique to solving CLRP<sub>q</sub>-EN and CLRP<sub>q</sub>-EX, three decisions must be made. The remaining subsections of this section describe the answers to these questions in detail, while we give a high level description here.

First, one must specify precisely the combinatorial objects whose generation is being attempted. In §IV-A, given a specific collection of constraints  $\mathcal{I}$  on the rank function of a polymatroid of ground set size  $N$ , we define the concept of linear  $\mathcal{I}$ -polymatroids which is a mathematical formalization of 'polymatroids in  $\mathcal{P}^q(\mathbf{c})$ , that satisfy  $\mathcal{I}$ ' as mentioned in CLRP $_q$ -EN. For a given class of codes  $\mathcal{P}^q(\mathbf{c})$  and constraints  $\mathcal{I}$  on a polymatroid of ground set size  $N$ , a  $\mathbb{F}_q$ -linear  $\mathcal{I}$ -polymatroid is a pair  $(P, \phi)$  where  $P$  is a  $\mathbb{F}_q$ -representable polymatroid in  $\mathcal{P}^q(\mathbf{c})$ , having ground set size  $N$  and  $\phi$  is a bijection  $\phi : [N] \rightarrow [N]$ . The domain of  $\phi$  is understood to be the ground set of  $P$  while the range is understood to be the set associated with the set function that  $\mathcal{I}$  is constraining (we choose to label both these sets with  $[N]$ ). In particular,  $\phi$  is a map under which  $P$  satisfies  $\mathcal{I}$ .  $\phi$  is reminiscent of the network-matroid mapping of Dougherty, Freiling and Zeger [25], albeit being set up the other way around (from a polymatroid to a network, when  $\mathcal{I}$  arises from a network coding instance). A  $\mathbb{F}_q$ -representable polymatroid for which such a mapping  $\phi$  exists is said to have the property of  $\mathcal{I}$ -feasibility. In order to embed the constraint of  $\mathcal{I}$ -feasibility into an orderly generation oriented algorithm gradually growing the polymatroid's ground set, we further expand this idea to polymatroids of ground set size  $i \leq N$  via the property of partial  $\mathcal{I}$ -feasibility or  $p\mathcal{I}$ -feasibility, to define linear  $p\mathcal{I}$ -polymatroids, which are  $\mathbb{F}_q$ -representable polymatroids with ground set size  $i \leq N$  for which there exists an injective mapping  $\phi : [i] \rightarrow [N]$ , under which it satisfies a subset of  $\mathcal{I}$  associated with  $\phi([i])$ . The mapping  $\phi$  in this case is called a  $p$ -map, which is shorthand for partial map. Noting that the smaller polymatroid created via the deletion of any ground set elements of a  $p\mathcal{I}$ -feasible polymatroid must also be  $p\mathcal{I}$ -feasible polymatroid, we arrive at the conclusion that the criterion of  $p\mathcal{I}$ -feasibility can be embedded into the orderly generation algorithm. Namely, if at any time in the extension process we encounter a polymatroid that is not  $p\mathcal{I}$ -feasible, we do not need to compute any extensions of this polymatroid, as they will also not be  $p\mathcal{I}$ -feasible.

In addition to the goal of generating only polymatroids which will ultimately obey the constraints  $\mathcal{I}$ , we are also interested in generating exclusively the *essentially different* ones. This leads to the next of the three decisions which must be made: the notion of equivalence. The equivalence relation  $\equiv$  mentioned while defining CLRP captures this idea. In §IV-B, we discuss two notions of isomorphism: strong isomorphism and weak isomorphism. Both of these notions have been used in literature to generate combinatorial objects related to polymatroids. Literature related to generation of matroids and 2-polymatroids [9], [39], [41] uses strong isomorphism. The literature concerning the generation/classification of linear codes [8] uses weak isomorphism as it is associated with the semi-linear isometry relation on linear codes of given block-length. We use words 'strong' and 'weak' to emphasize the fact that weak isomorphism is a refinement of strong isomorphism, which we elaborate on using example 1. The benefit of using weak isomorphism for representability polymatroids over strong isomorphism is that it enables group theoretic techniques to provide an algorithm that can exhaustively generate simple  $p\mathcal{I}$ -feasible polymatroids that are distinct under weak isomorphism. In order to generate representable polymatroids that are distinct under strong isomorphism, while also not necessarily simple, these weakly non-isomorphic can be subjected to further strong isomorphism testing among those pairs whose parameters admit the possibility of strong isomorphism. Ultimately, we settle on an algorithm which uses both of these notions of isomorphism together, which is implemented in our software ITAP, as described in Section V-B.

In section IV-C, we describe a general template for generating all members of a particular class of codes  $\mathcal{P}^q(\mathbf{c})$  up to equivalence relation  $\equiv$ , which is of interest by itself, as it allows one to construct inner bounds  $\Gamma_N^{\mathcal{P}^q(\mathbf{c})}$  on  $\overline{\Gamma}_N^*$ . While this template is motivated by algorithms to generate classes of polymatroids more general than linear polymatroids, we use a restrictive definition of polymatroid extension, that preserves  $\mathbb{F}_q$ -representability, thus avoiding the problem of handling non-representable extensions of representable polymatroids. §IV-D defines a notion of augmentation for  $p$ -maps, called *p-map extension*. This, along with our restrictive notion of polymatroid extension, provides an augmentation operation for  $p\mathcal{I}$ -polymatroids, settling the third key decision of choosing the augmentation operation for designing an orderly generation algorithm. We also provide an algorithmic description of how such augmentation can be performed in practice in §IV-D, along with the details of symmetry exploitation while performing such augmentation

in §IV-E.

### A. $p\mathcal{I}$ -feasibility, $p\mathcal{I}$ -polymatroids and $\mathcal{I}$ -polymatroids

For a collection of constraints  $\mathcal{I}$  we will first define the property of  $p\mathcal{I}$ -feasibility which plays a central role in algorithms discussed later in the paper. For simplicity, we assume that  $\mathcal{I}$  is presented as a set of linear constraints on the set function defined over  $[N]$ , with  $N$  being called the *size* of  $\mathcal{I}$ . For a polymatroid  $P = ([i], f)$  with  $i \leq N$ , we can consider a partial map ( $p$ -map) that is an injective mapping  $\phi$  from  $[i]$  to a  $[N]$  that satisfies the relevant part of  $\mathcal{I}$ . More formally, given a subset  $\mathcal{X} \subseteq [N]$  we denote by  $\mathcal{I}(\mathcal{X})$  the subset of  $\mathcal{I}$  that contains only those constraints whose involved sets, upon which the set function is evaluated, exclusively to include indices from  $\mathcal{X}$ .

**Definition 10.** A polymatroid  $([i], f)$  with  $i \leq N$  is a  $p\mathcal{I}$ -feasible if there exists an injective mapping  $\phi : [i] \rightarrow [N]$  s.t.  $f(\phi^{-1}(\cdot))$  satisfies  $\mathcal{I}(\phi([i]))$ .

We call a  $p\mathcal{I}$ -feasible polymatroid a  $p\mathcal{I}$ -polymatroid, while a  $p\mathcal{I}$ -polymatroid of size  $N$  is called a  $\mathcal{I}$ -polymatroid. If  $\mathcal{I}$  arises from a HMSNC instance, and  $([N], f)$  is a matroid, then  $\phi^{-1}$  in above definition is known as the *network-matroid* mapping [25]. We shall denote the injective map associated with a  $p\mathcal{I}$ -polymatroid as the  $p\mathcal{I}$ -map and the bijection associated with an  $\mathcal{I}$ -polymatroid as the  $\mathcal{I}$ -map. Note that the set of all bijections from  $[N]$  to itself, denoted as  $\Omega$  has size  $N!$  while set of all maps from  $[i]$  to  $\{j_1, \dots, j_i\} \subseteq [N]$  for  $i \leq N$  denoted as  $\Omega_p$  contains  $\sum_{k=0}^{N-1} \binom{N}{k} (N-k)!$  maps with  $\Omega \subseteq \Omega_p$ . Fig. 1 and Fig.2 give examples of an  $\mathcal{I}$ -matroid and an  $\mathcal{I}$ -polymatroid respectively.

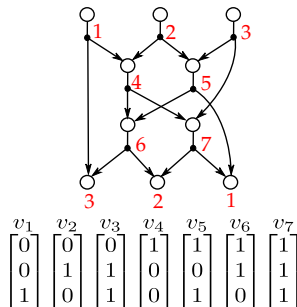


Figure 1: (top) the HMSNC instance Fano Network, and (bottom) a representation of the Fano matroid that is an  $\mathcal{I}$ -(poly)matroid with mapping  $\phi$  defined as  $\{1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 6, 6 \mapsto 5, 7 \mapsto 7\}$ .

$$\left\{ \begin{array}{l} V_1 \\ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{array}, \begin{array}{l} V_2 \\ \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \end{array}, \begin{array}{l} V_3 \\ \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \end{array}, \begin{array}{l} V_4 \\ \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \end{array}, \begin{array}{l} V_5 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array} \right\}$$

Figure 2: An  $\mathcal{I}$ -polymatroid for the collection of constraints  $\mathcal{I}$  arising from rank vector  $[2, 2, 4, 2, 4, 4, 4, 1, 2, 3, 4, 3, 4, 4, 4, 1, 3, 3, 4, 3, 4, 4, 4, 2, 3, 4, 4, 3, 4, 4, 4]$  with mapping  $\phi$  defined as  $\{1 \mapsto 4, 2 \mapsto 5, 3 \mapsto 1, 4 \mapsto 3, 5 \mapsto 2\}$ . This polymatroid is an extreme ray of the cone of linear rank inequalities in 5 variables [26].

Thus, each  $p\mathcal{I}$ -polymatroid is a pair  $(P, \phi)$  where  $P$  is a polymatroid representation and  $\phi$  is a  $p$ -map. The combinatorial objects we want to systematically generate are  $p\mathcal{I}$ -polymatroids belonging to a particular class of codes  $\mathcal{P}^q(\mathbf{c})$ ,  $\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$  up to an equivalence relation  $\equiv$ . From orderly generation perspective, each of these has size  $N$ . The smaller objects of size  $i < N$  belong to different classes of linear codes  $\mathcal{P}^q(\mathbf{c}_i)$  where  $\mathbf{c}_i = (i, (r_l, r_u), K, (\max(s_l, i), \min(i, s_u)))$ .

## B. Notions of polymatroid isomorphism and the equivalence relation $\equiv$

The most natural notion of isomorphism for polymatroids is the following one.

**Definition 11** (Strong Isomorphism). *Two polymatroids  $P_1 = (E_1, f_1)$  and  $P_2 = (E_2, f_2)$  are said to be isomorphic if there exists a bijection  $\phi : E_1 \rightarrow E_2$  s.t.  $f_1(S) = f_2(\phi(S)), \forall S \subseteq E_1$ , denoted as  $P_1 \cong P_2$ .*

Given two polymatroids  $P_1$  and  $P_2$ , the problem of determining if they are strongly isomorphic has received attention in the literature only in the special case where they are either representable matroids or graphic matroids. Testing if two matroids representable over  $\mathbb{F}_q$  are strongly isomorphic is known to be no easier than the graph isomorphism problem [47], whose complexity status remains unresolved. There exist necessary conditions for isomorphism, that can be checked in polynomial-time, e.g. for binary matroids [45]. The problem is somewhat easier if we know beforehand that  $\text{us}(P_1) = \text{us}(P_2)$ . Here, we can use the degree vector, as defined below.

**Definition 12.** *The degree vector  $(d_1, \dots, d_{|\text{us}(P)|+1})$  of a polymatroid  $P = (E, f)$  with a specified order on  $E$  is an integer vector of size  $|E| + 1$  where  $(E, f) = \text{us}(P)$  with the  $i$ th entry of the degree vector indicating the size of parallel class of the  $i$ th smallest non-loop element of  $E$  in  $P$  for  $i \in [|E|]$ , whereas the  $|E| + 1$ th element specifies the loop degree.*

An automorphism of a polymatroid is a strong isomorphism from a polymatroid to itself.

**Lemma 2.** *Let  $P_1 = (E_1, f_1)$  and  $P_2 = (E_2, f_2)$  be two polymatroids s.t.  $|E_1| = |E_2|$  and  $\text{us}(P_1) = \text{us}(P_2)$ . Then  $P_1$  and  $P_2$  are strongly isomorphic if and only if their associated degree vectors are identical up to an automorphism of  $\text{us}(P)$ .*

To introduce further notions of isomorphism, we first describe the group of semi-linear isometries of  $\mathbb{F}_q^r$  and describe its action on the set of all distinct representations of simple linear polymatroids of specified size and rank. Then we explain how this action results in a equivalence relation that is a weakening of the notion of isomorphism in definition 11. We essentially generalize the notion of semilinear isometry among the generator matrices of projective linear codes over  $\mathbb{F}_q$  [8] to that of weak isomorphism among the distinct representations of simple linear polymatroids.

**Definition 13.** *The mapping  $\sigma : \mathbb{F}_q^r \rightarrow \mathbb{F}_q^r$  is called semilinear if there exists an automorphism  $\alpha$  of  $\mathbb{F}_q$  such that for all  $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^r$  and all  $x \in \mathbb{F}_q$ , we have*

$$\sigma(\mathbf{u} + \mathbf{v}) = \sigma(\mathbf{u}) + \sigma(\mathbf{v}), \quad \sigma(x\mathbf{u}) = \alpha(x)\sigma(\mathbf{u}) \quad (15)$$

A semilinear isometry is a semilinear mapping that maps subspaces to subspaces. The set of all semilinear isometries forms a group known as the general semilinear group. Let  $GL(r, q)$  be the general linear group containing all  $r \times r$  invertible matrices over  $\mathbb{F}_q$  and let  $\text{Gal}(q)$  be the Galois group of  $\mathbb{F}_q$ .  $\text{Gal}(q)$  is a cyclic group of order  $t$  where  $q = p^t$  for a prime  $p$ , generated by the Frobenius automorphism  $x \mapsto x^p$ . Then the general semilinear group can be defined as follows.

**Definition 14.** *The semilinear isometries of  $\mathbb{F}_q^N$  form the general semilinear group,*

$$\Gamma L(r, q) \triangleq \{(\mathbb{A}, \alpha) \mid \mathbb{A} \in GL(r, q), \alpha \in \text{Gal}(q)\} \quad (16)$$

*The general semi-linear group  $\Gamma L(r, q)$  is the semidirect product  $GL(r, q) \rtimes \text{Gal}(q)$ . The identity element is the pair  $(\mathbb{I}_r, \text{id})$ , where  $\text{id}$  is the identity element in  $\text{Gal}(q)$ . The multiplication of two elements of  $\Gamma L(r, q)$  is given by,*

$$(\mathbb{A}_2, \alpha_2)(\mathbb{A}_1, \alpha_1) = (\mathbb{A} \cdot \alpha_2(\mathbb{A}_1), \alpha_2\alpha_1), \quad \forall (\mathbb{A}_1, \alpha_1), (\mathbb{A}_2, \alpha_2) \in \Gamma L(r, q) \quad (17)$$

$\Gamma L(r, q)$  acts naturally on  $\text{Gr}_q(r, k)$  as follows

$$\Gamma L(r, q) \times \text{Gr}_q(r, k) \rightarrow \text{Gr}_q(r, k) : ((\mathbb{A}, \alpha), \langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle) \mapsto \langle \alpha(\mathbf{v}_1)\mathbb{A}^t, \dots, \alpha(\mathbf{v}_k)\mathbb{A}^t \rangle \quad (18)$$

The subgroup of  $\Gamma L(r, q)$  that stabilizes each element of  $\text{Gr}_q(r, k)$  pointwise is  $\{(\mathbb{A}, \text{id}) \mid \mathbb{A} \in \mathcal{Z}_r\}$  where  $\mathcal{Z}_r$  is the center of  $GL(r, q)$ . This stabilizer is isomorphic to  $\mathcal{Z}_r$  itself. Hence,  $\Gamma L(r, q)$  induces the action of projective semilinear group given as,

$$P\Gamma L(r, q) \triangleq \Gamma L(r, q) / \mathcal{Z}_r. \quad (19)$$

on  $\text{Gr}_q(r, k)$ . The elements of  $P\Gamma L(r, q)$  are of the form  $(\mathbb{A}\mathcal{Z}_r, \alpha)$  for  $\mathbb{A} \in GL(r, q)$ . Furthermore, it can be expressed as the semidirect product

$$P\Gamma L(r, q) = PGL(r, q) \rtimes \text{Gal}(q). \quad (20)$$

The identity element is  $(\mathbb{I}_r\mathcal{Z}_r, \text{id})$  where  $\text{id}$  is the identity element in  $\text{Gal}(q)$ . The multiplication of two elements in  $P\Gamma L(r, q)$  is given as

$$(\mathbb{A}_2\mathcal{Z}_r, \alpha_2)(\mathbb{A}_1\mathcal{Z}_r, \alpha_1) = ((\mathbb{A}_2 \cdot \alpha_2(\mathbb{A}_1))\mathcal{Z}_r, \alpha_2\alpha_1) \quad (21)$$

The inverse element of  $(\mathbb{A}\mathcal{Z}_r, \alpha)$  is  $(\alpha^{-1}(\mathbb{A}))^{-1}\mathcal{Z}_r, \alpha^{-1}$ . The action of  $P\Gamma L(r, q)$  on  $\text{Gr}_q(r, k)$  is as follows

$$\gamma_k : P\Gamma L(r, q) \times \text{Gr}_q(r, k) \rightarrow \text{Gr}_q(r, k) : ((\mathbb{A}\mathcal{Z}_r, \alpha), \langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle) \mapsto \langle \alpha(\mathbf{v}_1)\mathbb{A}^t\mathcal{Z}_r, \dots, \alpha(\mathbf{v}_k)\mathbb{A}^t\mathcal{Z}_r \rangle \quad (22)$$

Let  $k(V)$  denote the dimension of a subspace  $V$ . The above action can be naturally extended to an action on  $\text{Gr}_q(r, K)$  which further induces an action on  $2^{\text{Gr}_q(r, K)}$  as,

$$\gamma' : P\Gamma L(r, q) \times 2^{\text{Gr}_q(r, K)} \rightarrow 2^{\text{Gr}_q(r, K)} : \{V_1, \dots, V_i\} \mapsto \{\gamma_{k(V_1)}(V_1), \dots, \gamma_{k(V_i)}(V_i)\} \quad (23)$$

for any subset of size  $i$  of  $\text{Gr}_q(r, K)$ . We shorten  $\gamma'(g, \{V_1, \dots, V_i\})$  as  $\{V_1, \dots, V_i\}g$ , for  $g \in P\Gamma L(r, q)$ . Given a collection  $K \subseteq [N]$  of distinct singleton ranks, let  $\mathcal{S}^q(N, r, K)$  be the set of polymatroid representations in  $\mathcal{P}^q(N, r, K, s)$  (described in §II-A) with  $s = N$  i.e. the representations associated with simple polymatroids. One can easily verify that this set is fixed setwise under the above action, as parameters  $N, r, K$  remain unchanged. We now define the notion of weak isomorphism.

**Definition 15.** (*Weak Isomorphism*) Two representations  $P_1 = \{V_1^1, \dots, V_N^1\}, P_2 = \{V_1^2, \dots, V_N^2\} \in \mathcal{S}_{N, r, K}^q$  are said to be weakly isomorphic if there exists a  $g \in P\Gamma L(r, q)$  s.t.

$$\{V_1^1, \dots, V_N^1\}g = \{V_1^2, \dots, V_N^2\} \quad (24)$$

denoted as  $P_1 \stackrel{W}{=} P_2$ .

**Lemma 3.** Let  $P_1, P_2 \in \mathcal{S}^q(N, r, K)$  be the representations of two simple  $\mathbb{F}_q$ -representable polymatroids s.t.  $P_1 \stackrel{W}{=} P_2$ . Then,  $P_1 \cong P_2$ .

The opposite of the above statement, however, is not true. It is possible for even the same  $\mathbb{F}_q$ -representable polymatroid can have several representations that are weakly non-isomorphic. The following example illustrates this phenomenon.

**Example 1.** Consider the following representations  $P_1, P_2 \in \mathcal{S}_{5, 5, \{2\}}^2$

$$P_1 \triangleq \left\{ \begin{array}{c} V_1 \quad V_2 \quad V_3 \quad V_4 \quad V_5 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \end{array} \right\} \quad (25)$$

$$P_2 \triangleq \left\{ \begin{array}{c} V'_1 \quad V'_2 \quad V'_3 \quad V'_4 \quad V'_5 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \end{array} \right\} \quad (26)$$

One can computationally verify that every isomorphism between  $P_1$  and  $P_2$  must map  $V_5$  to  $V'_5$  i.e. fix  $V_5$ . The subgroup of  $PGL(5, 2)$  that stabilizes  $V_5$  setwise contains matrices of the form  $\begin{bmatrix} A & \mathbb{O} \\ \mathbb{O} & B \end{bmatrix}$  where

$A \in PGL(2, 2)$  and  $B \in PGL(3, 2)$ . Hence, for  $P_1$  and  $P_2$  to be weakly isomorphic, we must have  $P_1 \stackrel{W}{=} P_2'$  (eq. (27),(28) ) i.e. there must exist a  $B \in PGL(3, 2)$  that maps  $P_1'$  to  $P_2'$ .

$$P_1' \triangleq \left\{ \begin{array}{c} W_1 \quad W_2 \quad W_3 \quad W_4 \\ \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix} \end{array} \right\} \quad (27)$$

$$P_2' \triangleq \left\{ \begin{array}{c} W_1' \quad W_2' \quad W_3' \quad W_4' \\ \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \end{array} \right\} \quad (28)$$

If such a  $B$  exists, then  $W_4^t B = W_i'^t$  for some  $i \in [4]$ . However, the row reduced echelon form of  $W_4^t$  differs from those of  $W_1'^t, \dots, W_4'^t$ , contradicting the fact that  $B \in PGL(3, 2)$ . Hence  $P_1 \stackrel{W}{\neq} P_2$ .

Because of the difficulty of isomorphism problems for graphs and their generalizations, some of methods to generate such objects are designed to outright avoid explicit isomorphism testing. The choice of isomorphism relation could be motivated by this issue, as we discuss in §V-B.

### C. Polymatroid extension and construction of all members of a class of codes

Polymatroid extension plays a central role in algorithms for exhaustive generation of polymatroids. It provides a means to construct polymatroids on ground set size  $i + 1$  from polymatroids on ground set size  $i$ . The following is a general definition of polymatroid extension which applies to arbitrary (not necessarily integer or representable) polymatroids.

**Definition 16.** A polymatroid  $(E', f')$  is said to be an extension of polymatroid  $(E, f)$  if  $E \subseteq E'$  and  $f'(\mathcal{S}) = f(\mathcal{S}) \forall \mathcal{S} \subseteq E$ . Furthermore, if  $|E' \setminus E| = t$  then  $(E', f')$  is said to be a  $t$ -extension of  $(E, f)$ .

If  $t$  is 1 and  $E' \setminus E = \{e\}$ , then we say that  $(E', f')$  is a 1-extension of  $(E, f)$  by an element  $e$ . The theory of unique 1-extensions for the special case of matroids was developed by Crapo [19] where he provided a method to construct all unique 1-extensions of a matroid. This method, along with explicit isomorphism testing was used by Blackburn et al. [9] to construct all non-isomorphic matroids on up to 8 elements. More recently Mayhew and Royle [41] constructed all matroids on 9 elements using the same method. Matsumoto et al. [39] extended Crapo's theory to avoid constructing isomorphic single element extensions and partially constructed matroids on 10 elements. Savitsky [51] generalized Crapo's method of producing unique 1-extensions of matroids to integer  $k$ -polymatroids, which are integer polymatroids with the rank of every singleton bounded above by  $k$  and generated a catalog of 2-polymatroids on up to 7 elements. Unfortunately, techniques described by Crapo et. al. [19] for matroids and Savitsky for [51] for  $k$ -polymatroids are far too general for our purpose. Matroid extensions followed by representability checking style algorithm has been proposed in e.g. [3], but has met with limited practical success for several reasons. Firstly, if  $(E, f)$  is a representable polymatroid, the extensions produced are not guaranteed to be representable, which means we must employ additional computation to find and weed out the ones that are non- representable. Secondly, these methods are only developed for polymatroids with specific sets of singleton ranks i.e.  $K_P = \{0, 1\}$  in case of Crapo et al.'s work and  $K_P = \{0, 1, \dots, k\}$  for some  $k \in \mathbb{N}$  in case of Savitsky's work. The third factor that discourages one from using such overly general techniques is the sheer rate at which number of general polymatroids or matroids grows as compared to their representable counterparts. For instance, in fig. 3 we can see the growth of number of all (non-isomorphic, integer valued) 2-polymatroids, all matroids, all ternary representable matroids and all binary representable matroids.

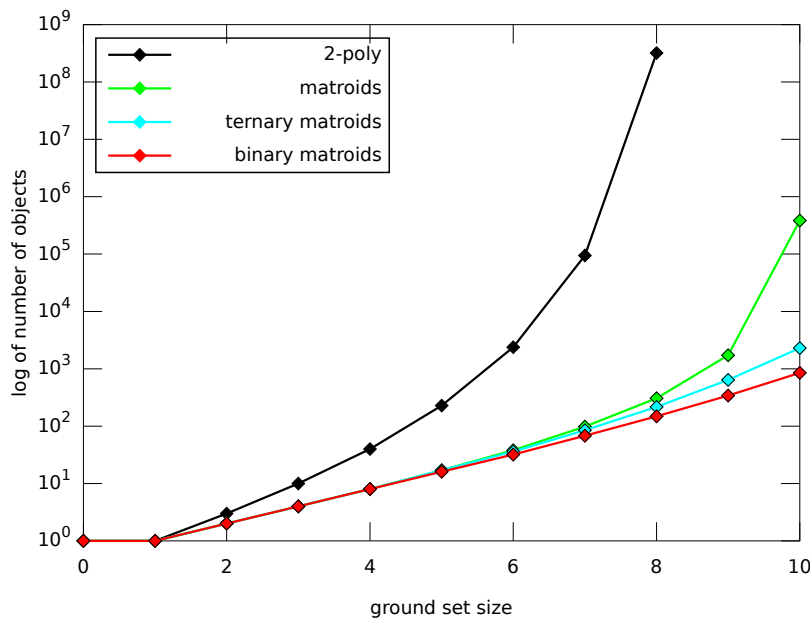


Figure 3: Log of number of all (non-isomorphic) 2-polymatroids [40], matroids [27], ternary matroids [38], and binary matroids [37], plotted against the ground set size

Bearing this in mind, we instead aim to enumerate representable polymatroids directly exclusively, and hence, we define a notion of extension for a polymatroid which we choose to use over the more general notion in def. 16, as it conveniently refers directly to the representation of the polymatroid.

**Definition 17.** Let  $P$  be a polymatroid in  $\mathcal{P}^q(i, (r, r), K, (0, i))$  represented as  $\{V_1, \dots, V_i\}$ . Then, a 1-extension of  $P$  is any polymatroid  $P'$  represented as  $\{V_1, \dots, V_i, V_{i+1}\}$  where  $V_{i+1} \in \mathbf{Gr}_q(r, K)$ .

Note that the above definition augments a polymatroid made up of a multiset of subspaces of  $\mathbb{F}_q^r$  by adding another subspace of  $\mathbb{F}_q^r$  to the multiset, thus keeping the underlying vector space dimension  $r$  as a constant. We further classify 1-extensions into two types: simple 1-extensions and a non-simple 1-extensions. A 1-extension is simple if  $|\mathbf{us}(P')| = |\mathbf{us}(P)| + 1$  and non-simple otherwise. For an extension to be simple,  $V_{i+1}$  must be distinct from each of  $V_1, \dots, V_i$ . On the other hand, an extension is non-simple if and only if  $V_{i+1}$  is a copy of one of  $V_1, \dots, V_i$  or it is an empty subspace with  $f(i+1) = 0$ .

Now we describe our basic strategy for constructing all polymatroids in  $\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u))$  up to some notion of equivalence  $\equiv$ . A basic assumption about  $\equiv$  is that for polymatroids belonging to the same equivalence class under  $\equiv$ , the parameters  $N, r, K$  and  $|\mathbf{us}(P)|$  are identical, which is indeed the case with both strong and weak isomorphism relations discussed in IV-B. We also assume that we have access to procedures  $\mathbf{se}(\cdot)$  and  $\mathbf{nse}(\cdot)$  which take as input a list of  $\equiv$ -inequivalent polymatroid representations and produce a list of  $\equiv$ -inequivalent simple and non-simple 1-extensions respectively. We defer the discussion of low-level details of how these procedures work in practice to the next section, where we point out several techniques in literature that can be used to implement such procedures. Fig. 4 describes how one can use procedures  $\mathbf{se}(\cdot)$  and  $\mathbf{nse}(\cdot)$  to construct all members of  $\mathcal{P}^q(N, (r, r), K, (s_l, s_u))$  up to an equivalence relation  $\equiv$ . This strategy can be used repeatedly for different values of  $r$  s.t.  $r_l \leq r \leq r_u$  to construct all members of  $\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u))$  up to  $\equiv$ . While our goal in this paper is to solve variants of  $\text{CLRP}_q$ , the strategy described in Fig. 4 can be used to construct inner bounds  $\Gamma_N^{\mathcal{P}^q(c)}$ , which might be of interest in their own right.

#### D. An augmentation operation for $p\mathcal{L}$ -polymatroids

We now describe the construction of all  $p\mathcal{L}$ -polymatroids of size  $i+1$  from non-isomorphic  $p\mathcal{L}$ -polymatroids of size  $i < N$  by combining linear 1-extension of  $p\mathcal{L}$ -polymatroids and extension of the



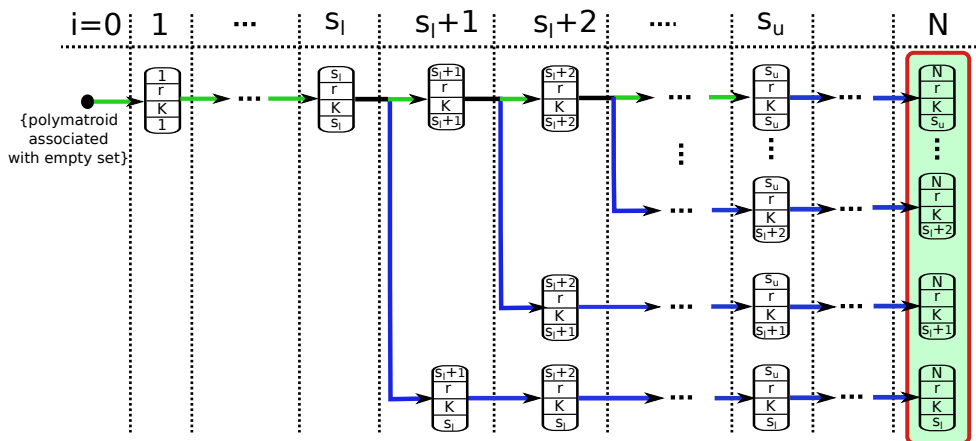


Figure 4: Construction of  $\equiv$ -inequivalent polymatroid representations belonging to the class  $\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u))$ , for some  $r_l \leq r \leq r_u$ . The green arrows indicate the use of simple extensions  $se(\cdot)$  while blue arrows indicate the use of non-simple extensions  $nse(\cdot)$ . Each box itself corresponds to a particular class of codes. The parameters specified from top to bottom are: 1) size or length  $i$ , dimension  $r$  of vector space over  $\mathbb{F}_q$  whose subspaces are used to build each polymatroid in the class, 3) set  $K$  of distinct singleton ranks, and 4)  $|us(P)|$  for each polymatroid  $P$  in the class.

associated partial maps. In the background setting provided by the strategy described in Fig. 4, to generate linear  $p\mathcal{I}$ -polymatroids, the basic problem we must be able to solve is that of determining if a given polymatroid is a  $p\mathcal{I}$ -polymatroid:

- [X1] For a collection of constraints  $\mathcal{I}$  of size  $N$ , given a polymatroid  $P = ([i], f)$ ,  $i \leq N$ , determine if  $P$  is a  $p\mathcal{I}$ -polymatroid.

In order to settle [X1], we must look for a  $p$ -map  $\phi$  under which  $P$  satisfies  $\mathcal{I}$ . If we are successful in finding a certificate  $p$ -map  $\phi$  showing that  $P$  is a  $p\mathcal{I}$ -polymatroid, we decide to keep  $P$ . Otherwise we reject  $P$  and all its  $t$ -extensions from contention.

Problem [X1] can be solved by using a backtracking approach. To see how, consider set of all possible  $p$ -maps  $\Omega_p$ , ordered using the lexicographic order described as follows. Let  $\delta$  be the map  $\{1 \mapsto i_1, \dots, |\delta| \mapsto i_{|\delta|}\}$  and  $\gamma$  be the map  $\{1 \mapsto j_1, \dots, |\gamma| \mapsto j_{|\gamma|}\}$  where  $|\delta|$  and  $|\gamma|$  denote the size of the domain of  $\delta$  and  $\gamma$  respectively with  $i_k \in [N], \forall k \in [|\delta|]$  and  $j_k \in [N], \forall k \in [|\gamma|]$ . Denote the ordinary lexicographic (dictionary) order on tuples of length  $\leq N$  with elements from  $[N]$  as  $\overset{L}{<}$ , then this ordering is directly extendable to partial maps as follows.

**Definition 18.** Let  $\delta, \gamma \in \Omega_p$  be distinct  $p\mathcal{I}$ -maps. Then  $\delta$  is smaller than  $\gamma$  if  $(i_t)_{t=1}^{|\delta|} \overset{L}{<} (j_t)_{t=1}^{|\gamma|}$ .

We now define the  $p$ -map tree which is a directed tree whose vertices are  $p$ -maps and the edges are defined using the notion of an extension of a  $p$ -map.

**Definition 19.** A  $p$ -map  $\delta' : [i+1] \rightarrow [N]$  is said to be an extension of a  $p$ -map  $\delta : [i] \rightarrow [N]$  if  $i < N$  and  $\delta(k) = \delta'(k), \forall k \in [i]$ .

We say that the  $p$ -map  $\delta$  in the above definition is a deletion of  $p$ -map  $\delta'$ . The  $p$ -map tree of order  $N$  is a directed graph  $T_N = (V_N, E_N)$  where  $V_n$  is the set of all  $p$ -maps and  $(u, v) \in E$  if  $v$  is an extension of  $u$ . Note that  $p$ -map extension and deletion provide a means to traverse the  $p$ -map tree in lexicographic order. Furthermore, given a vertex  $u$  (a  $p$ -map) in the tree, one can resume the traversal to produce all  $p$ -maps that are lexicographically greater than  $u$ . Given a  $p$ -map  $\delta = \langle i_1, \dots, i_k \rangle$  at depth  $k < N$  in the  $p$ -map tree  $T_N$ , its immediate descendants can be computed as  $\langle i_1, \dots, i_k, j \rangle$  where  $j \in [N] \setminus \{i_1, \dots, i_k\}$  and can be visited in lexicographical order. The parent of  $\delta$  can be obtained by deleting  $i_k$ . Thus, we need not explicitly store the  $p$ -map tree in order to traverse it.

One merit of considering the lexicographic ordering of  $p$ -maps and thinking of the collection of all such  $p$ -maps as a tree ordered under this ordering is that it allows the problem of finding a  $p$ -map, or lack

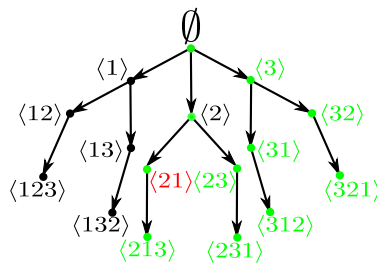


Figure 5: The  $p$ -map tree  $T_3$  with the subtree  $T_3^{>(21)}$ . For a collection of constraints  $\mathcal{I}$  of size 3, let a size 2 polymatroid  $(E, f)$  be a  $p\mathcal{I}$ -polymatroid with  $p\mathcal{I}$ -map  $\{1 \mapsto 2, 2 \mapsto 1\}$  (shown in red), and let  $(E', f')$  be its 1-extension. Then we need only traverse the vertices shown in green in worst case to determine if  $(E', f')$  is also a  $p\mathcal{I}$ -polymatroid.

of existence thereof, to be posed as a tree search algorithm. One way to solve [X1] is to traverse  $T_N$  in a depth first manner to depth  $i$ , while testing constraints  $\mathcal{I}(\delta([j+1])) - \mathcal{I}(\delta([j]))$  at each node associated with a  $p$ -map  $\delta$  at depth  $j$ ,  $j \leq i$ . In this instance, what is meant by depth first is that one extends a partial map adding mapped elements one by one until it is no longer possible to satisfy the constraints  $\mathcal{I}$  using it, i.e., until all 1 extensions of the partial map no longer obey the constraints. At that time, a backtracking step deletes the most recent extension, and the partial map extension process continues. If ever a complete traversal to depth  $i$  succeeds, then a  $p$ -map of size  $i$  has been found, and provides a certificate showing that [X1] has been solved and that  $P = ([i], f)$  is a  $p\mathcal{I}$ -polymatroid. Conversely, if the entire tree is exhausted, i.e. the algorithm terminates with no more backtracks or extensions possible, then [X1] has been answered in the negative. Of course, our primary interest in this manuscript is the construction of polymatroids with rank functions obeying a series of linear constraints through an extension process i.e. we would like be able to use the strategy in Fig. 4 while at the same time maintaining only those polymatroids that are  $p\mathcal{I}$ -feasible. The tree structure of the set of  $p$ -maps is also beneficial in this extension process. In particular, consider a  $p\mathcal{I}$ -polymatroid  $P = ([i], f)$  of size  $i < N$  with a  $p$ -map  $\phi$ , and let  $P' = ([i+1], f)$  be a 1-extension of  $P$ . Then, the  $p\mathcal{I}$ -polymatroid extension process must solve the following problem at each step.

- [X2] Determine if  $P' = ([i+1], f)$ , the 1-extension of a  $p\mathcal{I}$ -polymatroid  $P = ([i], f)$  with lexicographically minimum  $p$ -map  $\phi$ , is a  $p\mathcal{I}$ -polymatroid, and if so, find its lexicographically minimum  $p$ -map.

That is, we must determine if there exists a  $p$ -map  $\phi'$  for  $P'$  s.t. it is a  $p\mathcal{I}$ -polymatroid. Given  $\phi$ , we can use the following lemma to traverse only a subtree of  $T_N$  for determining if  $P'$  is a  $p\mathcal{I}$ -polymatroid.

**Lemma 4.** *Let  $P$  be a  $p\mathcal{I}$ -polymatroid with  $\phi$  being the lexicographically smallest  $p$ -map associated with it and let  $P'$  be a 1-extension of  $P$ . If  $P'$  is a  $p\mathcal{I}$ -polymatroid with  $\phi'$  being the  $p$ -map associated with it, then  $\phi' \stackrel{L}{>} \phi$ .*

This lemma shows that we can determine whether the polymatroid 1-extension  $P'$  is a  $p\mathcal{I}$ -polymatroid by traversing the  $p$ -map tree in depth-first fashion, resuming the tree traversal from  $\phi$ . Let  $V_i^{>\delta}$  be the set of all  $p$ -maps that are lexicographically greater than  $\delta$  and  $\hat{V}_i^\delta$  be the set of all ancestors of  $\delta$ . Denote by  $T_i(\delta)$  to be the subgraph of  $T_i$  induced by vertices  $V_i^{>\delta} \cup \hat{V}_i^\delta$  and the vertices. Hence, it suffices to traverse  $T_i(\delta)$  to settle [X2].

### E. Exploiting symmetry when augmenting $p\mathcal{I}$ -polymatroids

In many instances, depending on the low level techniques used for implementing procedures  $\mathbf{se}(\cdot)$  and  $\mathbf{nse}(\cdot)$ , either a symmetry group of the polymatroid  $P = ([i], f)$  at the current step of the polymatroid extension process, or a symmetry group of the constraints  $\mathcal{I}$  or both might be known. Knowledge of these groups can further reduce the amount of computation required in searching for  $p$ -maps in problem [X2].

In particular, we can assume that the symmetries of  $P = ([i], f)$  are specified as a group  $A \leq S_i$  where  $S_i$  is the group of all permutations of  $[i]$ : so that for each permutation  $a \in A$  and for each set  $\mathcal{E} \subseteq [i]$ ,  $f(a(\mathcal{E})) = f(\mathcal{E})$ . Similarly, the symmetries of  $\mathcal{I}$  are provided as a group  $B \leq S_N$  where  $S_N$  is the group of all permutations of  $[N]$ : for each element  $b \in B$ , if  $([N], f')$  is  $p\mathcal{I}$ -polymatroid, then so is  $([N], f' \circ b)$ . Together, as each putative partial map for  $P = ([i], f)$  is an injective map  $\phi : [i] \rightarrow [N]$ , the direct product  $A \times B$  acts on a putative partial map  $\phi$  via  $((a, b), \phi) \mapsto b(\phi(a(\cdot)))$ . When attempting to search for a  $p$ -map, then, one only needs to consider single representatives from the equivalence class created on the  $p$ -maps under this group action.

Formally, the associated problem can be stated as follows.

- [X3] Given symmetry groups  $A, B$  determine if  $P$  is a  $p\mathcal{I}$ -polymatroid.

At depth  $j \leq i$  in  $T_N$ , denote by  $A_{[j]}$  the subgroup of  $A$  that stabilizes  $[j]$  set-wise. We now consider the action of the direct product  $G_{[j]} \triangleq A_{[j]} \times B \leq A \times B$  on  $V_j$  which is the set of vertices of  $T_N$  at depth  $j \leq i$ . The composition in  $G_{[j]}$  is denoted as  $((a_1, b_1) * (a_2, b_2)) = (a_1 a_2, b_2 b_1)$ . One can see that  $((a_1 a_2, b_2 b_1) \delta)(x) = b_1 b_2 \delta(x(a_1 a_2)) = b_1(b_2 \delta(x a_1)) = b_1((a_2, b_2) f)(x a_1) = (a_1, b_2)((a_2, b_2) f)(x)$  for any  $x \in [j], j \leq i$  where  $[j]$  is the domain of  $p$ -map  $\delta$ . Let  $V_j^*$  be the transversal of orbits in  $V_j$  under the aforementioned action formed by choosing the lexicographically smallest  $p$ -map from each orbit. Let  $T_i^*$  be the subgraph of  $T_i$  induced by  $\cup_{j \leq i} V_j^*$ .

**Lemma 5.** *It suffices to traverse  $T_i^*$  instead of  $T_i$  to determine if  $P = ([i], f)$  is a  $p\mathcal{I}$ -polymatroid.*

**Example 2.** Consider the HMSNC instance shown in fig. 6. Let the associated constraints be  $\mathcal{I}$ . This network has a symmetry group of order 2 generated by permutations  $\{(3,4)\}$ . The polymatroid  $\{V_1, V_2, V_3\}$  in (29) is a  $p\mathcal{I}$ -polymatroid obtained via extending  $p\mathcal{I}$ -polymatroids  $P_1 = \{V_1\}$  and  $P_2 = \{V_1, V_2\}$ , in that order. Fig. 7 shows how the knowledge of network symmetry group, along with symmetries of the polymatroids  $P_i$  can be used to traverse only a subset of the vertices of the  $p$ -map tree when determining their  $p\mathcal{I}$  feasibility.

$$P_3 \triangleq \left\{ \begin{array}{c} V_1 \\ \left[ \begin{array}{cc} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{array} \right], \\ \left[ \begin{array}{cc} V_2 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{array} \right], \\ \left[ \begin{array}{cc} V_3 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{array} \right] \end{array} \right\} \quad (29)$$

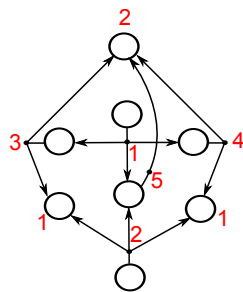


Figure 6: A HMSNC instance with  $N = 5$ . The symmetry group  $A$  of this instance is of order 2 generated by  $\{(3, 4)\}$ .

Problems [X1]-[X3] can be combined to form problem [X4] below:

- [X4] Determine if  $P' = ([i+1], f)$  is a  $p\mathcal{I}$ -polymatroid given symmetry groups  $A, B$  and the  $p$ -map  $\phi$  associated with  $p\mathcal{I}$ -polymatroid  $P = ([i], f)$  where  $P'$  is a 1-extension of  $P$ .

The above problem can be solved by combining the approaches to [X1]-[X3] i.e. it suffices to traverse  $T_{i+1}^*(\phi)$ , where, using induction on  $i$ , we assume that  $\phi$  is part of  $T_{i+1}^*$ .

The functionality of  $p$ -map extension, for generation of  $\mathcal{I}$ -polymatroids, is provided by the procedure `extend_pmap( $P', \mathbf{pc}, G$ )` that accepts a 1-extension  $P'$  of a  $p\mathcal{I}$ -polymatroid  $P$ , the  $p$ -map  $\mathbf{pc}$  and a group  $G$  of symmetries of  $\mathbf{us}(P')$ . Note that symmetries of  $P'$  can be directly deduced from those of  $\mathbf{us}(P')$ .

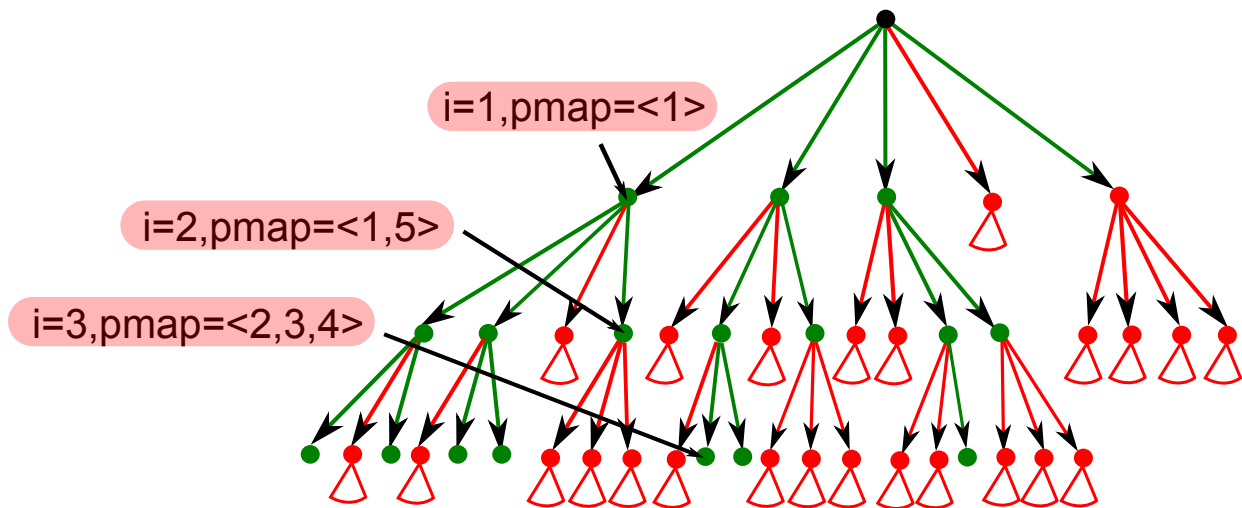


Figure 7: The nested  $p$ -map trees  $T_i$ ,  $i \leq 3$  for HMSNC instance in fig. 6. The subtrees  $T_i^*$  are shown in green. Each  $T_i^*$  is the subgraph of  $T_i$  induced by vertices associated  $p$ -maps that are with lexicographically smallest in their respective orbits under the the action of  $A \times B$  where  $B$  is the trivial group for  $i = 1$ , and is generated by  $\{(1, 2)\}, \{(1, 2), (1, 3, 2)\}$  for  $i = 2, 3$  respectively. The vertices at every level are drawn in lexicographic order (ascending from left to right).

If  $P'$  is indeed a  $p\mathcal{L}$ -polymatroid, then it returns a  $p$ -map  $\mathbf{c}$  associated with  $P'$  s.t.  $\mathbf{c} \stackrel{L}{>} \rho\mathbf{c}$  which serves as a certificate. Otherwise, it returns empty  $p$ -map, denoted as  $\phi_{\text{null}}$ . Note that  $p$ -map  $\mathbf{c}$  produced in this manner will itself be the lexicographically smallest such map associated with  $P'$ .

## V. AN ALGORITHM FOR SOLVING $\text{CLRP}_q\text{-EN}$

In this section, we build on various concepts described in previous section, to provide the high level description of an algorithm to solve  $\text{CLRP}_q\text{-EN}$  via exhaustive generation of  $p\mathcal{L}$ -polymatroids up to equivalence relation  $\equiv$ . The description is generic enough so that  $\equiv$  can be interpreted as either strong or weak isomorphism. We also discuss how procedures  $\text{se}(\cdot)$  and  $\text{nse}(\cdot)$  could be implemented in §V-B.

### A. High-level description of the algorithm

In §IV-C we discussed how to generate all members of a class of codes  $\mathcal{P}^q(\mathbf{c})$  up to an equivalence relation  $\equiv$ . We intend to use fig. 4 as a template for generating  $p\mathcal{L}$ -polymatroids. To that end, we establish some facts about the property of  $p\mathcal{L}$ -feasibility, that allow us to restrict the strategy in fig 4 to  $p\mathcal{L}$ -polymatroids only. The two main facts that help us achieve this are the *inheritedness* and *isomorph-invariance* of the property of  $p\mathcal{L}$ -feasibility.

**Definition 20.** A property  $\chi$  of polymatroids is said to be inherited if a polymatroid  $P$  has  $\chi$  then all polymatroids obtained from  $\mathcal{P}$  via deletion of ground set elements also have  $\chi$ .

Let  $P$  be a  $p\mathcal{L}$ -polymatroid with associated  $p$ -map  $\phi$ . One can form a  $p$ -map for polymatroid  $P'$  obtained by deletion from  $P$  by simply deleting mappings associated with deleted ground set elements. Such a  $p$ -map serves as a certificate of  $p\mathcal{L}$ -feasibility of  $P'$ , thus showing that property of  $p\mathcal{L}$ -feasibility is inherited. As an implication, every  $p\mathcal{L}$ -polymatroid of size  $i$  can be obtained via polymatroid extension and  $p$ -map extension from some  $p\mathcal{L}$ -polymatroid on ground set of size  $i - 1$ .

**Definition 21.** A property  $\chi$  of polymatroids is said to be  $\equiv$ -invariant wrt equivalence relation  $\equiv$ , if a polymatroid  $P$  has  $\chi$ , then all polymatroids equivalent to it under  $\chi$  also have  $\chi$ .

For both equivalence relations  $\cong$  and  $\stackrel{W}{\equiv}$  discussed in this work, members of the same equivalence class have the same rank function up to a permutation of the ground set. Hence,  $p\mathcal{L}$ -feasibility is both  $\cong$ -invariant and  $\stackrel{W}{\equiv}$ -invariant, as given a certificate  $\phi$  of  $p\mathcal{L}$ -feasibility of one member of the equivalence class,

we can construct such a certificate for every member of the said equivalence class, simply by applying an appropriate permutation to the domain of  $\phi$ . Fig. 8 describes our algorithm to solve  $\text{CLRP}_q\text{-EN}$ . This

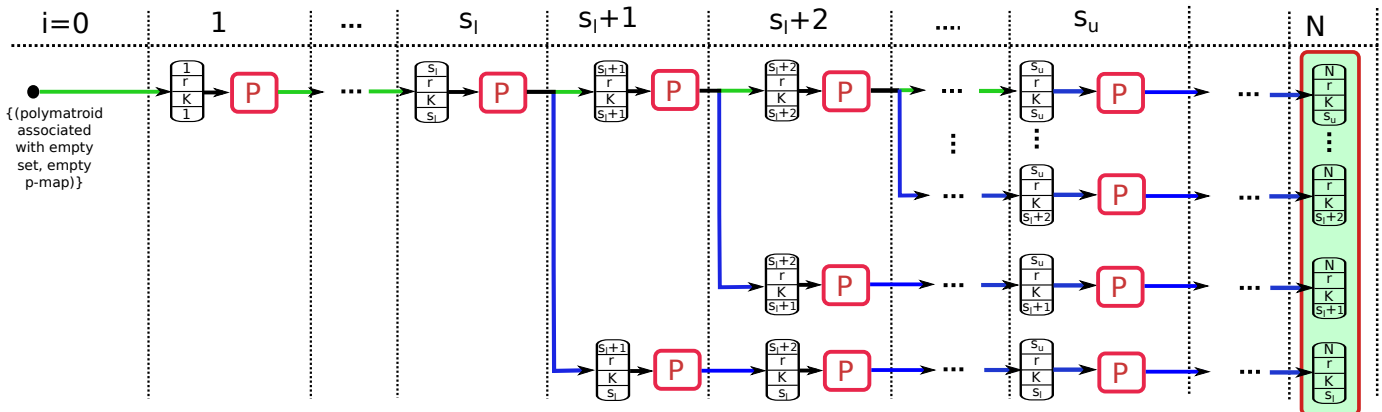


Figure 8: Construction of  $\equiv$ -inequivalent  $p\mathcal{L}$ -polymatroids belonging to the class  $\mathcal{P}^q(N, (r_l, r_u), K, (s_l, s_u))$ , for some  $r_l \leq r \leq r_u$ . The green arrows indicate the use of simple extensions  $\text{se}(\cdot)$  while blue arrows indicate the use of non-simple extensions  $\text{nse}(\cdot)$ . Each box itself corresponds to polymatroids belonging a particular class of codes. The parameters specified from top to bottom are: 1) size or length  $i$ , dimension  $r$  of vector space over  $\mathbb{F}_q$  whose subspaces are used to build each polymatroid in the class, 3) set  $K$  of distinct singleton ranks, and 4)  $\text{us}(P)$  for each polymatroid  $P$  in the class. The red box labeled  $P$  corresponds to procedure  $\text{extend\_pmap}(\cdot)$  that extends  $p$ -maps of the parents of polymatroids to find certificates of  $p\mathcal{L}$ -feasibility while filters out polymatroids for which no such extension exists.

is obtained essentially by adding the functionality of  $p$ -map extension to the strategy described in fig. 4. Any polymatroids that are found to be not  $p\mathcal{L}$ -feasible are filtered out, a convenient feature is made possible by inheriteness and isomorph-invariance of the property of  $p\mathcal{L}$ -feasibility.

### B. Low-level details: simple and non-simple polymatroid extensions

This section is concerned with the implementation of procedures  $\text{se}(\cdot)$  and  $\text{nse}(\cdot)$ . The two main aspects one must pay attention to are: a) the construction of *distinct* 1-extensions of a polymatroid and b) isomorph rejection. In case of  $\text{se}(\cdot)$ , we are given a list of  $\equiv$ -inequivalent polymatroids belonging to a class  $\mathcal{P}^q(i-1, (r, r), K, (s, s))$  and we want to construct a list of  $\equiv$ -inequivalent 1-extensions belonging to a class  $\mathcal{P}^q(i, (r, r), K, (s+1, s+1))$ . The exact techniques used will depend heavily on the choice of  $\equiv$ . There are techniques in literature that allow the construction of distinct 1-extensions linear extensions for  $K = \{0, 1\}$ , i.e. the case of  $\mathbb{F}_q$ -representable matroids. These procedures use *chains* of a matroid and are implemented in `sage-matroid` package of SageMath [46]. Isomorph rejection via pairwise isomorphism testing is then employed to reject strongly isomorphic 1-extensions. Note that approach using the chains of a matroid can also be extended to procedure  $\text{nse}(\cdot)$ .

An alternative approach, which allows arbitrary sets  $K$  of singleton ranks (and hence, to representably polymatroids as opposed to only representable matroids) is based on Leiterspiel, or the algorithm of snakes and ladders. This is a very general approach, designed for determining representatives of the orbits under action of a group  $G$  in the power set  $2^{\mathcal{X}}$  of a set  $\mathcal{X}$ . It can be used for generating any combinatorial objects that can be described as subsets of a set up to an equivalence relation that arises from the orbits of a group action on the set in question. It was first described in a purely group-theoretic language by Schmalz [52], whereas an interpretation more suitable to combinatorial generation can be found in [8]. Each member of  $\mathcal{P}^q(i, (r, r), K, (s+1, s+1))$  can be described as an  $i$ -subset of  $\text{Gr}_q(r, K)$ . Furthermore, weak isomorphism is in fact defined via a group action on  $\text{Gr}_q(r, K)$ , as seen in §IV-B. To authors' knowledge, weak isomorphism is maximal amongst all equivalence relations that can be

defined via a group action on  $\text{Gr}(q, K)$ , in a terms of coarseness of the partition induced on subsets of size  $i$  of  $\text{Gr}_q(r, K)$ . In exchange for weakness of the isomorphism relation, Leiterspiel allows us avoid explicit pairwise isomorphism testing along with providing access to subgroups of automorphism groups of polymatroids, which are constructed naturally in the process. These symmetries of polymatroids can be used in the determination of  $p\mathcal{I}$ -feasibility as described in §IV-E. Owing to its generality, and other advantages, the implementation ITAP accompanying this article uses Leiterspiel for the procedure  $\text{se}(\cdot)$ .

Next, for implementing the procedure  $\text{nse}$ , one can first form all distinct  $|\text{us}(P)|$  non-simple 1-extensions of each polymatroid  $P$  in the input list and resort to pairwise isomorphism testing with respect to the chosen equivalence relation. Note that lemma 2, dictates how explicit strong isomorphism testing for two polymatroids  $P_1$  and  $P_2$  with  $\text{us}(P_1) = \text{us}(P_2)$  can be performed. The statement of lemma 2 can be modified when one is interested in weak isomorphism testing, by substituting words 'weak' for 'strong' and by restring the meaning of automorphism group to be a subgroup of appropriate projective semilinear group. On the flipside, if we know beforehand that  $\text{us}(P_1) \neq \text{us}(P_2)$ , we can directly conclude that  $P_1 \not\cong P_2$  (alternatively,  $P_1 \stackrel{W}{\neq} P_2$ ). This allows us to restrict the explicit isomorphism testing to only the polymatroids with the same underlying simple polymatroid. Note that if Leiterspiel is used to construct simple polymatroids (as is done in ITAP), we have access to the automorphism group w.r.t. weak isomorphism of every simple polymatroid we construct. This gives us a head start in the application of lemma 2 as we are already aware of the automorphism group of  $\text{us}(P_1)$  ( $= \text{us}(P_2)$ ) w.r.t weak isomorphism, while we have a subgroup of automorphism group w.r.t. strong isomorphism.

When we are solving  $\text{CLRP}_q\text{-EN}$  to compute achievable network coding rate regions, we can also use a hybrid approach of switching between isomorphism relations, which is implemented in ITAP. This approach uses Leiterspiel to perform simple extensions (green arrows in the first horizontal level in Fig. 8) and uses explicit isomorph testing w.r.t strong isomorphism relation when performing non-simple extensions (blue arrows in Fig. 8). In this case the automorphism groups provided by Leiterspiel can be used in explicit strong isomorphism testing. This hybrid technique ultimately answers  $\text{CLRP}_q\text{-EN}$  with the strong isomorphism (i.e. equality of polymatroid rank vectors) notion of equivalence, even though intermediate stages – the simple extensions – make use of weak isomorphism equivalence relations. This approach suffices for computing the achievable rate regions, because all rate vectors achievable with codes in  $\mathcal{P}^q(\mathbf{c})$  can be obtained from the set of all strongly non-isomorphic  $p\mathcal{I}$ -polymatroids in  $\mathcal{P}^q(\mathbf{c})$ .

Algorithm 1 provides a detailed description of how to implement the general strategy in fig. 8. It closely matches our implementation in ITAP. We assume that we are given a collection of constraints  $\mathcal{I}$ , size of finite field  $q$ , and a class tuple  $\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$ . Algorithm 1 describes the construction for a specific  $r_l \leq r \leq r_u$ . The output is the a list of all weakly non-isomorphic  $\mathcal{I}$ -polymatroids in  $\mathcal{P}^q(N, (r, r), K, (s_l, s_u))$ . A list of weakly non-isomorphic polymatroids is denoted as  $\mathfrak{P}_{i,j}$ , where  $i$  is the size of polymatroids in the list and  $j$  is the size of underlying simple polymatroid of every polymatroid in the list. At the  $i$ th iteration of the algorithm, a collection of such lists of polymatroids of size  $i$  are created from a collection of lists of polymatroids of size  $i - 1$ . For every list  $\mathfrak{P}_{i,j}$ , a certificate map  $\text{cert}_{i,j}$  is also maintained, which maps members of  $\mathfrak{P}_{i,j}$  to the vertices of the  $p$ -map tree  $T_i$  at depth  $i$ , that correspond to the certificates of  $p\mathcal{I}$ -feasibility. The procedure  $\text{leiterspiel}(\cdot)$  (line 4) refers to the Leiterspiel algorithm as described in [8] (Algorithm 9.6.10), which serves as a concrete implementation of procedure  $\text{se}(\cdot)$ , which we mentioned previously, without giving any internal details (green arrows in fig. 8). The input to this procedure is the orbits datastructure, consisting of a list  $\mathfrak{P}_{i,i}$  for some  $1 \leq i \leq N$ , stabilizer map  $\sigma_{i,i}$  and the transporter map  $\varphi_{i,i}$ . The stabilizer map  $\sigma_{i,i}$  maps the members of  $\mathfrak{P}_{i,i}$  to subgroups of  $PGL(r, q)$  that are their automorphism groups. The transporter map  $\varphi_{i,i}$  maps a subset of size  $i$  of  $\text{Gr}_q(r, K)$  that is a  $p\mathcal{I}$ -polymatroid to the representative of its weak isomorphism class present in the list  $\mathfrak{P}_{i,i}$ . The procedure  $\text{pmapfilter}(\cdot)$  in lines 5,9 and 15 corresponds to the red boxes in fig 8. The input to this procedure is a list of polymatroids  $\mathfrak{P}_{i,j}$ , the associated certificate map  $\text{cert}_{i,j}$  and the stabilizer map  $\sigma_{j,j}$  which maps the underlying simple polymatroids of members of  $\mathfrak{P}_{i,j}$  to the respective stabilizers. It uses  $\text{extend\_pmap}(\cdot)$  (line 3) to extend the certificate  $p$ -map of the parent polymatroid obtained using function



**Input:**  $\mathcal{I}$ , a prime power  $q$ ,  $\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$  and vector space dimension  $r$

**Output:** Lists  $\mathfrak{P}_{N,s}$ ,  $s_l \leq s \leq s_u$  of codes in  $\mathcal{P}^q(\mathbf{c})$  and respective certificate maps

$$\text{cert}_{N,s} : \mathfrak{P}_{N,s} \rightarrow T_N$$

```

1  $\mathfrak{P}_{0,0} \leftarrow \{P_{\text{null}}\}$ 
2  $\text{cert}_{0,0}(P_{\text{null}}) \leftarrow \phi_{\text{null}}$ 
3 for  $1 \leq i \leq s_u$  do
4    $(\mathfrak{P}_{i,i}, \sigma_{i,i}, \varphi_{i,i}) \leftarrow \text{leiterspiel}(\mathfrak{P}_{i-1,i-1}, \sigma_{i-1,i-1}, \varphi_{i-1,i-1})$ 
5    $(\mathfrak{P}_{i,i}, \text{cert}_{i,i}) \leftarrow \text{pmapfilter}(P_{i,i}, \text{cert}_{i-1,i-1}, \sigma_{i-1,i-1})$ 
6   if  $i \geq s_l + 1$  then
7     for  $s_l \leq j \leq i - 1$  do
8        $\mathfrak{P}_{i,j} \leftarrow \text{nse}(\mathfrak{P}_{i-1,j})$ 
9        $(\mathfrak{P}_{i,j}, \text{cert}_{i,j}) \leftarrow \text{pmapfilter}(P_{i,j}, \text{cert}_{i-1,j}, \sigma_{j,j})$ 
10    end
11  end
12  for  $s_u + 1 \leq i \leq N$  do
13    for  $s_l \leq j \leq s_u$  do
14       $\mathfrak{P}_{i,j} \leftarrow \text{nse}(\mathfrak{P}_{i-1,j})$ 
15       $(\mathfrak{P}_{i,j}, \text{cert}_{i,j}) \leftarrow \text{pmapfilter}(P_{i,j}, \text{cert}_{i-1,j}, \sigma_{j,j})$ 
16    end
17  end
18 end
19 return  $\{\mathfrak{P}_{N,s_l}, \dots, \mathfrak{P}_{N,s_u}\}, \{\text{cert}_{N,s_l}, \dots, \text{cert}_{N,s_u}\}$ 

```

**Algorithm 1:** An algorithm to solve  $\text{CLRP}_q\text{-EN}$  as implemented in ITAP

$\text{parent}(\cdot)$ , and rejects any polymatroids for which no such extension exists. Note that  $\text{extend\_pmap}(\cdot)$  also takes the stabilizer subgroup of the underlying simple polymatroid of the polymatroid being tested, in order to exploit symmetry as described in §IV-E. Note that Leiterspiel, as described in [8], allows one to reject some of the generated objects if they do not satisfy an *inherited test function*, which is an indicator function for a any inherited property of the objects being generated. Hence, in actual implementation, rejection of polymatroids that are not  $p\mathcal{I}$ -feasible in line 5 is performed naturally in procedure leiterspiel( $\cdot$ ) itself. The procedure nse( $\cdot$ ) (lines 8 and 14) takes as input a list of polymatroids and outputs all strongly non-isomorphic non-simple extensions of the polymatroids in the list. For each polymatroid in the input list, it constructs all non-simple extensions (line 4 of nse) and rejects isomorphs using explicit strong isomorphism testing for polymatroids with identical underlying simple polymatroid (line 8 of nse).

```

1  $\mathfrak{P}' \leftarrow \emptyset$ 
2 for  $P \in \mathfrak{P}$  do
3    $\phi \leftarrow \text{extend\_pmap}(P, \text{cert}(\text{parent}(P)), \sigma(\text{us}(P)))$ 
4   if  $\phi \neq \phi_{\text{null}}$  then
5      $\mathfrak{P}' \leftarrow \mathfrak{P}' \cup \{P\}$ 
6      $\text{cert}'(P) \leftarrow \phi$ 
7   end
8 end
9 return  $\mathfrak{P}', \text{cert}'$ 

```

**Procedure**  $\text{pmapfilter}(\mathfrak{P}, \text{cert}, \sigma)$

```

1  $\mathfrak{P}' \leftarrow \emptyset$ 
2 for  $P \in \mathfrak{P}'$  do
3    $i \leftarrow \text{size of } \text{us}(P)$ 
4    $\mathfrak{P}'' \leftarrow i + 1$  non-simple extensions of  $P$ 
5   for  $P_{\text{ext}} \in \mathfrak{P}''$  do
6      $\text{badpoly} \leftarrow \text{false}$ 
7     for  $P'_{\text{ext}} \in \mathfrak{P}'$  do
8       if  $\text{us}(P_{\text{ext}}) = \text{us}(P'_{\text{ext}}) \wedge P_{\text{ext}} \cong P'_{\text{ext}}$  then
9          $\text{badpoly} \leftarrow \text{true}$ 
10      end
11     end
12     if  $\text{badpoly} = \text{false}$  then
13        $\mathfrak{P}' \leftarrow \mathfrak{P}' \cup \{P\}$ 
14     end
15   end
16 end
17 return  $\mathfrak{P}'$ 

```

**Procedure**  $\text{nse}(\mathfrak{P})$

## VI. COMPUTATIONAL EXPERIMENTS

Accompanying this article is an implementation of the strategy described in Fig. 8 written in GAP [30] that is available in form of a **GAP4** package named **ITAP** (Information Theoretic Achievability Prover) [34]. It uses Leiterspiel [8] to perform simple linear extensions. In this section we first consider a simple approach to measure the difficulty of solving a variant of  $\text{CLRP}_q\text{-EN}$  for a specific collection of constraints  $\mathcal{I}$ . We also consider several examples from literature to describe the functionality of **ITAP** via sample sessions in **ITAP**.

We will assume that every polymatroid generated using strategy in fig. 8 is endowed with a *rank oracle* i.e. a computer program that provides the rank of a subset of subspaces in time  $\mathcal{O}(1)$ . Denote by  $\text{RE}_{\mathcal{I}}(i, r, q, K)$ , the number of evaluations of the rank oracle performed while constructing  $p\mathcal{I}$ -polymatroids at iteration  $i$  from  $p\mathcal{I}$ -polymatroids constructed at iteration  $i - 1$ , for specific values of  $r, q$  and  $K$ , for a specific collection of constraints  $\mathcal{I}$ .  $\text{RE}_{\mathcal{I}}(i, r, q, K)$  can be written as,

$$\text{RE}_{\mathcal{I}}(i, r, q, K) = \text{RE}'_{\mathcal{I}}(i, r, q, K) \times \mathcal{N}_{i-1}^{r, q, K}, i \in [N] \quad (30)$$

where,  $\text{RE}'_{\mathcal{I}}(i, r, q, K)$  is the number of evaluations of the rank oracle per object and  $\mathcal{N}_{i-1}^{r, q, K}$  denotes number of  $p\mathcal{I}$ -polymatroids at iteration  $i$ . Note that the first term in the expression above depends on the low level implementation and the collection of constraints  $\mathcal{I}$ . The second term, however, depends completely on the constraints  $\mathcal{I}$ . Hence, we are motivated to discuss the number of  $p\mathcal{I}$ -polymatroids constructed by **ITAP** as a measure of difficulty of solving a  $\text{CLRP}_q$  variant for constraints  $\mathcal{I}$ . A closed form expression for the numbers of strongly non-isomorphic  $p\mathcal{I}$ -polymatroids in a particular class of codes for a particular collection of constraints  $\mathcal{I}$  is unknown. Note that the numbers of  $p\mathcal{I}$ -polymatroids in a particular class of codes constructed by **ITAP** upper bounds the number of strongly non-isomorphic  $p\mathcal{I}$ -polymatroids in a particular class of codes, due to the hybrid approach of switching between weak and strong isomorphism adopted by **ITAP** (see §V-B). Interestingly, we observe that these numbers are much smaller than the number of all codes up to strong isomorphism in the same class of codes, at least in cases where such upper bounds are known.

The examples we consider, along with many others, are inbuilt in **ITAP** as part of the catalog of examples. The first example we consider is that of enumeration of all rate vectors achievable with a specified class of codes. The rest of the examples are concerned with the existential questions arising in



varied contexts ranging from achievability proofs in network coding and secret sharing to proving linear rank inequalities. For each example, we state the associated constrained linear representability problem, plot the number of polymatroid representations constructed at the  $i$ th iteration of the algorithm along with known upper bounds, specify the time required to compute the answer, and describe the associated sample session with ITAP. All computations are performed on a 2 GHz Xeon CPU E5-2620 running Ubuntu 12.04 OS.

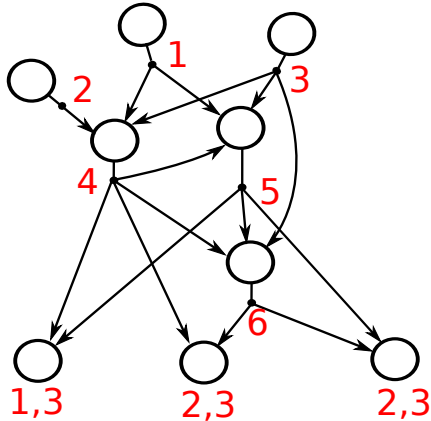


Figure 9: A HMSNC instance HN1 with 6 random variables considered in example 3

**Example 3.** Consider the 6-variable HMSNC instance HN1 in Fig. 9. It consists of 3 source random variables and 3 edge random variables. The exact rate region of this network is also shown in below, which happens to be polyhedral.

$$\mathcal{R}_{\text{HN1}} = \left\{ (\omega, \mathbf{r}) \in \mathbb{R}^6 \left| \begin{array}{l} R_4 \geq \omega_1 \\ R_4 + R_5 \geq \omega_1 + \omega_2 + \omega_3 \\ R_6 \geq \omega_1 \\ R_4 + R_6 \geq h_2 + \omega_3 \\ R_4 + R_5 + 2R_6 \geq \omega_1 + 2\omega_2 + 2\omega_3 \\ R_5 + R_6 \geq \omega_2 + \omega_3 \end{array} \right. \right\} \quad (31)$$

The network constraints associated with this network are,

$$\mathcal{I}_{\text{HN1}} = \left\{ \begin{array}{l} \{h_1 + h_2 + h_3 = h_{1,2,3}\}, \{h_{1,2,3} = h_{1,2,3,4}\}, \\ \{h_{1,3,4} = h_{1,3,4,5}\}, \{h_{3,4,5} = h_{3,4,5,6}\}, \\ \{h_{4,5} = h_{1,3,4,5}\}, \{h_{4,6} = h_{2,3,4,6}\}, \\ \{h_{5,6} = h_{2,3,5,6}\} \end{array} \right\} \quad (32)$$

We can construct achievable rate region that matches the exact rate region in (31) if we use codes from class  $\mathcal{P}^q(6, (1, 4), \{0, 1, 2\}, (1, 6))$ , as shown in the sample ITAP session. This computation takes about 387 sec. Constructing an achievable rate region from class  $\mathcal{P}^q(6, (1, 3), \{0, 1, 2\}, (1, 6))$ , however, results in a smaller rate region, shown in (34), computation that takes about 32 sec. The tree of  $p\mathcal{I}_{\text{HN1}}$ -polymatroids generated by ITAP in the latter case is shown in Fig. 10. The leaves of this tree correspond to all weakly non-isomorphic network codes that belong to the family of representable integer polymatroids determined by the aforementioned parameters. Each leaf comes with a  $p$ -map that determines the rate vector achieved by the associated code, which is also shown in the figure. This  $p$ -map has the property that it is the lexicographically smallest map among all valid  $p$ -maps. By traversing rest of the  $p$ -map tree for these  $\mathcal{I}_{\text{HN1}}$ -polymatroids, we recover the following collection of achievable rate vectors:

$$\left\{ \begin{array}{l} [1, 1, 1, 1, 2, 2], [1, 1, 1, 2, 1, 2], \\ [1, 1, 1, 2, 2, 1], [1, 1, 1, 2, 2, 2] \end{array} \right\} \quad (33)$$

To obtain the inequality description of the achievable rate region, we follow the procedure mentioned at the end of §III-A. This completes the computation of achievable rate region.

$$\mathcal{R}_{\text{in}} = \left\{ (\boldsymbol{\omega}, \mathbf{r}) \in \mathbb{R}^6 \left| \begin{array}{l} \omega_i \geq 0, i \in [3] \\ R_i \geq \omega_k, i \in \{4, 5, 6\}, k \in [3] \\ R_i + R_j \geq 3\omega_k, \forall \{i, j\} \subset \{4, 5, 6\} \text{ and } k \in [3] \\ R_4 + R_5 + R_6 \geq 5\omega_i, i \in [3] \end{array} \right. \right\} \quad (34)$$

ITAP session with example 3

```
gap> N:=HyperedgeNet1();
[ [ [ [ 1, 2, 3 ], [ 1, 2, 3, 4 ] ], [ [ 1, 3, 4 ], [ 1, 3, 4, 5 ] ],
  [ [ 3, 4, 5 ], [ 3, 4, 5, 6 ] ], [ [ 4, 5 ], [ 1, 3, 4, 5 ] ],
  [ [ 4, 6 ], [ 2, 3, 4, 6 ] ], [ [ 5, 6 ], [ 2, 3, 5, 6 ] ] ], 3, 6 ]
gap> rlist:=proveregion(N,2,GF(2),[4]);; # k=2,opt_dmax=4=max. code dimension
gap> Size(rlist[1]); # number of distinct achievable rate vectors found
122
gap> rlist[1][78]; # an achievable rate vector
[ 2, 0, 1, 2, 1, 1 ]
gap> lrs_path:="/home/aspitrg3-users/jayant/lrslib-061/";; # path to lrslib
gap> rrcompute(rlist[1],N[2],N[3],lrs_path); # compute achievable rate region

*redund:lrslib v.6.1 2015.11.20(lrsgmp.h gmp v.5.0)
*Copyright (C) 1995,2015, David Avis avis@cs.mcgill.ca
*Input taken from file /tmp/tmxYdXYT/file1.ext
*Output sent to file /tmp/tmxYdXYT/file1red.ext

*0.056u 0.004s 648Kb 0 flts 0 swaps 0 blks-in 8 blks-out

*lrs:lrslib v.6.1 2015.11.20(lrsgmp.h gmp v.5.0)
*Copyright (C) 1995,2015, David Avis avis@cs.mcgill.ca
*Input taken from file /tmp/tmxYdXYT/file1red.ext
H-representation
begin
***** 7 rational
 0 0 0 0 1 0 0
 0 1 0 0 0 -1 0
 0 0 0 0 0 1 0
 0 0 0 0 0 0 1
 0 0 0 1 0 0 0
 0 1 1 0 -1 -1 -1
 0 0 1 1 0 -1 -1
 0 0 1 0 0 0 0
 0 1 1 2 -1 -2 -2
 0 1 0 1 0 -1 -1
end
*Totals: facets=10 bases=22
*Dictionary Cache: max size= 6 misses= 0/21 Tree Depth= 5
*lrs:lrslib v.6.1 2015.11.20(32bit,lrsgmp.h)
*0.000u 0.000s 648Kb 0 flts 0 swaps 0 blks-in 0 blks-out
```

**Example 4.** This is a collection of examples from network coding literature: the so called matroidal and discrete polymatroidal networks (see [25], [42]). These networks are constructed to mimic the dependencies of matroids and integer polymatroids respectively. As a result, the known results regarding the representability of these polymatroids carry forward to the networks, thus providing us with the networks for which achievability or non-achievability of certain rate vectors is established by construction.

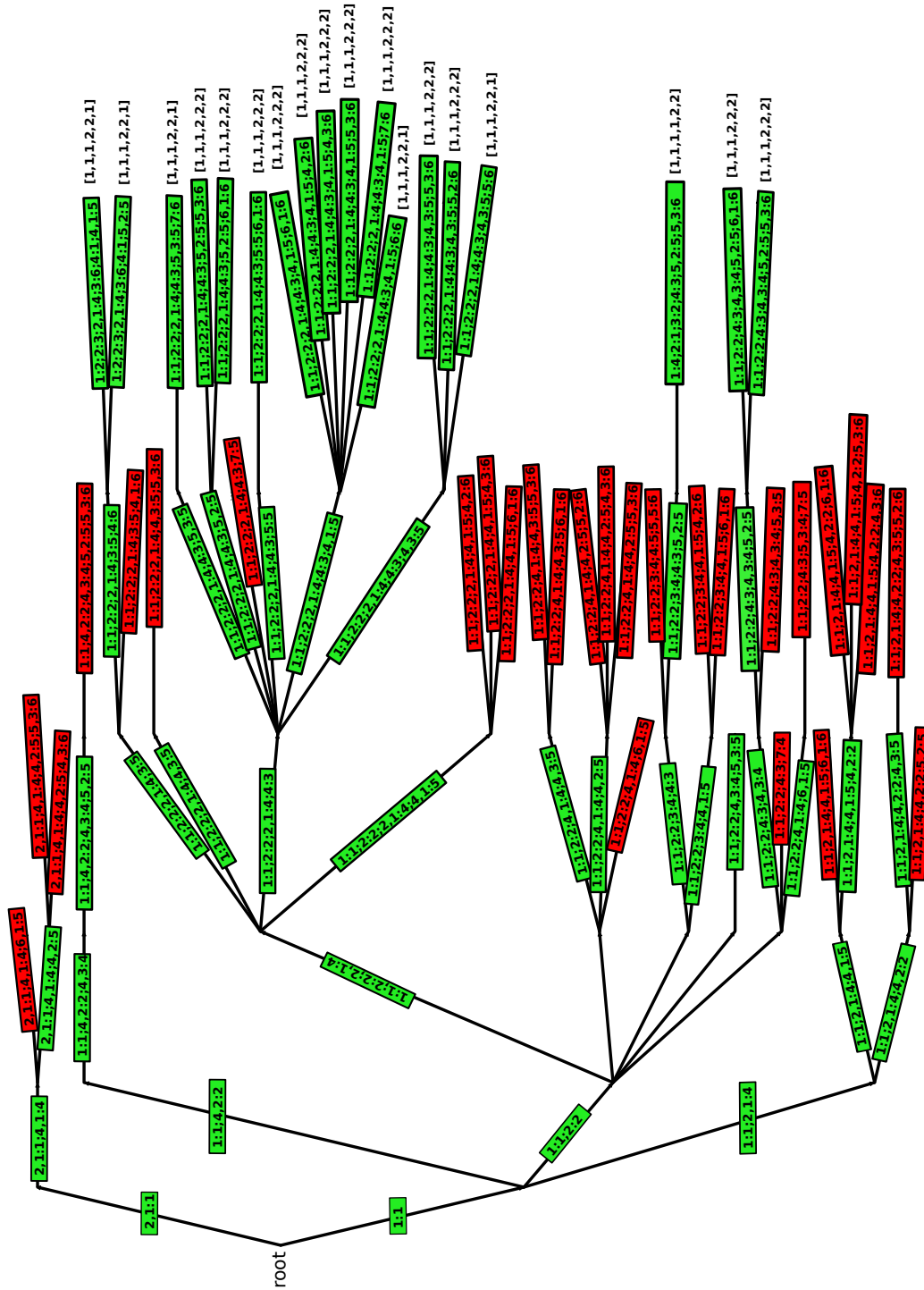


Figure 10: The generation tree for example 3 with class of codes  $\mathcal{P}^2((6, (3, 3), 1, 2, (6, 6)))$ . The strings associated with edges encode the polymatroids and associated  $p$ -maps in a compact form. A string  $i,j;k;l,m:n$  is to be interpreted as the polymatroid associated with the subspace arrangement  $\{\{i,j\}, \{l,m\}\}$  where numbers  $i,j,l,m$  correspond to integer representation of binary vectors in  $\mathbb{F}_2^3$  and numbers  $k,n$  correspond to subscripts of the random variables associated with the network.

The matroidal networks we consider are the Fano, Non-Fano and Vámos networks, whereas the discrete polymatroidal network we use as example is the network constructed from the polymatroid associated with a scaled version of  $U_4^2$  matroid. Equations below describe the constraints associated with each of these networks. The Fano network is size  $N = 7$  network associated with the Fano matroid. Rate vector  $(\omega_i = 1, R_j = 1, i \in [3], j \in [7] \setminus [3])$  is achievable for this network using linear network coding only over a finite field of even characteristic, as the Fano matroid is only representable over such fields.

$$\mathcal{I}_{\text{Fano}} = \left\{ \begin{array}{l} \{h_1 + h_2 + h_3 = h_{1,2,3}\}, \{h_{1,2} = h_{1,2,4}\}, \\ \{h_{2,3} = h_{2,3,5}\}, \{h_{4,5} = h_{4,5,6}\}, \\ \{h_{3,4} = h_{3,4,7}\}, \{h_{1,6} = h_{3,1,6}\}, \\ \{h_{6,7} = h_{2,6,7}\}, \{h_{5,7} = h_{1,5,7}\} \end{array} \right\} \quad (35)$$

ITAP session with Fano Network in Example 4

```
gap> FanoNet ();
[ [ [ [ 1, 2 ], [ 1, 2, 4 ] ], [ [ 2, 3 ], [ 2, 3, 5 ] ],
  [ [ 4, 5 ], [ 4, 5, 6 ] ], [ [ 3, 4 ], [ 3, 4, 7 ] ],
  [ [ 1, 6 ], [ 3, 1, 6 ] ], [ [ 6, 7 ], [ 2, 6, 7 ] ],
  [ [ 5, 7 ], [ 1, 5, 7 ] ] ], 3, 7 ]
gap> rlist:=proverate(FanoNet(), [1,1,1,1,1,1,1], GF(2), []);
gap> rlist[1]; # Fano matroid is representable over GF(2)
true
gap> DisplayCode(rlist[2]);
1->1
. . 1
=====
2->2
. 1 .
=====
3->4
. 1 1
=====
4->3
1 . .
=====
5->6
1 . 1
=====
6->5
1 1 .
=====
7->7
1 1 1
=====
gap> rlist:=proverate(FanoNet(), [1,1,1,1,1,1,1], GF(3), []);
gap> rlist[1]; # Fano matroid is not representable over GF(3)
false
```

The second matroidal network we consider is the Non-Fano network, which is also a size  $N = 7$  network, for which the rate vector  $(\omega_i = 1, R_j = 1, i \in [3], j \in [7] \setminus [3])$  is achievable via linear network coding only over a finite field of odd characteristic.

$$\mathcal{I}_{\text{NonFano}} = \left\{ \begin{array}{l} \{h_1 + h_2 + h_3 = h_{1,2,3}\}, \\ \{h_{1,2,3} = h_{1,2,3,4}\}, \{h_{1,2} = h_{1,2,5}\}, \\ \{h_{1,3} = h_{1,3,6}\}, \{h_{2,3} = h_{2,3,7}\}, \\ \{h_{4,5} = h_{3,4,5}\}, \{h_{4,6} = h_{2,4,6}\}, \\ \{h_{4,7} = h_{1,4,7}\}, \{h_{5,6,7} = h_{1,2,3,5,6,7}\} \end{array} \right\} \quad (36)$$

The third matroidal network we consider is the Vámos network of size  $N = 8$  for which the rate vector  $(\omega_i = 1, R_j = 1, i \in [4], j \in [8] \setminus [4])$  is not achievable via linear coding over any finite field.

$$\mathcal{I}_{\text{Vámos}} = \left\{ \begin{array}{l} \{h_1 + h_2 + h_3 + h_4 = h_{1,2,3,4}\}, \{h_{1,2,3,4} = h_{1,2,3,4,5}\}, \\ \{h_{1,2,5} = h_{1,2,5,6}\}, \{h_{2,3,6} = h_{2,3,6,7}\}, \\ \{h_{3,4,7} = h_{3,4,7,8}\}, \{h_{4,8} = h_{2,4,8}\}, \\ \{h_{2,3,4,8} = h_{1,2,3,4,8}\}, \{h_{1,4,5,8} = h_{1,2,3,4,5,8}\}, \\ \{h_{1,2,3,7} = h_{1,2,3,4,7}\}, \{h_{1,5,7} = h_{1,3,5,7}\} \end{array} \right\} \quad (37)$$

The last network we consider is the  $2U_4^2$  network of size  $n = 4$ , whose network constraints mimic the dependencies of the  $U_4^2$  matroid i.e. the 4 point line. This matroid is a forbidden minor for matroid representability over  $\mathbb{F}_2$  [43], which means that the rate vector  $(\omega_i = 1, R_j = 1, i \in [2], j \in [4] \setminus [2])$  is not achievable for this network via linear network coding over  $\mathbb{F}_2$ . However, the polymatroid  $2U_4^2$ , which is obtained by scaling the rank function of  $U_4^2$  by 2, is linearly representable over  $\mathbb{F}_2$ , implying that rate vector  $(\omega_i = 2, R_j = 2, i \in [2], j \in [4] \setminus [2])$  is achievable for this network using linear coding over  $\mathbb{F}_2$ .

$$\mathcal{I}_{2U_4^2} = \left\{ \begin{array}{l} \{h_1 + h_2 = h_{1,2}\}, \{h_{1,2} = h_{1,2,3}\}, \\ \{h_{1,3} = h_{1,2,3}\}, \{h_{2,3} = h_{1,2,3}\}, \\ \{h_{1,2} = h_{1,2,4}\}, \{h_{1,4} = h_{1,2,4}\}, \\ \{h_{3,4} = h_{1,3,4}\}, \{h_{3,4} = h_{2,3,4}\}, \{h_{2,4} = h_{1,2,4}\} \end{array} \right\} \quad (38)$$

Now that we have described the four network coding instances, we can ask ITAP some questions whose answers we already know.

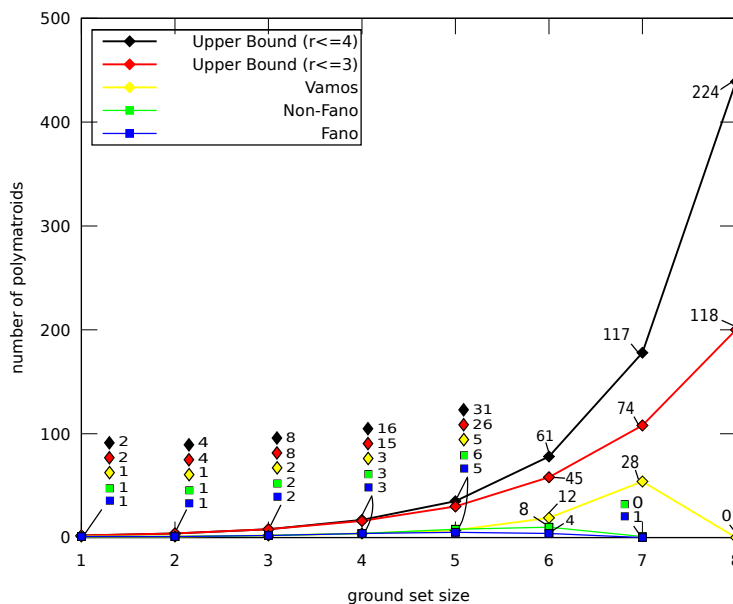


Figure 11: Number matroid representations over  $\mathbb{F}_2$  maintained by ITAP at different iterations for Fano (blue), Non-Fano (green) and Vámos (yellow) networks along with upper bound which is the number of all non-isomorphic  $\mathbb{F}_2$ -representable matroids of rank  $\leq 3$  for Fano and Non-Fano networks while it is the number of  $\mathbb{F}_2$ -representable matroids of rank  $\leq 4$  for the Vámos network

For Fano, Non-Fano and Vámos networks, we test whether rate vector  $(\omega_i = 1, R_j = 1, i \in [k], j \in [N] \setminus [k])$  is achievable over  $\mathbb{F}_2$  and  $\mathbb{F}_3$ . The sample session with for Fano network with ITAP is also shown. The numbers of  $p\mathcal{I}$ -polymatroids are shown in figures 11 and 12. The upper bounds in these figures are the numbers of rank  $\leq 3$  and rank  $\leq 4$  non-isomorphic binary and ternary representable matroids

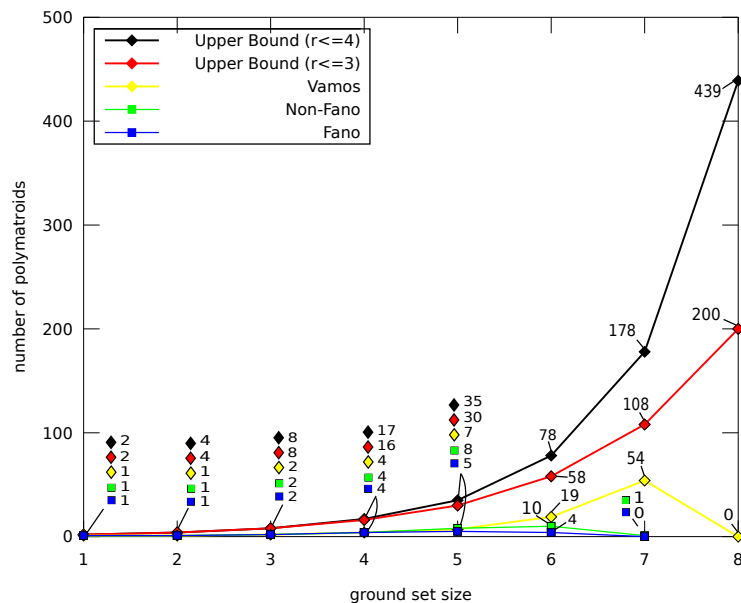


Figure 12: Number of weakly non-isomorphic matroid representations over  $\mathbb{F}_3$  at different iterations for Fano, Non-Fano and Vámos networks along with upper bound (the number of all non-isomorphic  $\mathbb{F}_3$ -representable matroids of suitable rank)

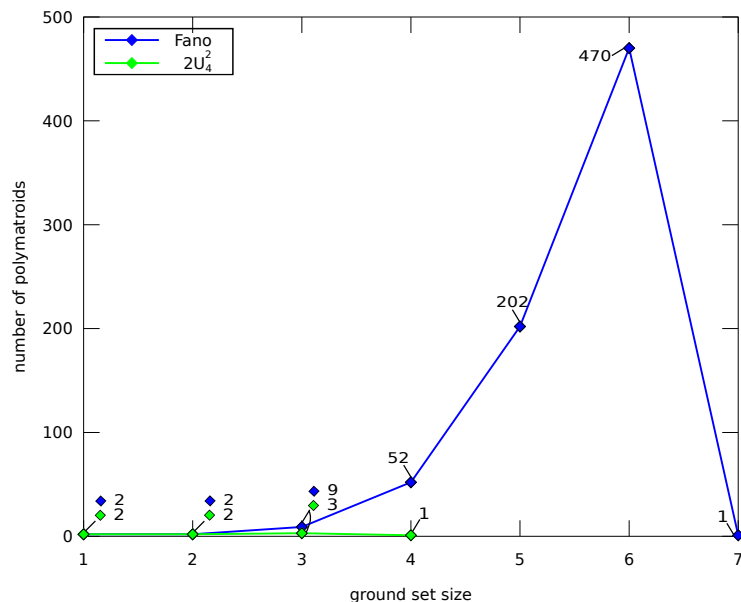


Figure 13: Number of polymatroid representations over  $\mathbb{F}_2$  maintained by ITAP at different iterations for Fano and  $2U_4^2$  networks

respectively, which were first obtained by Wild (see [37], [60]). One can see from the plots that the number  $p\mathcal{L}$ -polymatroids maintained by ITAP in each instance is much smaller than the respective upper bounds. The time required for testing scalar solvability of Fano and Non-Fano networks is 1 seconds and 2 seconds respectively over  $\mathbb{F}_2$  whereas it is 5 seconds and 4 seconds respectively over  $\mathbb{F}_3$ . Timing results for Vámos network are discussed in detail in example 7.

For Fano and  $2U_4^2$  networks, we test if rate vector  $(\omega_i = 2, R_j = 2, i \in [k], j \in [N] \setminus [k])$  is achievable. We know that the answer is affirmative for both of these instances. This rate vector dictates that for Fano network, the class of codes to search for achievability construction is  $\mathcal{P}^a(7, (6, 6), \{2\}, (3, 7))$ . Whereas,

for  $2U_4^2$  network, we have the class  $\mathcal{P}^q(4, (4, 4), \{2\}, (2, 4))$ . The result, i.e. the numbers of weakly non-isomorphic representations constructed at each iteration by ITAP is shown in figure 13. This plot is left without any upper bounds, as the only known upper bound is the number of general 2-polymatroids obtained via Savitsky's enumeration [51], already shown in Fig. 3. The time required in this case is 142 minutes and 1 seconds for Fano and  $2U_4^2$  networks respectively. ■

**Example 5.** ([6], [44]) Let  $\Gamma = \{\{2, 3\}, \{3, 4\}, \{4, 5\}\}$  be an access structure for sharing a secret with 4 parties labeled  $\{2, 3, 4, 5\}$  with the dealer labeled 1. This example appears in [6], whereas an explicit multi-linear secret sharing scheme for this access structure with secret size  $r_1 = 2$  and share sizes  $r_2 = 2, r_3 = 3, r_4 = 3, r_5 = 2$  can be found in [44]. For the purpose of reproducing this scheme with ITAP, equations (13) and (14) (constraints  $\mathcal{I}_\Gamma$ ) along with the requirement to have specified share sizes form collection of constraints  $\mathcal{I}$ . The constraints imply that the class of codes in which an achievable construction might exist is  $\mathcal{P}^q(5, (3, 12), \{2, 3\}, (2, 5))$ . Equation (39) gives the representation constructed by ITAP, with  $p$ -map  $\{1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3, 4 \mapsto 5, 5 \mapsto 4\}$ . The sample ITAP session is also shown. This computation takes about 32 min. ■

$$P \triangleq \left\{ \begin{array}{c} s_1 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \\ s_2 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \\ s_3 \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \\ s_4 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \\ s_5 \\ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array} \right\} \quad (39)$$

ITAP session for Example 5

```
gap> B:=BenalohLeichter();
[ [ 1, 2 ], [ 2, 3 ], [ 3, 4 ] ]
gap> rlist:=provers(B,5,[2,2,3,3,2],GF(2),[]);;
gap> rlist[1];
true
gap> DisplayCode(rlist[2]);
1->1
. . . . 1 .
. . . . . 1
=====
2->2
. . 1 . . .
. . . 1 . .
=====
3->3
. 1 . . . .
. . 1 . . 1
. . . 1 1 .
=====
4->5
1 . . . . .
. 1 . . . .
=====
5->4
1 . . . . 1
. 1 . . 1 .
. . 1 . . .
=====
```

**Example 6.** This example is concerned with proving linear rank inequalities amongst  $N$  random variables. Dougherty, Freiling and Zeger use a computational technique [23] to find non-redundant linear rank





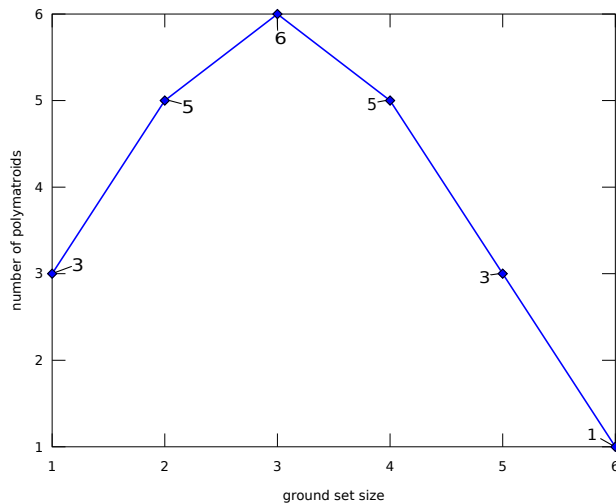


Figure 15: Number of  $p\mathcal{L}$ -polymatroid representations over  $\mathbb{F}_2$  of various ranks constructed by ITAP at different iterations for example 6.

q	Comb. Gen.	Gröbner
2	130	4
2	1330	5
4	5400	7
5	>2 hrs	5
7	>2 hrs	5
8	>2 hrs	7
9	>2 hrs	7

Table II: Time in seconds to test scalar solvability of Vámos network w.r.t. Field size  $q$

instance to an instance of Network Coding over Direct Acyclic Multi-graphs (NCDAMG) is provided in appendix A. The first instance for which we compare the two methods is the Vámos network. Being a 'no' instance of  $\text{CLRP}_q\text{-EX}$ , this is expected to trigger the worst behaviour out of a combinatorial generation based algorithm (in a sense that the algorithm must traverse the entire search tree, in order to conclude that a solution does not exist). Our results are summarized in table X, which suggest the same. On the other hand, we also find type of instances that incite bad behaviour from Gröbner basis computation based method. The number of indeterminates in path gain formulation depends on the number of paths. If the NCDAMG instance produced by algorithm 2 has  $p$  source-sink paths for a rate vector  $(\omega_i = 1, R_j = 1), i \in [k], j \in [N] \setminus [k]$ , doubling each rate produces a NCDAMG instance with  $2^p$  paths. The instance we compare the performance of the two methods is a Multilevel Diversity Coding System (MDCS) [62] instance with  $N = 7$ , described as follows:

$$\mathcal{I}_{\text{MDCS}} = \left\{ \begin{array}{l} \{ \{h_1 + h_2 + h_3 = h_{1,2,3}\}, \{h_{1,2,3} = h_{1,2,3,4}\}, \\ \{h_{1,2,3} = h_{1,2,3,5}\}, \{h_{1,2,3} = h_{1,2,3,6}\}, \\ \{h_{1,2,3} = h_{1,2,3,7}\}, \{h_4 = h_{1,4}\}, \{h_5 = h_{1,5}\}, \\ \{h_{4,5} = h_{1,2,4,5}\}, \{h_{6,7} = h_{1,2,6,7}\}, \\ \{h_{4,6} = h_{1,2,3,4,6}\}, \{h_{5,7} = h_{1,2,3,5,7}\} \end{array} \right\} \quad (41)$$

## VII. CONCLUSION AND FUTURE WORK

This article defined the existential and enumerative variants of the constrained linear representability problem for polymatroids, and showed that special instances of these problems include the construction of achievability proofs in network coding and secret sharing. An algorithm built from group theoretic

Rate vector	Type of instance	Comb. Gen.	Gröbner
[1, 1, 1, 1, 1, 1, 1]	no	4	1
[1, 1, 1, 2, 1, 1, 1]	no	8	1
[1, 1, 1, 2, 2, 1, 1]	yes	9	>1 hr
[1, 1, 1, 2, 2, 2, 2]	yes	3	>1 hr
[1, 1, 1, 2, 1, 1, 2]	yes	5	>1 hr

Table III: Time in seconds to test achievability of a given rate vector over  $\mathbb{F}_2$

techniques for combinatorial generation was developed to solve this problem, and an implementation of this algorithm in the GAP package **ITAP** accompanies the article. Several experiments with the developed enumerative method demonstrated its utility as well as improvement in runtime over competing methods for solving CLRP<sub>q</sub>-EX in some problems. As network coding and secret sharing constructions in general necessitate nonlinear codes, a key future extension of the work will focus on finding nonlinear achievability constructions when linear ones fail. In this vein, the group theoretic method of combinatorial generation employed here, Leiterspiel, can also be adapted to efficiently generate such nonlinear dependence structures, as demonstrated in [64], [65].

#### ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation under the awards CCF-1016588 and CCF-1421828.

#### APPENDIX A

##### TRANSFORMATION OF A HMSNC INSTANCE INTO A NCDAMG INSTANCE

We specify a NCDAMG instance  $A'$  as per the terminology in [55], by a tuple  $(\mathcal{V}', \mathcal{E}', \mathcal{S}', \mathcal{T}', g)$  where  $(\mathcal{V}', \mathcal{E}')$  is a directed acyclic multigraph,  $\mathcal{S}', \mathcal{T}' \subseteq V'$  are sets of source and sink nodes respectively, and  $g$  is the demand function assigning exactly one member of  $\mathcal{S}'$  to each  $t \in \mathcal{T}'$ . Each edge  $e \in \mathcal{E}'$  is a triplet  $(v_1, v_2, c)$  where  $v_1, v_2 \in \mathcal{V}'$  and  $c$  is the edge label or color. Algorithm 2 accepts a HMSNC instance in form of the associated constraints  $\mathcal{L}_i, i \in [3]$ , number of source  $k$ , number of random variables  $N$  and a rate vector  $(r_1, \dots, r_N)$ . At the beginning, all members of  $A'$  are empty. Algorithm 2 populates various member of  $A'$  and also maintains a function  $\text{msg2node} : \mathcal{X} \rightarrow \mathcal{V}'$  where  $\mathcal{X} \subseteq [N]$ . For message labels  $i$  not in  $\mathcal{X}$  at any point, we say that  $\text{msg2node}(i)$  is not defined. For each constraint  $l$  in  $\mathcal{L}_2 \cup \mathcal{L}_3$ , we use functions  $\text{imsg}(l)$  and  $\text{omsg}(l)$  to refer to the input and output message labels involved in constraint  $l$ . At the beginning  $\text{msg2node}(i)$  is undefined for each  $i \in [N]$ . First for each source message  $i \in [k]$ ,  $r_i$  nodes are added to sets  $\mathcal{V}'$  and  $\mathcal{S}'$  (lines 2-4, fig. 16). These are the source nodes of NCDAMG instance  $A'$ . Second, it goes through constraints  $\mathcal{L}_2$ , considering at each iteration of the while loop at lines 5-9, a constraint  $l$  s.t.  $\text{msg2node}(i)$  is defined for each  $i \in \text{imsg}(l)$ . The new nodes and edges, added to  $\mathcal{V}'$  and  $\mathcal{E}'$  using procedure  $\text{convertL2}$ , are summarized as a gadget in figure 16. Finally, for each decoding constraint  $l \in \mathcal{L}_3$ , if  $|\text{omsg}(l)| = 1$  a single decoder node is added whereas if  $|\text{omsg}(l)| > 1$  multiple decoder nodes are added to  $\mathcal{V}'$ , in while loop at lines 10-14 using procedure  $\text{convertL3}$ . The demand function  $g$  for these decoder nodes is also set during the same procedure. Throughout algorithm 2, the number of parallel edges added between nodes depends on the rate vector. Thus, given a HMSNC instance  $A$  and a rate vector  $(r_1, \dots, r_N)$ , algorithm 2 constructs a NCDAMG instance  $A'$  such that the following holds:

**Lemma 6.** *Rate vector  $(r_1, \dots, r_N)$  is achievable in  $A$  with vector linear network codes if  $A'$  is scalar linear solvable.*

**Proof:** If  $A'$  is scalar linear solvable, there exists a representable matroid  $M$  associated with the scalar linear solution. In the matrix representation of  $M$ , each column is associated with an edge in  $A'$ . We can create a  $N$ -subspace arrangement  $\{V_1, \dots, V_N\}$  from this matroid s.t.  $V_i, i \in [N]$  is the span of columns associated with edge incoming to  $\text{msg2node}(i)$ . ■

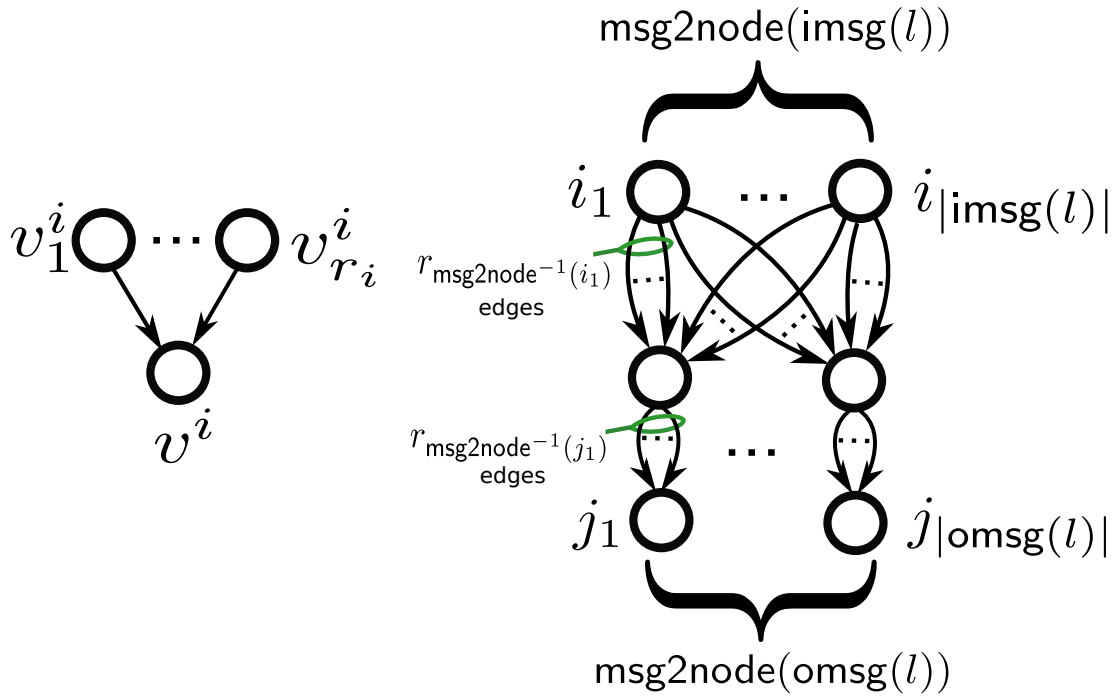


Figure 16: (left) Gadget used by algorithm 2 for source messages and, (right) gadget used for intermediate constraints  $l \in \mathcal{L}_2$

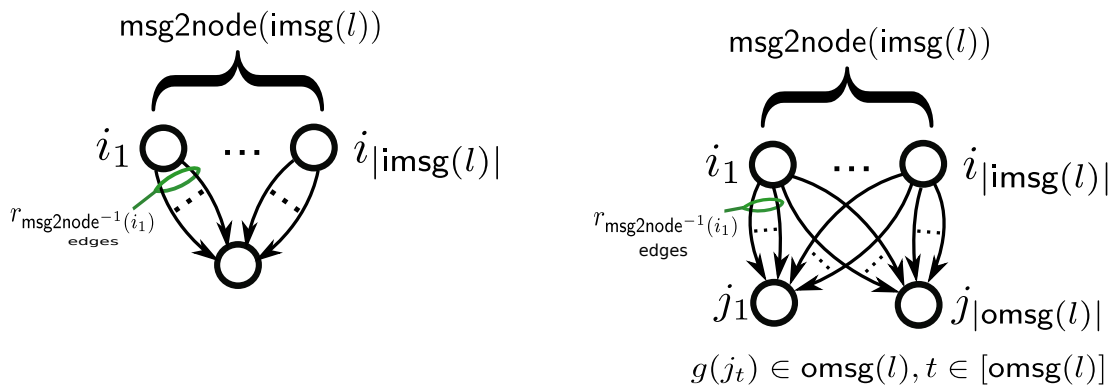


Figure 17: Gadgets used by algorithm 2 for decoder constraints. (left) the case  $|\text{omsg}(l)| = 1$  and (right) the case  $|\text{omsg}(l)| > 1$

**Input:** Sets  $\mathcal{L}_1, \mathcal{L}_2$  and  $\mathcal{L}_3$  associated with HMSNC instance  $A$ , no. of sources  $k$ , no. of variables  $N$ , rate vector  $\mathbf{r} = (r_1, \dots, r_N)$

**Output:** A NCDAMG instance  $A' = (\mathcal{V}', \mathcal{E}', \mathcal{S}', \mathcal{T}', g)$

```

1  $\mathcal{V}' \leftarrow \emptyset, \mathcal{E}' \leftarrow \emptyset, g \leftarrow$  empty function,  $\text{msg2node} \leftarrow$  empty function,  $\mathcal{L} \leftarrow \emptyset$ 
2 foreach  $i \in [k]$  do
3    $\mathcal{V}' \leftarrow \mathcal{V}' \cup \{v_1^i, \dots, v_{r_i}^i\}, \mathcal{S}' \leftarrow \mathcal{S}' \cup \{v_1^i, \dots, v_{r_i}^i\}, \mathcal{V}' \leftarrow \mathcal{V}' \cup v^i, \text{msg2node}(i) \leftarrow v^i$ 
4 end
5 while  $\mathcal{L}_2 \not\subseteq \mathcal{L}$  do
6    $l \leftarrow$  constraint in  $\mathcal{L}_2$  not in  $\mathcal{L}$  with  $\text{msg2node}(i)$  defined for each  $i \in \text{imsg}(l)$ 
7    $(\text{msg2node}, \mathcal{V}', \mathcal{E}') \leftarrow \text{convertL2}(l, \text{msg2node}, \mathcal{V}', \mathcal{E}', \mathbf{r})$ 
8    $\mathcal{L} \leftarrow \mathcal{L} \cup \{l\}$ 
9 end
10 while  $\mathcal{L}_3 \not\subseteq \mathcal{L}$  do
11    $l \leftarrow$  constraint in  $\mathcal{L}_3$  not in  $\mathcal{L}$ 
12    $(\text{msg2node}, \mathcal{V}', \mathcal{E}', \mathcal{T}', g) \leftarrow \text{convertL3}(l, \text{msg2node}, \mathcal{V}', \mathcal{E}', \mathcal{T}', g, \mathbf{r})$ 
13    $\mathcal{L} \leftarrow \mathcal{L} \cup \{l\}$ 
14 end
15 return  $(\mathcal{V}', \mathcal{E}', \mathcal{S}', \mathcal{T}', g)$ 

```

**Algorithm 2:** Algorithm to transform a HMSNC instance to a NCDAMG instance

```

1 foreach  $o \in \text{omsg}(l)$  do
2    $\mathcal{V}' \leftarrow \mathcal{V}' \cup \{v_1^o\}, \mathcal{V}' \leftarrow \mathcal{V}' \cup \{v_2^o\}, \text{msg2node}(o) \leftarrow v_2^o$ 
3   foreach  $i \in \text{imsg}(l)$  do
4      $\mathcal{E}' \leftarrow \mathcal{E}' \cup \{(\text{msg2node}(i), v_1^o, c_1), \dots, (\text{msg2node}(i), v_1^o, c_{r_i})\}$ 
5   end
6    $\mathcal{E}' \leftarrow \mathcal{E}' \cup \{(v_1^o, v_2^o, c_1), \dots, (v_1^o, v_2^o, c_{r_o})\}$ 
7 end
8 return  $\text{msg2node}, \mathcal{V}', \mathcal{E}'$ 

```

**Procedure**  $\text{convertL2}(l, \text{msg2node}, \mathcal{V}', \mathcal{E}', \mathbf{r})$

```

1 if  $|omsg(l)|$  is 1 then
2    $\mathcal{V}' \leftarrow \mathcal{V}' \cup \{v^l\}$ 
3   foreach  $i \in imsg(l)$  do
4      $\mathcal{E}' \leftarrow \mathcal{E}' \cup \{(msg2node(i), v^l, c_1), \dots, (msg2node(i), v^l, c_{r_i})\}$ 
5      $g(v^l) \leftarrow omsg(l)$ 
6   end
7    $\mathcal{T}' \leftarrow \mathcal{T}' \cup \{v^l\}$ 
8 end
9 else
10  foreach  $o \in omsg(l)$  do
11     $\mathcal{V}' \leftarrow \mathcal{V}' \cup \{v_o^l\}$ 
12    foreach  $i \in imsg(l)$  do
13       $\mathcal{E}' \leftarrow \mathcal{E}' \cup \{(msg2node(i), v_o^l, c_1), \dots, (msg2node(i), v_o^l, c_{r_i})\}$ 
14       $g(v_o^l) \leftarrow \{o\}$ 
15    end
16     $\mathcal{T}' \leftarrow \mathcal{T}' \cup \{v_o^l\}$ 
17  end
18 end
19 return  $msg2node, \mathcal{V}', \mathcal{E}', \mathcal{T}, g$ 

```

**Procedure**  $convertL3(l, msg2node, \mathcal{V}', \mathcal{E}', \mathcal{T}, g, r)$

## REFERENCES

- [1] Jayant Apte. chm-An Implementation of Convex Hull Method, 2014. <http://www.ece.drexel.edu/walsh/aspitrg/software.html>.
- [2] Jayant Apte, Qi Chen, and John MacLaren Walsh. Symmetries in the entropy space, 2015. submitted, Available Online: <https://sites.google.com/site/jayantapteshomepage/>.
- [3] Jayant Apte, Congduan Li, and J.M. Walsh. Algorithms for computing network coding rate regions via single element extensions of matroids. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 2306–2310, June 2014.
- [4] Jayant Apte and John MacLaren Walsh. Exploiting symmetry in computing polyhedral bounds on network coding rate regions. In *2015 International Symposium on Network Coding, NetCod 2015, Sydney, Australia, June 22-24, 2015*, pages 76–80, 2015.
- [5] Amos Beimel. Secret-sharing schemes: A survey. In YeowMeng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer Berlin Heidelberg, 2011.
- [6] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Proceedings on Advances in Cryptology, CRYPTO '88*, pages 27–35, New York, NY, USA, 1990. Springer-Verlag New York, Inc.
- [7] Michael Bertilsson and Ingemar Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - AUSCRYPT 1992*, volume 718 of *Lecture Notes in Computer Science*, pages 67–79. Springer Berlin Heidelberg, 1993.
- [8] A. Betten, M. Braun, H. Friepertinger, A. Kerber, A. Kohnert, and A. Wassermann. *Error-Correcting Linear Codes: Classification by Isometry and Applications*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2006.
- [9] John E. Blackburn, Henry H. Crapo, and Denis A. Higgs. A catalogue of combinatorial geometries. *Mathematics of Computation*, 27(121):pp. 155–166, 1973.
- [10] C. Blundo, A. De Santis, D.R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology*, 8(1):39–64, 1995.
- [11] Ning Cai and R.W. Yeung. Secure network coding. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, pages 323–, 2002.
- [12] Congduan Li. *On Multi-source Multi-Sink Hyperedge Networks: Enumeration, Rate Region Computation, and Hierarchy*. PhD thesis, Drexel University, Philadelphia, PA, 2015.
- [13] Congduan Li, Jayant Apte, John MacLaren Walsh, Steven Weber. A new computational approach for determining rate regions and optimal codes for coded networks. In *The 2013 IEEE International Symposium on Network Coding (NetCod 2013)*, June 2013.
- [14] Congduan Li, John MacLaren Walsh, Steven Weber. A computational approach for determining rate regions and codes using entropic vector bounds. In *50th Annual Allerton Conference on Communication, Control and Computing*, October 2012.
- [15] Congduan Li, Steven Weber, and John MacLaren Walsh. On Multilevel Diversity Coding Systems. *IEEE Trans. Inform. Theory*. Submitted on July 21, 2014. Reviews received January 6, 2016, revised April 4, 2016.
- [16] Congduan Li, Steven Weber, and John Walsh. On Multi-source Networks: Enumeration, Rate Region Computation, and Hierarchy. *IEEE Trans. Inform. Theory*. Submitted July 21, 2015.
- [17] M. Costantini and W. de Graaf. singular, the gap interface to singular, Version 12.04.28, Apr 2012. GAP package.
- [18] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.
- [19] Henry H. Crapo. Single-element extensions of matroids. *J. Res. Natl. Bur. Standards, Sec. B: Math. & Math. Phys.*, 69B(1-2):55–65, 1965.
- [20] L. Csirmaz. Information inequalities for four variables. Available Online: <https://www.eprints.renyi.hu/65/1/benson.pdf>, 2013.
- [21] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schoenemann. Singular 4-0-2 — A computer algebra system for polynomial computations, 2015.
- [22] Martenvan Dijk, Wen-Ai Jackson, and Keith M. Martin. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography*, 15(3):301–321, 1998.
- [23] R. Dougherty. Computations of linear rank inequalities on six variables. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 2819–2823, June 2014.
- [24] R. Dougherty, C. Freiling, and K. Zeger. Six new non-shannon information inequalities. In *Information Theory, 2006 IEEE International Symposium on*, pages 233–236, July 2006.
- [25] R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-shannon information inequalities. *Information Theory, IEEE Transactions on*, 53(6):1949–1969, 2007.
- [26] R. Dougherty, C. Freiling, and K. Zeger. Linear rank inequalities on five or more variables. *arXiv cs.IT/0910.0284v3*, 2009.
- [27] Eric W. Weisstein. Sequence A055545, Number of matroids on n points. The On-Line Encyclopedia of Integer Sequences. <http://oeis.org/A055545>.
- [28] F. Matúš. Infinitely Many Information Inequalities. In *IEEE International Symposium on Information Theory (ISIT)*, pages 41–44, June 2007.
- [29] S. Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39:55–72, 1978.
- [30] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, 2015.
- [31] Jim Geelen, Bert Gerards, and Geoff Whittle. Solving rota's conjecture. *Notices of the AMS*, 61(7):736–743, 2014.
- [32] D. Hammer, A. Romaschenko, and N. Vereshchagin A. Shen. Inequalities for shannon entropy and kolmogorov complexity. *Journal of Computer and System Science*, 60(2):442–464, April 2000.
- [33] A. W. Ingleton. Representation of matroids. *Combin. Math. Appl.*, pages 149–167, 1971.
- [34] Jayant Apte and John MacLaren Walsh. Information theoretic achievability prover -a gap4 package, 2015. <http://www.ece.drexel.edu/walsh/aspitrg/software.html>.
- [35] R. Koetter and M. Medard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11(5):782–795, Oct 2003.

- [36] C. Lassez and J-L. Lassez. Quantifier elimination for conjunctions of linear constraints via a convex hull algorithm. In Donald, Kapur, and Mundy, editors, *Symbolic and Numerical Computation for Artificial Intelligence*. Academic Press, 1993.
- [37] Marcel Wild. Sequence A076766, Number of nonisomorphic binary matroids on an  $n$ -set., The On-Line Encyclopedia of Integer Sequences. <http://oeis.org/A076766>.
- [38] Marcel Wild. Sequence A076892, Number of nonisomorphic ternary matroids on an  $n$ -set., The On-Line Encyclopedia of Integer Sequences. <http://oeis.org/A076892>.
- [39] Yoshitake Matsumoto, Sonoko Moriyama, Hiroshi Imai, and David Bremner. Matroid enumeration for incidence geometry. *Discrete Comput. Geom.*, 47(1):17–43, January 2012.
- [40] Max Alekseyev. Sequence A256157, Number of 2-polymatroids on  $n$  unlabeled points., The On-Line Encyclopedia of Integer Sequences. <http://oeis.org/A256157>.
- [41] Dillon Mayhew and Gordon F. Royle. Matroids with nine elements. *Journal of Combinatorial Theory, Series B*, 98(2):415 – 431, 2008.
- [42] Vijayaradharaj T. Muralidharan and B. S. Rajan. Linear network coding, linear index coding and representable discrete polymatroids, 2014. Available Online: <http://arxiv.org/abs/1306.1157>.
- [43] J. G. Oxley. *Matroid Theory*. Oxford University, 2011.
- [44] C. Padró. *Lecture Notes in Secret Sharing*. Central European University, 2013, 2013. Available: <http://www-ma4.upc.edu/~cpadro/arc02v03.pdf>.
- [45] R.A. Pendavingh. On the evaluation at  $(-i, i)$  of the tutte polynomial of a binary matroid. *Journal of Algebraic Combinatorics*, 39(1):141–152, 2014.
- [46] Rudi Pendavingh, Stefan Van Zwam, et al. *Sage Matroid Package, included in Sage Mathematics Software 5.11*. The Sage Matroid Development Team, 2013. <http://www.sagemath.org>.
- [47] E. Petrank and R.M. Roth. Is code equivalence easy to decide? *Information Theory, IEEE Transactions on*, 43(5):1602–1604, Sep 1997.
- [48] R. Pulikoonattu, E. Perron, and S. Diggavi. X-information theoretic inequality prover(xitip), 2008. <http://xitip.epfl.ch/>.
- [49] R. Rado. Note on independence functions. *Proceedings of the London Mathematical Society*, s3-7(1):300–320, 1957.
- [50] Gian-Carlo Rota. Combinatorial theory, old and new. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3*, pages 229–233. Gauthier-Villars, Paris, 1971.
- [51] Thomas J. Savitsky. Enumeration of 2-polymatroids on up to seven elements, 2014. Available Online: <http://arxiv.org/abs/1401.8006>.
- [52] Bernd Schmalz. Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen. (Use of subgroup ladders for the determination of double cosets). *Bayreuther Math. Schr.*, 31:109–143, 1990.
- [53] A. Shamir. How to share a secret. *Commu. Assoc. Comput.*, 22:612–613, 1979.
- [54] Douglas R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.
- [55] Abhay T. Subramanian and Andrew Thangaraj. Path gain algebraic formulation for the scalar linear network coding problem. *IEEE Transactions on Information Theory*, 56(9):4520–4531, 2010.
- [56] Chao Tian. Characterizing the rate region of the  $(4, 3, 3)$  exact-repair regenerating codes. *IEEE Journal on Selected Areas in Communications*, 32(5):967–975, 2014.
- [57] Marten van Dijk. A linear construction of secret sharing schemes. *Designs, Codes and Cryptography*, 12(2):161–201, 1997.
- [58] Marten van Dijk, Tom Kevenaar, Geert-Jan Schrijen, and Pim Tuyls. Improved constructions of secret sharing schemes by applying  $(\lambda, \omega)$ -decompositions. *Inf. Process. Lett.*, 99(4):154–157, August 2006.
- [59] W. Xu, J. Wang, J. Sun. A projection method for derivation of non-Shannon-type information inequalities. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2116 – 2120, 2008.
- [60] Marcel Wild. Enumeration of binary and ternary matroids and other applications of the brylawski-lucas theorem. *Preprint Nr. 1693, Tech. Hochschule Darmstadt*, 1994.
- [61] X. Yan, R.W. Yeung, and Zhen Zhang. An implicit characterization of the achievable rate region for acyclic multisource multisink network coding. *IEEE Trans. on Inform. Theory*, 58(9):5625–5639, 2012.
- [62] R. W. Yeung. *Information Theory and Network Coding*. Springer, 2008.
- [63] Ying-On Yan and Raymond Yeung. Itip-information theoretic inequality prover, 2008. <http://user-www.ie.cuhk.edu.hk/ITIP/>.
- [64] Yunshu Liu. *Extremal Entropy: Information Geometry, Numerical Entropy Mapping, and Machine Learning Application of Associated Conditional Independences*. PhD thesis, Drexel University, Philadelphia, PA, 2016.
- [65] Yunshu Liu, and John MacLaren Walsh. Mapping the Region of Entropic Vectors with Support Enumeration & Information Geometry. *IEEE Trans. Inform. Theory*. Submitted December 08, 2015.
- [66] Z. Zhang and R W. Yeung. On Characterization of Entropy Function via Information Inequalities. *IEEE Transactions on Information Theory*, 44(4), July 1998.