Algorithms for Computing Network Coding Rate Regions via Single Element Extensions of Matroids

Jayant Apte, Congduan Li, John MacLaren Walsh
Drexel University, Dept. of ECE, Philadelphia, PA 19104, USA
jsa46@drexel.edu, congduan.li@drexel.edu, jwalsh@coe.drexel.edu

***Abstract*—We propose algorithms for finding extreme rays of rate regions achievable with vector linear codes over finite fields $\mathbb{F}_q, q \in \{2,3,4\}$ for which there are known forbidden minors for matroid representability. We use the idea of single element extensions (SEEs) of matroids and enumeration of non-isomorphic matroids using SEEs, to first propose an algorithm to obtain lists of all non-isomorphic matroids representable over a given finite field. We modify this algorithm to produce only the list of all non-isomorphic connected matroids representable over the given finite field. We then integrate the process of testing which matroids in a list of matroids form valid linear network codes for a given network within matroid enumeration. We name this algorithm, which essentially builds all matroids that form valid network codes for a given network from scratch, as *network-constrained matroid enumeration*.**

***Index Terms*—Single emement extensions, rate regions of multi-source network coding problems, region of entropic vectors**

I. Introduction

The rate region for multi-source multicast network coding (MSNC) can be expressed implicitly in terms of the closure of the region of entropic vectors $\overline{\Gamma_N^*}$[1]. A variety of polyhedral inner bounds on $\overline{\Gamma_N^*}$ (not yet completely characterized) have since been found [2], [3], and explicit polyhedral inner bounds on the rate region of MSNC problems can be obtained from these polyhedral inner bounds on $\overline{\Gamma_N^*}$. Since these bounds are polyhedral, they can be described as either the minimal set of bounding halfspaces or as conic hull of set of extreme rays. The goal of rate region computation is to compute the minimal representation (either inequalities or extreme rays) of the associated polyhedron. In this paper we address the problem of computing the extreme ray representations of inner bounds on the rate region obtained from matroid inner bounds which are also achievable with vector linear codes [4].

The expression provided by [1] for the MSNC capacity region is

$$\mathcal{R} = \Lambda\left(\text{proj}_{Y_S}\left(\overline{\text{con}\left(\Gamma_N^* \cap \mathcal{L}_{123}\right)} \cap \mathcal{L}_{45}\right)\right). \qquad (1)$$

For brevity, the notation used in (1) is same as that of [1]. One can compute a polyhedral inner bound on the rate region by substituting $\overline{\Gamma_N^*}$ with a polyhedral inner bound as

$$\mathcal{R}^{in} = \Lambda\left(\text{proj}_{Y_S}\left(\Gamma_N^{poly} \cap \mathcal{L}_{12345}\right)\right). \qquad (2)$$

For basic definitions and terminology regarding matroids we refer to [5]. Let M be a matroid on ground set $E(M)$ of size $N' \geq N$ and $\mathcal{V}$ be the set of random variables (corresponding to sources and messages) in the MSNC problem such that $|\mathcal{V}| = N$. A *matroid-network mapping* is a surjective map $\gamma : E(M) \to \mathcal{V}$, and its inverse image $\gamma^{-1} : \mathcal{V} \to 2^{E(M)} \setminus \phi$ is a *network-matroid mapping*.

Definition 1. A matroid M with rank function r and a matroid-network mapping γ form a *feasible linear network code* if $r(\gamma^{-1}(\cdot))$ satisfies all network constraints $\mathcal{L}_{12345}$ imposed on the entropy $h(\cdot)$ of subsets of random variables by the network in (2).

Now we introduce the two polyhedral inner bounds considered in this paper: Γ_N^q and $\Gamma_{N,k,q}^{\subset space}$. For a matroid M of ground set size N, the ranks of all non-empty subsets of ground set can be stacked to form the rank vector $\mathbf{r}$ of M.

Definition 2. Γ_N^q is the conic hull of rank vectors of all $\mathbb{F}_q$-representable matroids of ground set size N.

Another type of inner bound called subspace inner bound can be obtained by N-partitioning the ground set of size $k \geq N$ matroids and creating a new rank vector by stacking together the ranks of subsets of the partition which is the dimension vector of an N-subspace arrangement.

Definition 3. $\Gamma_{N,k,q}^{\subset space}$ is the conic hull of dimension vectors of all N-subspace arrangements over $\mathbb{F}_q$ that are themselves obtained by N-partitioning the ground set of some $\mathbb{F}_q$-representable matroid on $k \geq N$ elements.

The achievability of rate region $\mathcal{R}^{in}$ computed using bounds in definitions 2 & 3 was established in [4]. We are interested in literally *computing* the polyhedral cones $\mathcal{R}^{in}$, Γ_N^q, and $\Gamma_{N,k,q}^{\subset space}$. Straight-forward ways of computing $\mathcal{R}^{in}$ using polyhedral computation techniques have been discussed in [4].

However, the straight-forward polyhedral computation approach from [4] becomes computationally intractable due to dependency on lists of all non-isomorphic matroids which are very large along with available only for ground set sizes $N \leq 9$[6] and partially for $N = 10$[7]. To motivate the work in this paper, Fig. 1 compares numbers of nonisomorphic matroids forming various matroid bounds on region of entropic vectors. From it, we can observe that there are exponentially more non-isomorphic matroids than there are non-isomorphic binary/ternary representable matroids. A further exponential reduction in number is observed when passing to those non-isomorphic representable matroids with at least one matroid network mapping giving a feasible network code. We expect

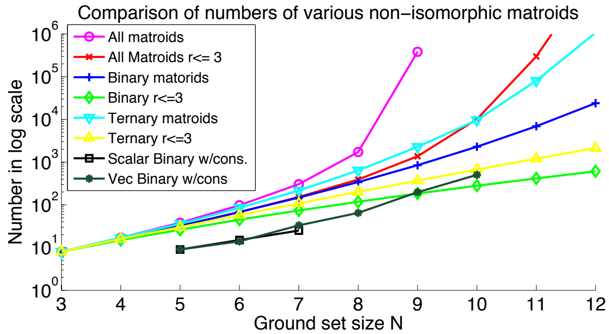

Figure 1: Number of matroids in different polyhedral bounds

that like several other enumeration problems (viz. polyhedral vertex enumeration), the algorithms to enumerate (list) all members of sets in figure 1 to be output sensitive at best. This motivates us to design algorithms for enumerating smaller subsets of all matroids such as those that are representable and obey the constraints imposed by a network. These can be considerably fewer in number as evidenced by the bottom two lines in Fig. 1, which were obtained with the constraints from a small network coding problem.

For these reasons, we seek to design algorithms to solve following problems (note that $q \in \{2,3,4\}$):

(P1) List all non-isomorphic matroids forming Γ_N^q
(P2) List all non-isomorphic extreme rays of Γ_N^q
(P3) List all non-isomorphic matroids forming bounds $\Gamma_N^q \cap \mathcal{L}_{12345}$ and $\Gamma_{N,k,q}^{\subset space} \cap \mathcal{L}_{12345}$

For this purpose we explore matroid enumeration using SEEs which has been a prevalent technique for general matroid enumeration. A SEE of a matroid M is a matroid N such that M can be obtained by a single element deletion from N [5]. The works [8], [6] and [7] use the idea of SEEs to enumerate and list non-isomorphic matroids. All three algorithms use SEEs to construct size n matroids from size $n-1$ matroids which is done recursively. Specifically, the algorithm of [7] performs only those SEEs that lead to non-isomorphic matroids, thus saving a lot of computation.

To solve (P1), in §II we adapt the non-isomorphic matroid enumeration algorithm of [7] to enumerate exclusively those matroids representable over fields $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_4$. To solve problem (P2) we use the relationship between matroid connectivity and the extremality of its rank vector in §III. In §IV we propose a technique that finds all possible mappings between k-partition of ground set of a matroid and k variables in the network under which given matroid forms valid network code for given network coding problem. We call this technique *constraint permutation*. In V we propose the *network constrained enumeration* algorithm, which solves (P3). The definitions of SEEs, modular cut and $\mathbb{F}_q$-representability are in [5] (pp. 264, 266 & 12 resp.) while the definitions of reverse lexicographic order, canonical matroid, taboo flat and mechanism for obtaining encoding of canonical SEE of a canonical matroid are in [7] (pp. 33,34).

II. Enumerating matroids representable over a specific field

To solve (P1) using matroid enumeration, we integrate the test for $\mathbb{F}_q$-representability into the matroid enumeration algorithm proposed in [7]. A matroid is $\mathbb{F}_q-$representable if and only if all of its minors are $\mathbb{F}_q-$representable. One way to characterize $\mathbb{F}_q$-representable matroids is by listing *forbidden* or *excluded* minors. ([5] , pg 193). For instance, a matroid is binary if and only if it has no U_4^2-minor [5]. Similar characterizations exist for $\mathbb{F}_3$ and $\mathbb{F}_4$. The recently announced proven [9] Rota's conjecture asserts that for any finite $q > 0$ there is a finite collection of forbidden minors [10]. Such characterizations are fortuitous for directly enumerating $\mathbb{F}_q$-representable matroids for $q \in \{2,3,4\}$ because if matroid M has a minor K and if N is an SEE of M, then K is also a minor of N. This in turn implies, for $q \in \{2,3,4\}$ if a matroid M is not $\mathbb{F}_q$-representable, then its SEE is also not $\mathbb{F}_q$-representable. Hence, we can embed a minor checking test into a SEE based non-isomorphic matroid enumeration algorithm [7] removing at each new ground set size all of those newly extended matroids which have the forbidden minors because any further extensions along them will still have the forbidden minors, and thus not be representable. Algorithm

Input: Lists $\mathscr{M}_{n-1}^r, \mathscr{M}_{n-1}^{r-1}$ of nonisomorphic matroids
Output: List $\mathscr{M}_n^r$ of $\mathbb{F}_q$-representable matroids

```
1  𝓜_n^r ← φ
2  foreach M ∈ 𝓜_{n-1}^r do
3      foreach Modular cut 𝒜(≠ φ) of M do
4          if 𝒜 has no taboo flat then
5              N ← M +_𝒜 e_n
6              if N has F_q forbidden minors then
7                  𝓜_n^r ← 𝓜_n^r ∪ N
8              end
9          end
10     end
11 end
12 foreach M ∈ 𝓜_{n-1}^{r-1} do
13     N ← M +_φ e_n
14     if N has F_q forbidden minors then
15         𝓜_n^r ← 𝓜_n^r ∪ N
16     end
17 end
18 return 𝓜_n^r
```

Algorithm 1: $\mathbb{F}_q$ representable matroid enumeration

1 does exactly this, mimicking [7] except in lines 6 and 14, where matroids that are not $\mathbb{F}_q$-representable are discarded. Note: The notation $M +_{\mathcal{M}} e$ is borrowed from [5], pg 269 and refers to SEE of matroid M with modular cut $\mathcal{M}$

III. Enumerating connected matroids

Connectivity is a property some matroids exhibit that turns out to be important for solving problem (P2). Below, $\mathsf{extr}(\mathcal{C})$ is the set of extreme rays of polyhedral cone $\mathcal{C}$, $r_M(\cdot)$ is the rank function of matriod M and CM is the class of connected matroids.

Definition 4. Connectivity[11]: A matroid $M = (E, \mathcal{I})$ belongs to class CM if for every proper subset U of E $r_M(U) + r_M(E \setminus U) > r_M(E)$.

Prior work by Li. et al. [3] showed that:

Theorem 1. *(Li et. al.[3]) If* $\mathbf{r} \in \textit{extr}(\Gamma_N^q)$*, then* $\mathbf{r}$ *is rank vector of some matroid* $M \in CM$.

Definition 3 and following theorem mean that $\text{extr}(\Gamma_{N,k,q}^{\subset space})$ can be obtained from size k connected matroids.

Theorem 2. *Every* $\mathbf{d} \in \textit{extr}(\Gamma_{N,k,q}^{\subset space})$ *can be obtained as linear projection of some* $\mathbf{r} \in \textit{extr}(\Gamma_k^q)$

Lemmas 1 and 2 prove that the class CM is closed under SEE.

Lemma 1. *If* $M \in CM$ *with non-empty modular cut* $\mathcal{M}$ *and* $N = M +_{\mathcal{M}} e$*, then* $N \in CM$.

Proof: Note that rank of matroid $M +_{\mathcal{M}} e$ is $r_M(E)+1$ if and only if $\mathcal{M} = \phi$ ([5], pg 269). Hence when $\mathcal{M} \neq \phi$, $M +_{\mathcal{M}} e$ has the same rank as M. Further, for any $U \subsetneq E \cup e$,

$$\begin{aligned} r_N(U) + r_N(\{E \cup e\} \setminus U) &\geq r_M(U) + r_M(E \setminus U) \\ &> r_M(E) = r_N(E \cup e) \quad \blacksquare \end{aligned}$$

Lemma 2. *If* $M \in CM$ *and* $N = M +_{\mathcal{M}} e$ *with* $\mathcal{M} = \emptyset$*, then* $N \in CM$

Proof: This can be proved by following series of inequalities:

$$\begin{aligned} r_N(U) + r_N(\{E \cup e\} \setminus U) &\geq^{(a)} r_M(U) + r_M(E \setminus U) + 1 \\ &> r_M(E) + 1 = r_N(E \cup e) \end{aligned}$$

where (a) follows from the fact that WLOG, we can assume $e \notin U$ and since $\{E \cup e\} \setminus U = (E \setminus U) \cup e$, $r_N(\{E \cup e\} \setminus U) = r_M(E \setminus U) + 1$ by theorem 7.2.3([5]). ■

Since class CM is closed under SEE, if we start with lists $\mathscr{C}_{n-1}^r$ and $\mathscr{C}_{n-1}^{r-1}$ of all non-isomorphic connected matroids of ground set size $n-1$, rank r and ground size $n-1$, rank $r-1$ respectively and perform canonical extensions with non-empty and empty modular cuts respectively, the resultant extensions will all be connected. Unfortunately the list of size n, rank r matroids so obtained is not exhaustive, as is evidenced by the uniform matroid U_n^{n-1}. Any single element deletion of this matroid will produce U_{n-1}^{n-1} which is not a connected matroid, and hence U_n^{n-1} falls into the critical class of UCM matroids defined below.

Definition 5. Unreachable Connected Matroids(UCM) are a subclass of connected matroids M that are connected but all deletions of them $M \setminus e, e \in E(M)$ are not connected.

Connected matroid enumeration will depend on matroid duality and a theorem by Tutte:

Theorem 3. *([5], pg 123) A matroid* M *is connected if and only if its dual is connected.*

Theorem 4. *(Tutte[12], [5], pg 126) If* M *is a connected matroid then, for every* $e \in E(M)$ *at least one of* $M \setminus e$ *or* M/e *are connected.*

Theorem 4 tells us that any matroid $M \in UCM$ has at least one single element contraction that is connected. We also know that $M/e = (M^* \setminus e)^*$. Note that M^* and $M^* \setminus e$ are connected since they are duals of connected matroids. This leads us to the following lemma:

Lemma 3. *If a matroid* $M \in UCM$*, then its dual* $M^* \notin UCM$

Hence, if $M \in UCM$, M^* can be obtained via extension of a connected matroid. To find size n rank r connected matroids, we present an algorithm that uses lists of non-isomorphic connected matroids $\mathscr{C}_{n-1}^r, \mathscr{C}_{n-1}^{r-1}, \mathscr{C}_{n-1}^{n-r}, \mathscr{C}_{n-1}^{n-r-1}$ and produces lists of non-isomorphic connected matroids $\mathscr{C}_n^r$ and $\mathscr{C}_n^{n-r}$. Given a set of canonical matroids A denote by $\text{see}(A)$ the set of all canonical SEEs of matroids in A.

Input: Lists $\mathscr{C}_{n-1}^r, \mathscr{C}_{n-1}^{r-1}, \mathscr{C}_{n-1}^{n-r}, \mathscr{C}_{n-1}^{n-r-1}$ of connected matroids
Output: Lists $\mathscr{C}_n^r$ and $\mathscr{C}_n^{n-r}$ of connected matroids
1 $\mathscr{C}_n^r \leftarrow \phi$
2 $\mathscr{C}_n^{n-r} \leftarrow \phi$
3 $\mathscr{C}_n^r \leftarrow \text{see}(\mathscr{C}_{n-1}^r) \cup \text{see}(\mathscr{C}_{n-1}^{r-1})$
4 $\mathscr{C}_n^{n-r} \leftarrow \text{see}(\mathscr{C}_{n-1}^{n-r}) \cup \text{see}(\mathscr{C}_{n-1}^{n-r-1})$
5 $\mathscr{C}_n^r \leftarrow \text{unique}(\mathscr{C}_n^r \cup \text{minrevlex}(\text{dual}(\mathscr{C}_n^{n-r}))$
6 $\mathscr{C}_n^{n-r} \leftarrow \text{unique}(\mathscr{C}_n^{n-r} \cup \text{minrevlex}(\text{dual}(\mathscr{C}_n^r))$
7 **return** $\mathscr{C}_n^r$ *and* $\mathscr{C}_n^{n-r}$

Algorithm 2: Connected matroid enumeration

Algorithm 2 performs connected matroid enumeration. At the end of line 4 the lists $\mathscr{C}_n^r$ and $\mathscr{C}_n^{n-r}$ produced do not have UCM matroids. From Lemma 3 we know that matroids isomorphic to the duals of UCM matroids of size n and rank r are present in the list $\mathscr{C}_n^{n-r}$ while matroids isomorphic to duals of UCM matroids of size n rank $n-r$ are present in the list $\mathscr{C}_n^r$. Hence lines 5 and 6 find dual matroids of $\mathscr{C}_n^{n-r}$ and $\mathscr{C}_n^r$ respectively. The encoding of these duals may not be canonical(i.e. if a matroid is canonical then its dual is not necessarily canonical). To counter this difficulty, we use procedure $\text{minrevlex}(A)$ which given a set of matroids A returns the canonical encodings of each matroid in A. Finally, procedure $\text{unique}(.)$ removes extra copies of matroids that will be produced as a result of taking the dual.

While enumerating all connected matroids might be of interest to some, we are interested in enumerating all connected matroids that are representable over certain $\mathbb{F}_q, q \in \{2, 3, 4\}$ and solving problem (P2). To that end, we can replace procedure $\text{see}(A)$ by $\text{see}(A, q)$ i.e. one that only produces canonical SEEs that are representable over $\mathbb{F}_q$, by removing any SEEs that have forbidden minors, along the lines of algorithm 1. In that case, only $\mathbb{F}_q$-representable connected matroid lists would suffice as input to the algorithm which is due to the fact that if a matroid is representable over $\mathbb{F}_q$ its dual is also representable over $\mathbb{F}_q$ ([5], pg 193). Hence, the duals of size n and rank r $\mathbb{F}_q$-representable UCM matroids are present in the list $\mathscr{C}_n^{n-r}$ produced at line 4 and we obtain the complete size n rank r connected matroid list in line 5.

IV. Constraint permutation

The matroid to network mapping γ creates a partition $\mathcal{P}$ of $E(M)$ containing sets $P_1, \ldots, P_N$. The goal of constraint permutation is, to find for a given matroid M and pre-specified partition sizes $b_1, \ldots, b_N$, all matroid to network mappings γ such that (M, γ) forms a feasible linear network code for a given N-variable MSNC problem on a directed graph $\mathcal{G} = (V_{\mathcal{G}}, E_{\mathcal{G}})$. A naive method of doing this forms all $\binom{|E(M)|}{b_1, b_2, \ldots, b_N} \cdot N!$ possible mappings γ then checks all $|V_{\mathcal{G}}| + 1$ network constraints for each one yielding $\binom{|E(M)|}{b_1, b_2, \ldots, b_N} \cdot N!(|V_{\mathcal{G}}| + 1)$ total constraint tests. However, the $N! \cdot (|V_{\mathcal{G}}| + 1)$ part can be bettered by using constraint permutation.

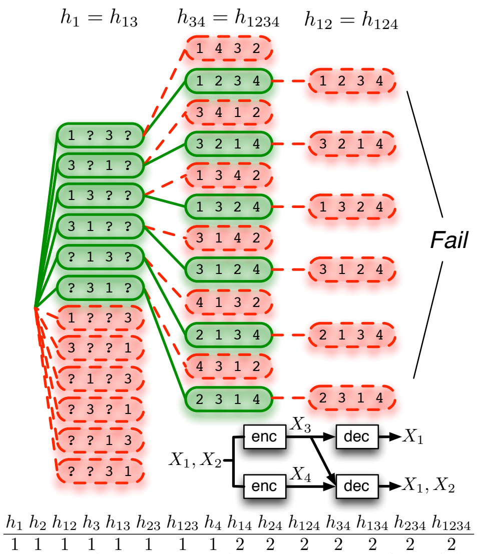

Figure 2: Constraint permutation on a matroid with the specified rank vector. The partition sizes $b_i = 1, \forall i \in [N]$

Definition 6. A **partial permutation** of $\mathcal{P}$ is a bijective map $\phi : S_\phi \to S'_\phi$ for some $S_\phi \subseteq \mathcal{P}, S'_\phi \subseteq \{1, \ldots, N\}$

We represent partial permutations by M-strings, e.g. if $N = 5$ an example is $< 1, 2, 3, ?, ? >$. The number i in j^{th} position means $p_j \mapsto i$: i.e. partition p_j maps to variable labeled i. The "?" stands for "we don't know yet". We call partial permutation $\phi' : S_{\phi'} \to S'_{\phi'}$ an extension of partial permutation $\phi : S_\phi \to S'_\phi$ if $S_\phi = S_{\phi'} \setminus \{A\}$ for some $A \in \mathcal{P} \setminus S_\phi$. A partial permutation ϕ is said to *define a variable* $v \in [N]$ if $v \in S'_\phi$.

Consider a set of network coding constraints $c_1, \ldots, c_n$. Let $V_{c_i}, i \in [n]$ be the variables appearing in constraint c_i. Given an order on constraints i.e. $c_i < c_j$ if $i < j$, we seek to find the number of constraint tests required for finding all valid labelings a given partition of ground set of a matroid. Define the sets of free variables $F_1, \ldots, F_n$ where $F_i = V_{c_i} \setminus \bigcup_{j=1}^{i-1} V_{c_j}$. To avoid creating $N!$ dimension vectors corresponding to isomorphs of subspace arrangelemt $M^{\mathcal{P}}$ created by partion $\mathcal{P}$, one can test the same subspace dimension vector under *versions of the same constraint created by certain partial permutations*. e.g. constraint $H(X_1, X_2, X_3) = H(X_1, X_2)$ under $<?, ?, ?, 1, 2, 3>$ becomes $H(X_4, X_5, X_6) = H(X_4, X_5)$. Overall, we need to test under all partial permutations ϕ with $S'_\phi = \{1, 2, 3\}$. Hence, finding all permutations satisfying a constraint c_i would require $\binom{N}{|V_{c_i}|}.|V_{c_i}|!$ constraint tests. Instead of testing for a single constraint, we need to test satisfaction of a set of constraints. This can be achieved via a tree like mechanism of constraint tests on partial permutations as explained in Fig. 2. At depth i, we test the rank vector under versions of ith constraint that are obtained under partial permutations that *define* variables $\bigcup_{j \in [i]} F_j$. These partial permutations are themselves obtained as extensions of partial permutations that *define* variables $\bigcup_{j \in [i-1]} F_j$ and satisfy constraints $V_{c_i}, i \in [i-1]$ Hence we obtain a tighter upper bound on number of tests that must be performed per N-partition of ground set,i.e. the multinomial coefficient, $t = \binom{N}{|F_1|, \ldots, |F_n|}$ which is a substantial reduction relative to $N!$.

V. Network Constrained enumeration

In this section, we propose an algorithm to solve problem (P3), called *network constrained enumeration*. First, we define the concept of partial network to matroid mapping ξ.

Definition 7. Partial matroid-network mapping ξ from the ground set of matroid M to set of network variables $\mathcal{V}$ is a not necessarily surjective map $\xi : E(M) \to \mathcal{V} \cup v_\phi$

Here v_ϕ is the empty variable. We abbreviate partial matroid-network mapping as p-map. Given a p-map ξ, we say that a variable $v \in \mathcal{V}$ is defined if there exists $e \in E(M)$ s.t. $\xi(e) = v$ otherwise, it is undefined. For the variables $v \in \mathcal{V}$ that are defined $\xi^{-1}(v)$ is the set of all $e \in E(M)$ s.t. $\xi(e) = v$. A p-map can also be empty i.e. $\xi(e) = v_\phi \; \forall e \in E(M)$. Now we define partially feasible network code (p-code).

Definition 8. A matroid M with a p-map ξ is a **Partially Feasible Linear Network Code** (p-code) if $r_M(\xi^{-1}(\cdot))$ satisfies all network constraints imposed on the entropy $h(\cdot)$ of subsets of *defined* random variables by the network.

Similar to general matroid enumeration algorithm in [7], the network constrained enumeration would begin with the matroid defined on the empty set and the empty p-map and perform SEEs of matroids thus adding one element every iteration to ground the set. However, instead of producing at the end of the process a list of all non-isomorphic matroids, we wish only to enumerate those non-isomorphic $\mathbb{F}_q$-representable matroids M which, together with some surjective matroid-network mapping $\gamma(\cdot)$, form a feasible linear network code for the network. When we are finished, for each such network constrained matroid M in the list, we wish to have a list of all matroid-network maps γ_k such the pair (M, γ_k) form a feasible linear network code. For this reason, the SEE based algorithm will operate on lists $\mathcal{L}_n$ whose elements are pairs $(M, \mathcal{Q}^M)$ of a non-isomorphic matroid M with a list $\mathcal{Q}^M$ of all p-maps such that (M, ξ) form a p-code.

Definition 9. A p-map ξ_1 is said to be an **extension** of a p-map ξ_2, denoted by $\xi_2 \subseteq \xi_1$ if $\xi_2(E(M)) \setminus v_\emptyset \subseteq \xi_1(E(M)) \setminus v_\emptyset$ and for all $v \in \xi_2(E(M)) \setminus v_\emptyset$, $\xi_1^{-1}(v) = \xi_2^{-1}(v)$. In this instance, we also say that ξ_2 is a **deletion** of ξ_1.

Definition 10. Given a set Ξ of p-maps, $\Xi' \subseteq \Xi$ is said to be **extension maximal** subset if every $\xi \in \Xi$ can be obtained as deletion of some $\xi' \in \Xi'$.

Hence, for every matroid, it suffices to maintain only a list of extension maximal p-maps that yield p-codes. At the nth iteration, the algorithm will find every matroid M in the class of non-isomorphic matroids (the canonical matroids) that is a single element extension of M' (the parent matroid) available from $n-1$th iteration that is $\mathbb{F}_q$ representable, along with the set $\mathcal{Q}^M$ containing every p-map ξ such that (M,ξ) forms a p-code. Each such p-map ξ will be an extension of some $\xi' \in \mathcal{Q}^{M'}$, a p-map that forms a p-codewith the parent matroid.

Algorithm 3 is the network constrained matroid enumeration algorithm. It takes as input an MSNC problem and N^*, the maximum ground set up to which matroid enumeration is allowed to continue. Let $E(M) = E(M') \cup \{e_n\}$, so that $\{e_n\}$ is the new ground set element the extension created. To create $\mathcal{Q}^M$ from $\mathcal{Q}^{M'}$, we use procedure extendpmaps$(M, M', \mathcal{Q}^{M'})$. This procedure makes use of a function candidates which forms the list of unique deletions of a list of p-map which, at the current stage in the matroid extension process, could still be extended in the remaining $N^* - |E(M)|$ extension rounds in a way that would define all of the random variables in the network. Mathematically, this function can be expressed as

$$\text{candidates}(\mathcal{Q}^{M'}) = \left\{ \xi \,\middle|\, \begin{array}{l} |\xi(E(M')) \setminus v_\phi| \geq |\mathcal{V}| - (N^* - |E(M')| + 1) \\ \text{and } \exists\ \xi' \in \mathcal{Q}^{M'} \text{ such that } \xi \subseteq \xi' \end{array} \right\} \quad (3)$$

Such a process will find all extension maximal p-maps that, together with the matroid M will form a p-code.

Input: A N-variable MSNC problem and maximum ground set size N^*
Output: All pairs (M,ξ) such that M is a non-isomorphic (canonical) matroid with $N \leq E(M) \leq N^*$ and (M,ξ) is a feasible linear network code

$\mathscr{M}^0 \leftarrow \{$matroid M^ϕ on empty set$\}$
$\mathcal{Q}^M \leftarrow \{$ empty p-map$\}$
for $i \in \{1, \ldots, N^*\}$ **do**
  $\mathscr{M}^i \leftarrow \text{see}(\mathscr{M}^{i-1}, q)$
  foreach $M \in \mathscr{M}^i$ **do**
    $M' \leftarrow$ parent matroid of M
    $\mathcal{Q}^M \leftarrow \text{extendpmaps}(M, M', \mathcal{Q}^{M'})$
    if $\mathcal{Q}^M$ *is empty* **then**
      $\mathscr{M}^i \leftarrow \mathscr{M}^i \setminus M$
    end
    foreach $\xi \in \mathcal{Q}^M$ **do**
      if (M,ξ) *is a feasible linear network code* **then**
        Output (M,ξ)
      end
    end
  end
end
return

Algorithm 3: ncmatenum

$\mathcal{Q}^M \leftarrow \emptyset$
$e_n \leftarrow E(M) \setminus E(M')$
foreach $\xi_i \in$ *candidates*$(\mathcal{Q}^{M'})$ **do**
  foreach $\mathcal{U} \subseteq \xi_i^{-1}(v_\emptyset)$ **do**
    foreach $v \in \mathcal{V} \setminus \xi_i(E(M))$ **do**
      form ξ_o s.t. $\xi_o : E(M) \to \mathcal{V}$ such that $\xi_o(e) = \xi_i(e)\ \forall e \in E(M) \setminus (\{e_n\} \cup \xi_i^{-1}(v_\emptyset) \setminus \mathcal{U})$ and $\xi_o(e) = v\ \forall e \in \mathcal{U} \cup e_n$
      if (M, ξ_o) *is a p-code* **then**
        $\mathcal{Q}^M \leftarrow \mathcal{Q}^M \cup \xi_o$
      end
    end
  end
end
return $\mathcal{Q}^M$

Procedure extendpmaps$(M, M', \mathcal{Q}^{M'})$

VI. Conclusions

In this paper, motivated by demonstrated huge reductions in complexity for calculating MSNC achievable rate regions, we presented new methods to directly enumerate non-isomophic: 1) representable matroids, 2) extremal representable matroids, and 3) representable matroids capable of being mapped onto a network and obeying its constraints.

Acknowledgments

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

References

[1] 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.

[2] J. M. Walsh and S. Weber. Relationships among bounds for the region of entropic vectors in four variables. In *2010 Allerton Conference on Communication, Control, and Computing*, September 2010.

[3] Congduan Li, John MacLaren Walsh, Steven Weber. Matroid bounds on the region of entropic vectors. In *51th Annual Allerton Conference on Communication, Control and Computing*, October 2013.

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

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

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

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

[8] John E. Blackburn, Henry H. Crapo, and Denis A. Higgs. A catalogue of combinatorial geometries. *Mathematics of Computation*, 27(121):pp. 155–166, 1973.

[9] Rota's Conjecture: Researcher solves 40-year-old math problem. phys.org article posted Aug 15, 2013.

[10] 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.

[11] Alexander Schrijver. *Combinatorial optimization: polyhedra and efficiency*, volume 24. Springer, 2003.

[12] WT Tutte. Connectivity in matroids. *Canad. J. Math*, 18:1301–1324, 1966.