Algorithms for computing limits on information flow and storage in networks

Jayant Apte (Advisor: John Walsh)

Department of Electrical and Computer Engineering
Drexel University, Philadelphia

10th August, 2016

Outline

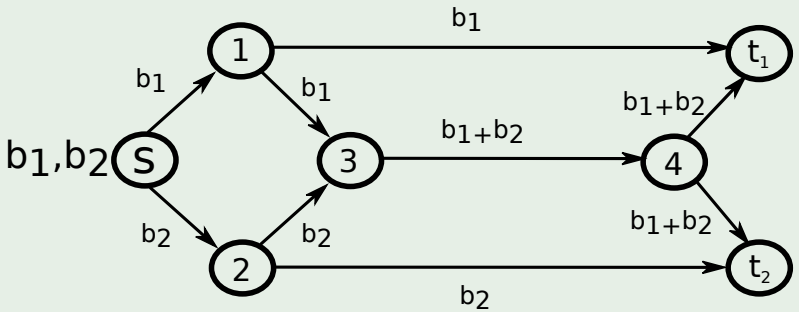
1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

Network coding (Single Multicast)

- Introduced by Ahlswede et. al. in 2000 [ACLY00].

Example



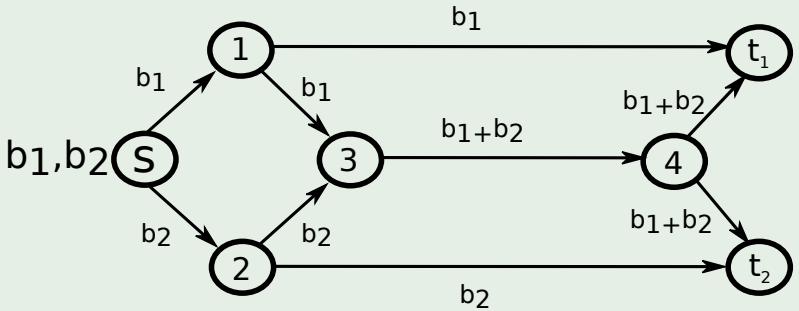
Single Multicast: The Butterfly Network

- Directed acyclic multigraph with one source and multiple sinks.
- Each edge has a non-negative capacity.
- Nodes can code (compute a function of inputs and forward the result).
- Routing rate = 1.5, Network Coding rate = 2.

Network coding (Single Multicast)

- Introduced by Ahlswede et. al. in 2000 [ACLY00].

Example



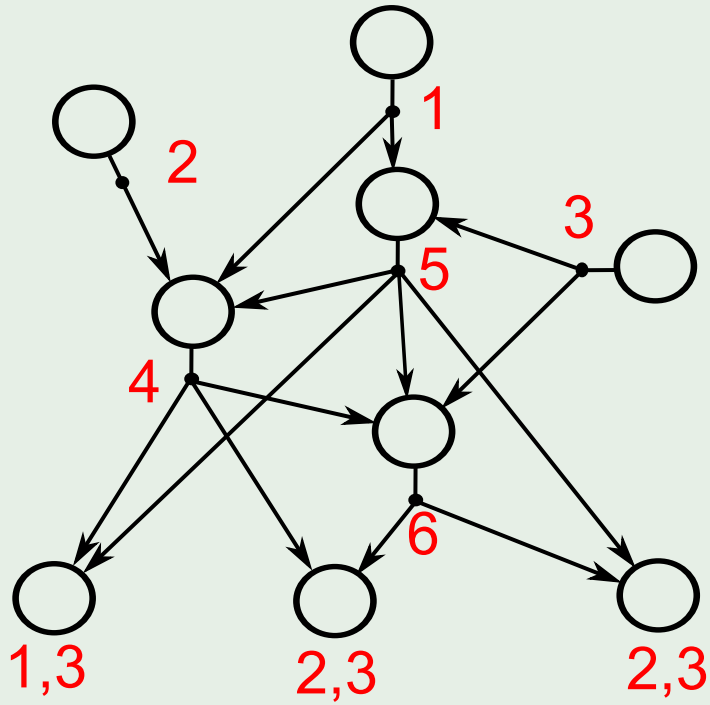
Single Multicast: The Butterfly Network

- Polynomial time deterministic [JSC+05] and randomized [HMK+06] algorithms for code construction.
- Cut-set bounds (max-flow min-cut thm.) are tight [Yeu08].
- Linear coding suffices to achieve optimum multicast rate [Yeu08].

The General Problem: HMSNC

- Multi-source Multi-sink Network Coding over Directed Acyclic Hypergraphs
- Multiple independent sources
- Multiple sinks demanding subsets of source messages
- Directed hyperedges carry same message to different nodes

Example



HMSNC instance HN1

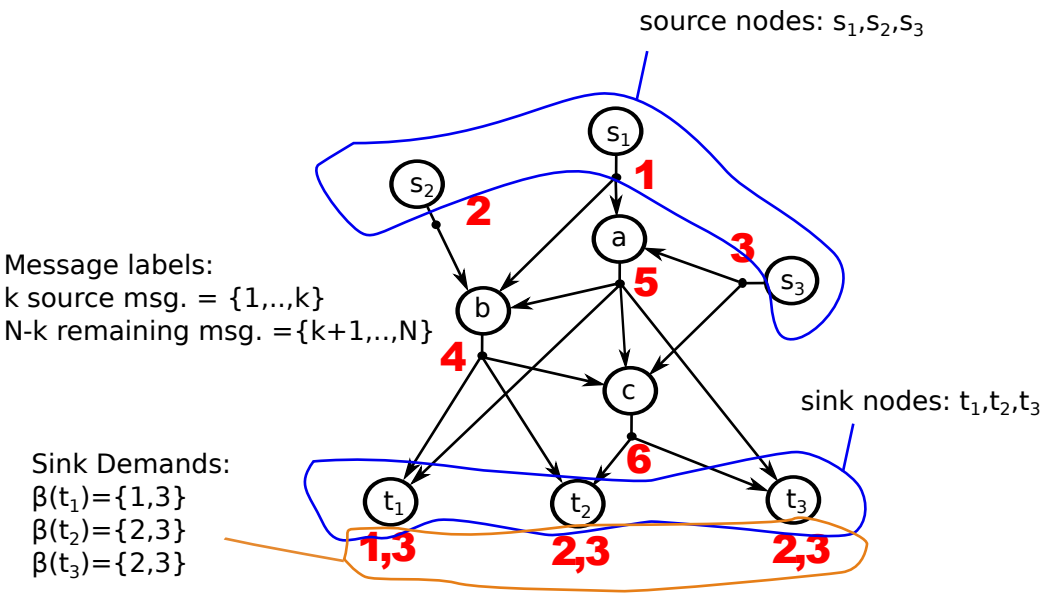
The curious case of HMSNC

- There exist network instances that require non-linear network codes to achieve the vector of optimum information transfer rates for the sources [DFZ05],
- Cut-set bounds are loose [Yeu08],
- There exist network instances for which determining the vector of optimum information transfer rates for the sources requires *new laws of information theory*, called the non-Shannon-type information inequalities [DFZ07],
- The problem of determining the *scalar linear capacity* is NP-hard [LL04].

Drexel UNIVERSITY

HMSNC: formal definition

- A HMSNC instance A is completely described by the tuple $\mathrm{A} = (\mathscr{S}, \mathscr{G}, \mathscr{T}, \mathscr{E}, \beta)$.
- A directed acyclic hypergraph $(\mathscr{V}, \mathscr{E})$ with $\mathscr{V} = \mathscr{S} \cup \mathscr{T} \cup \mathscr{G}$
- $\mathscr{E}$ is the set of directed hyperedges of the form $(v, \mathscr{A})$ where $v \in \mathscr{V}, \mathscr{A} \subseteq \mathscr{V} \setminus \{v\}$.



HMSNC Constraints

- 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.
- Entropy function $\mathbf{h}$ maps any probability mass function for $\mathbf{X_N}$ to $\mathbb{R}^{2^N-1}$. Constraints on the entropy function: $\mathcal{I}_\mathsf{A} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$

$$\mathbf{h}_{[k]} = \sum_{i \in [k]} \mathbf{h}_k \qquad \text{(source independence)}$$

Form set $\mathcal{L}_1$ containing only the above constraint.

$$\mathbf{h}_{\mathsf{In}(g) \cup \mathsf{Out}(g)} = \mathbf{h}_{\mathsf{In}(g)},\ \forall g \in \mathscr{G} \qquad \text{(node constraints)}$$

Collect node constraints in a set $\mathcal{L}_2$.

$$\mathbf{h}_{\mathsf{In}(t) \cup \beta(t)} = \mathbf{h}_{\mathsf{In}(t)},\ \forall t \in \mathscr{T}. \qquad \text{(decoding constraints)}$$

The decoding constraints are collected in a set $\mathcal{L}_3$.

HMSNC: Network Codes

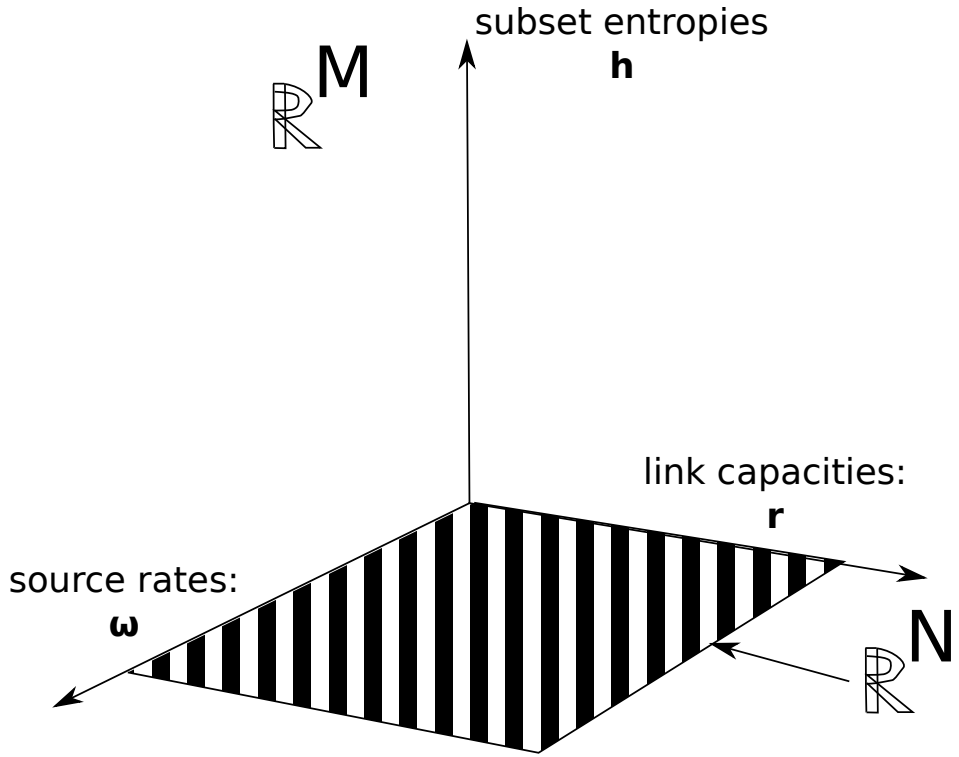
A network code

Definition

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 $\mathcal{I}_{\mathrm{A}}$.

HMSNC: Rate Regions

- Let $\mathbb{R}^M$ be the space with subset entropies $\mathbf{h}_A, A \subseteq [N]$, source rate variables $\boldsymbol{\omega} = (\omega_i \mid i \in [k])$, and edge capacity variables $\mathbf{r} = (R_j \mid j \in [N] \setminus [k])$ as co-ordinates, i.e. $M = 2^N - 1 + N$.
- *rate vector* to is any vector $(\widetilde{\boldsymbol{\omega}}, \widetilde{\mathbf{r}}) \in \mathbb{R}^N$, obtained by concatenating a specified vector of source rates $\widetilde{\boldsymbol{\omega}}$ and a specified vector of edge capacities $\widetilde{\mathbf{r}}$.
- The achievable rate region of a HMSNC instance is the set of all rate vectors $(\widetilde{\boldsymbol{\omega}}, \widetilde{\mathbf{r}}) \in \mathbb{R}^N$, for which there exists a block code with a diminishing probability of error.



HMSNC: Rate Regions via the Entropy Function Region

A vector $\widetilde{\mathbf{h}} \in \mathbb{R}^{2^N-1}$ is entropic if is arises from a valid N-variate probability mass function via the entropy function. Define the region of entropic vectors as $\Gamma^*_N \triangleq \{\widetilde{\mathbf{h}} \in \mathbb{R}^{2^N-1} \mid \widetilde{\mathbf{h}} \text{ is entropic } \}$.

Implicit characterization of the rate region

Result of Yan et.al.[YYZ12], and Li et.al[Con]

$$\mathcal{R}^* = \text{proj}_{\boldsymbol{\omega},\mathbf{r}}(\overline{\text{con}(\Gamma^*_N \cap \mathscr{L})} \cap \mathscr{L}')$$

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

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

$$\mathscr{L}' \triangleq \left\{ (\widetilde{\mathbf{h}}, \widetilde{\boldsymbol{\omega}}, \widetilde{\mathbf{r}}) \in \mathbb{R}^M \;\middle|\; \begin{array}{l} (\widetilde{\mathbf{h}} \text{ satisfies } \mathcal{L}_3) \\ \wedge(\widetilde{\mathbf{r}}_i \geq \widetilde{\mathbf{h}}_i, \forall i \in [N] \setminus [k]) \\ \wedge(\widetilde{\boldsymbol{\omega}}_i \leq \widetilde{\mathbf{h}}_i, \forall i \in [k]) \end{array} \right\}$$

What do we know about Γ_N^*?

One line answer: very little!

- Its closure $\overline{\Gamma_N^*}$ is a convex cone.
- Γ_N^* is not yet fully characterized for $N \geq 4$.
- The known partial characterizations are in the form of linear information inequalities. An information inequality for N discrete random variables is an inequality of the following form,

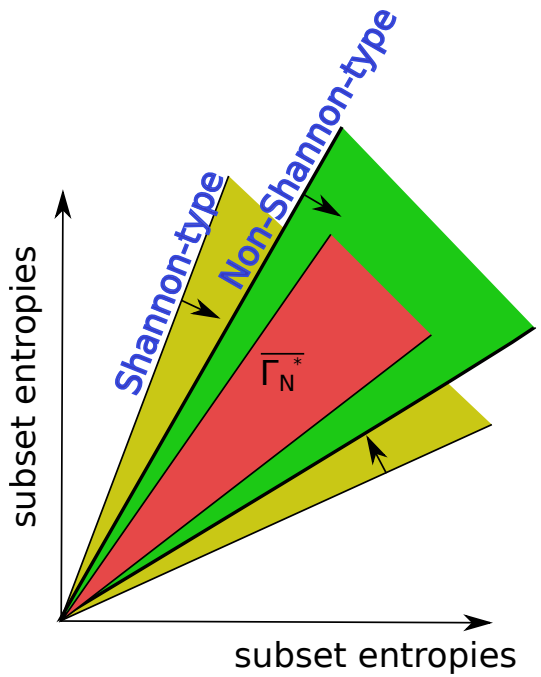
$$\sum_{A \subseteq [N]} \lambda_A \mathbf{h}_A \geq 0$$

where $\lambda_A \in \mathbb{R}$ for all $A \subseteq [N]$, that is satisfied by every entropic vector $\mathbf{h} \in \Gamma_N^*$.

What do we know about Γ_N^*?

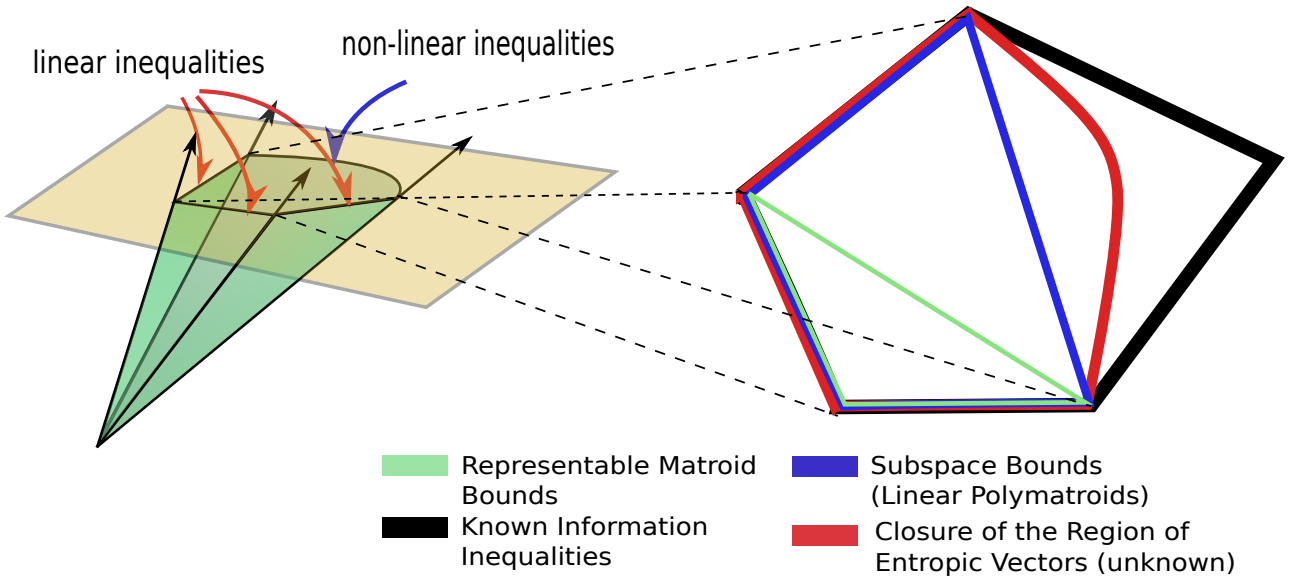
One line answer: very little!

- Entropy function satisfies polymatroidal axioms [Fuj78] and any consequences of them, which are also called the Shannon-type information inequalities.
- Inequalities not implied by the polymatroidal axioms, that are satisfied by all entropic vectors exist and are called the non-Shannon type information inequalities. The first such inequality was found by Zhang and Yeung [Z. 98].
- Hundreds of linear non-Shannon type inequalities have been found since the Zhang-Yeung inequality [DFZ11, Csi13].
- Matús [F. 07] has shown that for $N \geq 4$, an infinite number of linear information inequalities is necessary to determine $\overline{\Gamma_N^*}$.



How to characterize HMSNC rate regions?

Compute sandwich bounds. If they match, declare victory!



Sandwich Bounds

$$\mathcal{R}_{\mathsf{x}} = \mathrm{proj}_{\boldsymbol{\omega},\mathbf{r}}(\Gamma_{\mathsf{x}} \cap \mathscr{L} \cap \mathscr{L}'), \mathsf{x} \in \{\mathsf{in},\mathsf{out}\}$$

The traditional (no computer assistance) approach

- **Outer Bounds**: Invoke known information inequalities one by one to arrive at a set of inequalities bounding the rate region.
- **Inner bounds**: Construct codes for achieving every extreme point of the outer bound based on intuition. If this fails, try constructing a tighter outer bound.

What is wrong with this?

- Can take hours to prove one rate region.
- No general technique is known to find putative inequalities bounding the rate regions.
- No general technique is known for computing rate region inner bounds achievable with a specific class of codes.

Here are the putative inequalities bounding the rate region. Are you sure you want to spend all your wishes on these?. - Genie

This thesis

- **Inner Bounds**: Algorithms for computing inner bounds on rate regions achievable with a given class of linear codes based on combinatorial generation. These can be also used to test the achievability of a specific rate vector with a specified class of linear codes.
- **Outer Bounds**: Algorithms for computing the tightest collection of inequalities bounding the rate region implied by a specified set of linear information inequalities.
- **Software tools**: Two open-source software projects, Information Theoretic Achievability Prover (ITAP) and Information Theoretic Converse Prover (ITCP), implementing the algorithms developed.

Drexel UNIVERSITY

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

Subspace arrangements

Definition

A subspace arrangement in a k-dimensional vector space $V = \mathbb{K}^k$ over some field $\mathbb{K}$ is a multiset of N subspaces $\mathscr{S} = \{V_1, V_2, \ldots, V_N\}$ with $V_n \subseteq V \ \forall n \in [N]$. The rank function of the subspace arrangement is $\mathrm{rk} : 2^{[N]} \to \mathbb{Z}$ defined as

$$\mathrm{rk}(\mathscr{I}) \triangleq \dim \sum_{i \in \mathscr{I}} V_i, \quad \forall \mathscr{I} \subseteq [N]$$

- Every rk is a polymatroid.
- We call polymatroids arising this way *linear polymatroids*.
- Every rk is in $\overline{\Gamma^*_N}$ [HRAS00].(Converse is not true)

Representation of a linear polymatroid

- If a polymatroid arises from a subspace arrangement over $\mathbb{F}_q$, we call it $\mathbb{F}_q$-representable or $\mathbb{F}_q$-linear.

Definition

A representation of a $\mathbb{F}_q$-representable polymatroid $([N], f)$ associated with a multiset $\mathscr{S} = \{V_1, \ldots, V_n\}$ 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 $i \in [N]$.

Example: $f(S) = \min(2, |S|), \ \ \forall S \subseteq [3]$

$$\left\{ \begin{matrix} \mathbb{M}(1) & \mathbb{M}(2) & \mathbb{M}(3) \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, & \begin{bmatrix} 1 \\ 0 \end{bmatrix}, & \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{matrix} \right\}$$

What do we mean by a class of linear codes?

A class of linear codes $\mathscr{P}^q(\mathbf{c})$ is a set of representations of linear polymatroids, completely specified by the class tuple

$$\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$$

.

- $N =$ Number of subspaces (count duplicates and 0-dim subspaces)
- (r_l, r_u): Representations can contain subspaces of $\mathbb{F}_q^r$ for a fixed $r_l \leq r \leq r_u$.
- $K =$ Set of allowed subspace dimensions.
- (s_l, s_u): Range of allowed sizes of underlying unique simple polymatroid[1] $\mathrm{us}(P)$ of a representation P

[1] $\mathrm{us}(P)$ is obtained by removing duplicates and 0-dim subspaces

Drexel UNIVERSITY

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

CLRP variants

Existential

[CLRP$_q$-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 $\mathscr{P}^q(\mathbf{c})$.

Special Cases:

- Testing representability of a polymatroid (E, f) over a finite field $\mathbb{F}_q$,
- Achievability of a specified rate vector with $\mathscr{P}^q(\mathbf{c})$ in HMSNC (Existing technique: Koetter-Medard formulation)
- Existance of a Multi-linear Secret Sharing Scheme achieving a certain information ratio.

CLRP variants

Enumerative

[CLRP$_q$-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 $\mathscr{P}^q(N, (r_l, r_u), K, (s_l, s_u))$ representable over $\mathbb{F}_q$, that satisfy $\mathcal{I}$.

- Choose $\equiv$ s.t. "satisfying network constraints" is invariant under $\equiv$.
- Compute all $\equiv$-inequivalent members in $\mathscr{P}^q(\mathbf{c})$ satisfying network constraints.
- Compute all possible rate vectors achievable with them.
- Obtain inequalities bounding the achievable rate regions using polyhedral computation.

Drexel UNIVERSITY

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

$\mathcal{I}$-polymatroids and $p\mathcal{I}$-polymatroids

- $\mathcal{I}$ is a collection of linear constraints on the rank function of a polymatroid of size N.

Definition

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

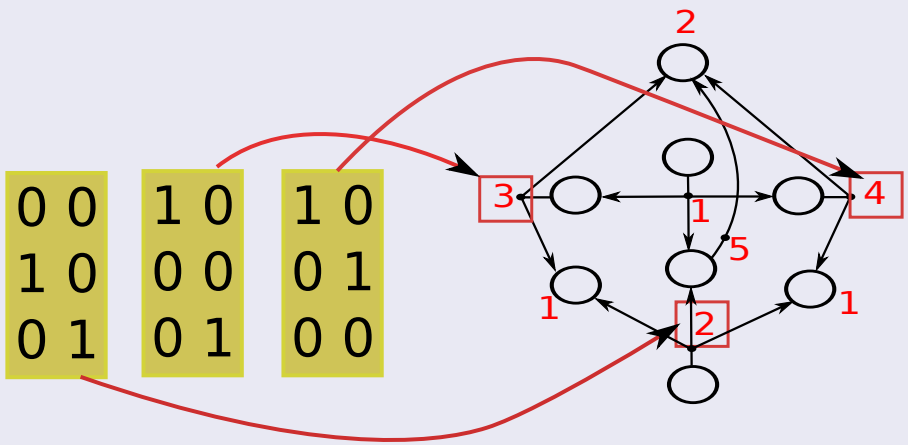
- If $i < N$ it is called $p\mathcal{I}$-polymatroid.
- If $i = N$ it is called $\mathcal{I}$-polymatroid.
- If $\mathcal{I}$ arises from network coding constraints,

$$\text{linear network code} \iff \text{linear } \mathcal{I} - \text{polymatroid}$$

Drexel UNIVERSITY

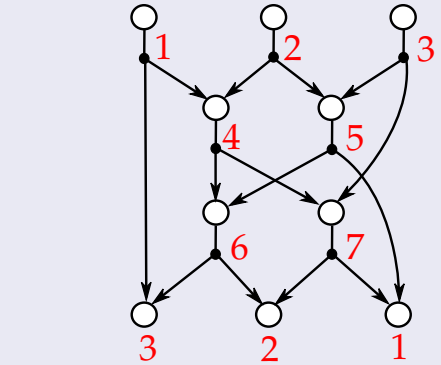
Examples

A partially feasible polymatroid



Examples

A $\mathcal{I}_{\text{Fano}}$ – *polymatroid*



$$\begin{matrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{matrix}$$
$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\mathbf{c} = (7, (3, 3), \{1\}, (7, 7))$$

$$\{1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 6, 6 \mapsto 5, 7 \mapsto 7\}$$

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

Examples

Constraints arising from a specified rank function

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

$$\mathbf{c} = (5, (4, 4), \{1, 2\}, (5, 5))$$

$$\{1 \mapsto 4, 2 \mapsto 5, 3 \mapsto 1, 4 \mapsto 3, 5 \mapsto 2\}$$

$$[2, 2, 4, 2, 4, 4, 4, 1, 2, 3, 4, 3, 4, 4, 4, 1, 3, 3, 4, 3, 4, 4, 4, 2, 3, 4, 4, 3, 4, 4, 4]$$

Equivalence relation $\equiv$

- Equivalent representations must have identical class tuples

Definition (Strong Isomorphism)

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

Equivalence relation $\equiv$

- Equivalent representations must have identical class tuples

Definition (Weak Isomorphism)

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

$$\{V_1^1, \dots V_N^1\}g = \{V_1^2, \dots, V_N^2\}$$

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

- $P\Gamma L(r, q)$ is the projective semilinear group.
- Contains all distance preserving automorphisms of $\mathbb{F}_q^r$.
- Acts on members of $\mathrm{Gr}_q(r, K)$ by applying a field automorphism and then multiplication by a matrix

Which one to use?

- Its a tradeoff

Lemma

Weak isomorphism relation is a refinement of the strong isomorphism relation

$$P_1 \triangleq \left\{ \begin{matrix} V_1 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \end{matrix}, \begin{matrix} V_2 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \end{matrix}, \begin{matrix} V_3 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} \end{matrix}, \begin{matrix} V_4 \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix} \end{matrix}, \begin{matrix} V_5 \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \end{matrix} \right\}$$

$$P_2 \triangleq \left\{ \begin{matrix} V_1' \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \end{matrix}, \begin{matrix} V_2' \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \end{matrix}, \begin{matrix} V_3' \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} \end{matrix}, \begin{matrix} V_4' \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \end{matrix}, \begin{matrix} V_5' \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \end{matrix} \right\}$$

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

Generic Orderly generation

- Objects to be generated: Define precisely the combinatorial objects to be generated.
- Order: Associate a non-negative integer "order" with each object that roughly corresponds to its size.
- Augmentation: Define a notion of augmentation.
- Generation: Construct $\equiv$-inequivalent objects of order i from $\equiv$-inequivalent objects of order $i-1$.

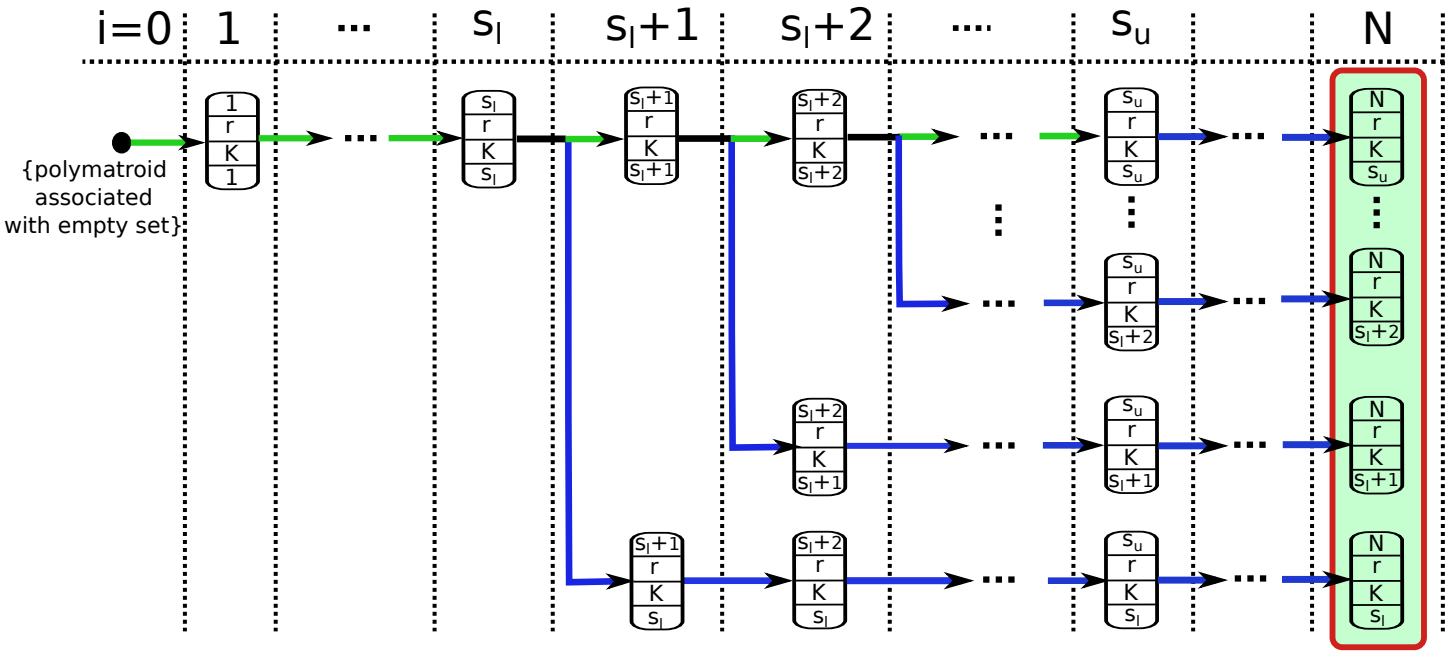
Orderly generation of all $\equiv$-inequivalent members of $\mathscr{P}^q(\mathbf{c})$

Let $\mathbf{c} = (N, (r_l, r_u), K, (s_l, s_u))$

- Objects to be generated: Polymatroids belonging to classes $\mathscr{P}^q(i, (r_l, r_u), K, (0, \max(i, s_u)))$ for $i \in [N]$ (polymatroids that could be augmented to get members of the target class)
- Order: i
- Augmentation: Polymatroid extension (a class-specific definition that keeps r and K unchanged)
- Generation: (Extension + explicit isomorph testing) for strong isomorphism and Leiterspiel[BBF$^+$06] for weak isomorphism

Generating all $\equiv$-inequivalent members of a specific class

- Let $\mathscr{P}^q(\mathbf{c}) = \cup_{r_l \le r \le r_u} \mathscr{P}^q(\mathbf{c}_r)$
- Seperately generate $\mathscr{P}^q(\mathbf{c}_r)$, where $\mathbf{c}_r = (N, (r, r), K, (s_l, s_u))$



inequivalent simple extensions (augment without duplicates and 0-dim supspaces)

inequivalent non-simple extensions (augment only using duplicates and 0-dim supspaces)

What about CLRP_q-EN?

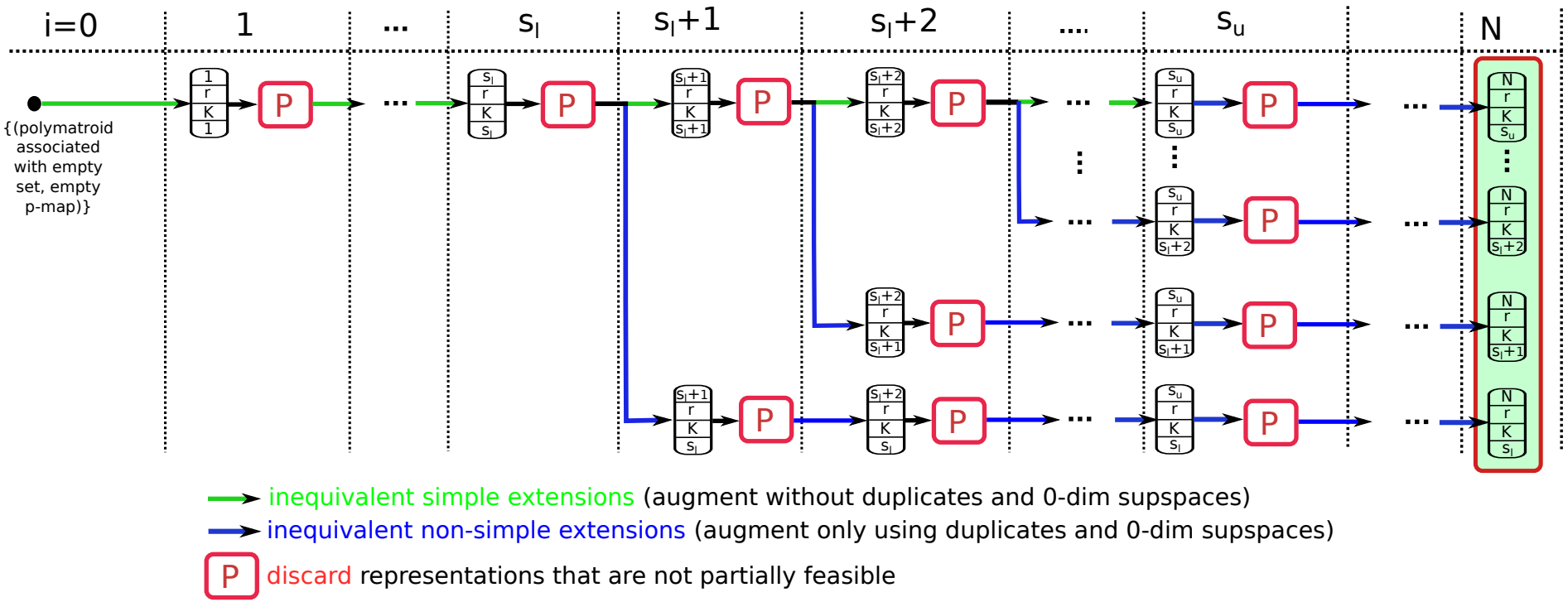
- Objects to be generated: $p\mathcal{I}$-polymatroids belonging to classes $\mathscr{P}^q(i,(r_l,r_u),K,(0,\max(i,s_u)))$ for $i \in [N]$, each specified as a pair (P,ϕ)
- Order: same as before.
- Augmentation: same as before.
- Generation: same as before
- Filter: Remove extensions that are not $p\mathcal{I}$-feasible

Why is this possible?

- $p\mathcal{I}$-feasibility is both strong and weak isomorph-invariant.
- $p\mathcal{I}$-feasibility is inherited property w.r.t. our special definition of polymatroid extension i.e.
- Deleting a subspace from a representation of $p\mathcal{I}$-polymatroid preserves $p\mathcal{I}$-feasibility.

An Algorithm to solve CLRP$_q$-EN

- Let $\mathscr{P}^q(\mathbf{c}) = \cup_{r_l \le r \le r_u} \mathscr{P}^q(\mathbf{c}_r)$
- Seperately generate $\mathscr{P}^q(\mathbf{c}_r)$, where $\mathbf{c}_r = (N, (r, r), K, (s_l, s_u))$

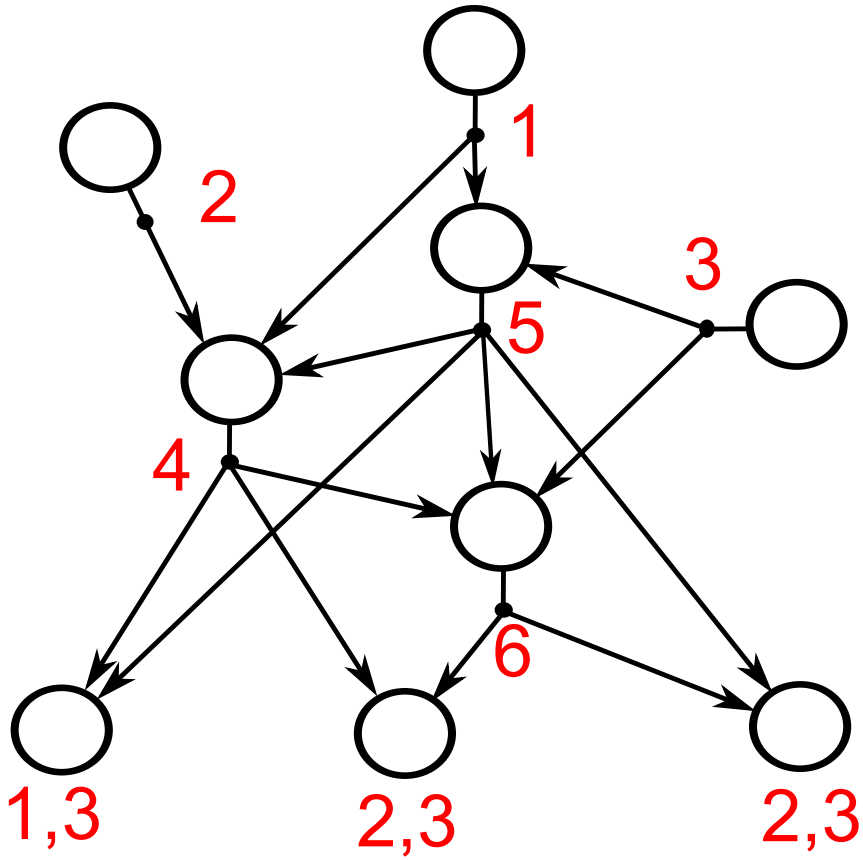


Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

Example of rate region computation with ITAP



Example of rate region computation with ITAP

Constraints:

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

Exact rate region:

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

(Achieved by class $\mathscr{P}^2(6, (1,4), \{0,1,2\}, (1,6))$)

ITAP session with HN1

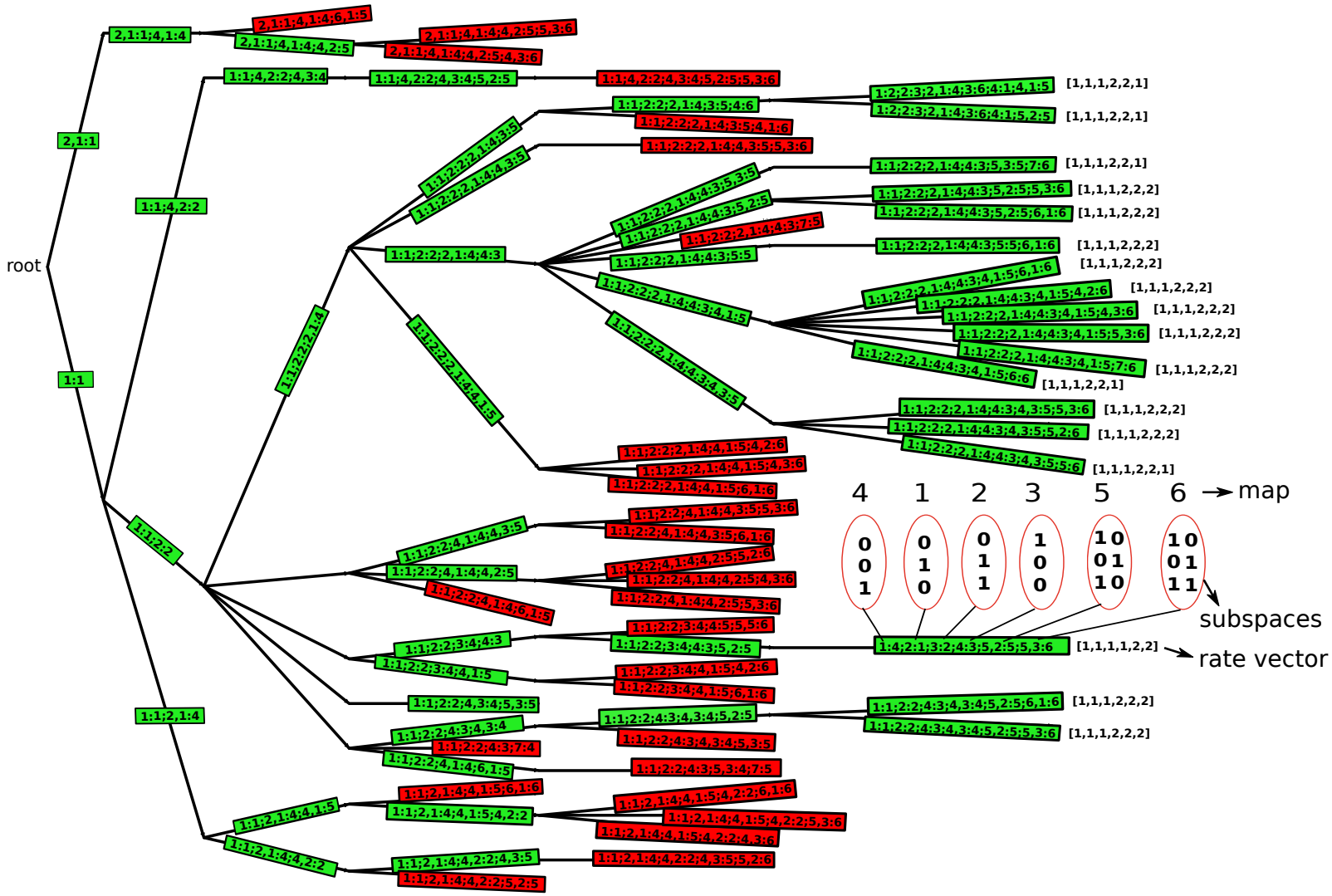
```
gap> N:=HyperedgeNet1();
[ [ [ [ 1, 2, 3 ], [ 1, 2, 3, 4 ] ], [ [ 1, 3, 4 ], [ 1, 3, 4, 5 ] ],
      [ [ 3, 4, 5 ], [ 3, 4, 5, 6 ] ], [ [ 4, 5 ], [ 1, 3, 4, 5 ] ],
      [ [ 4, 6 ], [ 2, 3, 4, 6 ] ], [ [ 5, 6 ], [ 2, 3, 5, 6 ] ] ], 3, 6 ]
gap> rlist:=proveregion(N,2,GF(2),[4]);; # k=2,opt_dmax=4=max. 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
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
```

Compute achievable rate region with a smaller class

Achievable rate region with class $\mathscr{P}^2(6,(1,3),\{0,1,2\},(1,6))$

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

Full generation tree containing $p\mathcal{I}_{\mathrm{HN1}}$-polymatroids from class $\mathscr{P}^2(6,(1,3),\{0,1,2\},(1,6))$



Other computations with ITAP

- CLRP$_q$-EX for network coding and secret sharing using combinatorial generation (see examples in the thesis, no time today!)
- CLRP$_q$-EX via a variant of Koetter and Medard's algebraic formulation [KM03] called the path gain formulation [ST10]. Uses Gröbner basis computation via an interface to Singular [CdG12].
- CLRP$_q$-EX for specified polymatroid rank vectors: Used to determine under which symmetry conditions, Shannon-type inequalities suffice to characterize entropy region, exhaustively for $N = 4, 5$.

Theorem

For $N \geq 6$, Cyclic entropic set functions $\subsetneq$ Cyclic polymatroidal set functions

[ACW16]Jayant Apte, Qi Chen, John MacLaren Walsh, "Symmetries in the entropy Space", accepted, the 2016 IEEE Information Theory Workshop, Cambridge, UK

Comparison with Subramanian-Thangraj (ST) algebraic formulation

- We consider a MDCS (Multilevel Diversity Coding System) instance, a special case of HMSNC.
- Expected to invoke bad behaviour from ST formulation, as number of indeterminates in the polynomial equations grows badly with increase in the rates.

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

Comparison with Subramanian-Thangraj (ST) algebraic formulation

- Vamos Network is a network constructed from the Vamos matroid.
- Vamos matroid is not $\mathbb{F}_q$-linear for any q, in fact non-entropic.
- Expected to invoke bad behaviour from an enumerative algorithm.

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

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

Outer Bounds: Verification vs Enumeration

[Verify] Determine if a specified collection of linear information inequalities and network coding constraints imply a putative inequality in $(\boldsymbol{\omega}, \mathbf{r})$ variables.

- Linear feasibility problem in the dual space.
- ITIP[YR08] and XITIP [RES08] can do the job.
- Can minimize l_1 norm in the dual space to find the sparsest proof[Tia14, Con].

[EPOBs] Determine the tightest collection of implied inequalities bounding the rate region, given a collection of linear information inequalities.

- This is an enumeration problem.
- [Tia14] uses a series of linear programs to determine the boundary of an outer bound on the rate region in $\mathbb{R}^2$, fits inequalities, and proves them using [Verify].
- Need systematic and general approach that applies to HMSNC. .

This thesis

Compute the inequality representation of $\mathcal{R}_{\text{out}}$ described as:

$$\mathcal{R}_{\text{out}} = \text{proj}_{\boldsymbol{\omega},\mathbf{r}}(\Gamma_{\text{out}} \cap \mathscr{L} \cap \mathscr{L}')$$

- Γ_{out} is polyhedral.
- $\mathscr{L}$ and $\mathscr{L}'$ are halfspaces and hyperplanes.
- All the semantics of polyhedral projection problem.

Issues?

- We are removing exponentially many dimensions.
- Fourier-Motzkin Elimination is a classical technique for polyhedral projection. (chokes for most non-trivial EPOB problems!)
- Must pass through exponentially many intermmediate polyhedra, which could be far more terrible (large/degenerate) than the projection polytope.
- Solution: Work in projection space directly.

Drexel UNIVERSITY

Algorithms working in the projection space

- Benson's outer approximation algorithm: Builds progressive outer bounds to the projection by solving linear programs over the original polytope. Originally ment for solving MOLPs.
  Harold P. Benson (1998). "An Outer Approximation Algorithm for Generating All Efficient Extreme Points in the Outcome Set of a Multiple Objective Linear Programming Problem". Journal of Global Optimization 13 (1): 124.
- Convex Hull Method: Builds progressive inner bounds to the projection by solving linear programs over the original polytope.
  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.
- Deriving non-Shannon-type inequalities computationally is a closely related problem where we are eliminating exponentially many variables.

Algorithms working in the projection space

- Benson's outer approximation algorithm: Builds progressive outer bounds to the projection by solving linear programs over the original polytope. Originally meant for solving MOLPs.
  Used by Csirmaz [Csi13] for deriving non-Shannon-type information inequalities.
- Convex Hull Method: Builds progressive inner bounds to the projection by solving linear programs over the original polytope. Used by Xu, Wang, and Sun [W. 08] for deriving non-Shannon-type information inequalities.
- Deriving non-Shannon-type inequalities computationally is a closely related problem where we are eliminating exponentially many variables.

Drexel UNIVERSITY

This Thesis

Clean-up of CHM:

- Modern, more efficient subroutines
- Better handling of unbounded polyhedra
- Exact rational arithmetic implementation in C [Apt14]

A symmetry exploiting CHM (symCHM), that uses the knowledge of symmetries of polytopes to:

- Solves less linear programs
- Efficient inner bound updates

Drexel UNIVERSITY

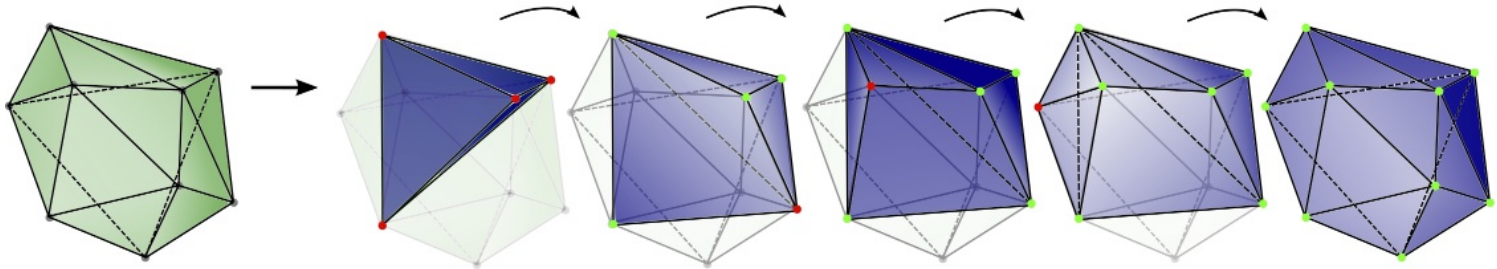
Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

How does CHM work?

Input: Polytope $\mathcal{P}$ specified as inequalities
Output: Projection polytope $\text{proj}_k(\mathcal{P})$ specified as inequalities *and* extreme points



Constructs Progressively better inner bounds to the projection polytope

- Solves linear programs of the following form:

$$\min_{\mathbf{x} \in \text{proj}_k \mathcal{P}} \mathbf{c}^T \mathbf{x} \quad = \quad \min_{\mathbf{y} \in \mathcal{P}} [\mathbf{c}^T, \mathbf{0}_{d-k}^T] \mathbf{x}, \quad \text{and}, \tag{1}$$

to test if a facet of inner bound is a facet of projection (terminal facet), otherwise, obtains a boundary point of projection as,

$$\underset{\mathbf{x} \in \text{proj}_k \mathcal{P}}{\text{argmin}} \ \mathbf{c}^T \mathbf{x} \quad = \quad \text{proj}_k \left(\arg \min_{\mathbf{y} \in \mathcal{P}} [\mathbf{c}^T, \mathbf{0}_{d-k}^T] \mathbf{x} \right).$$

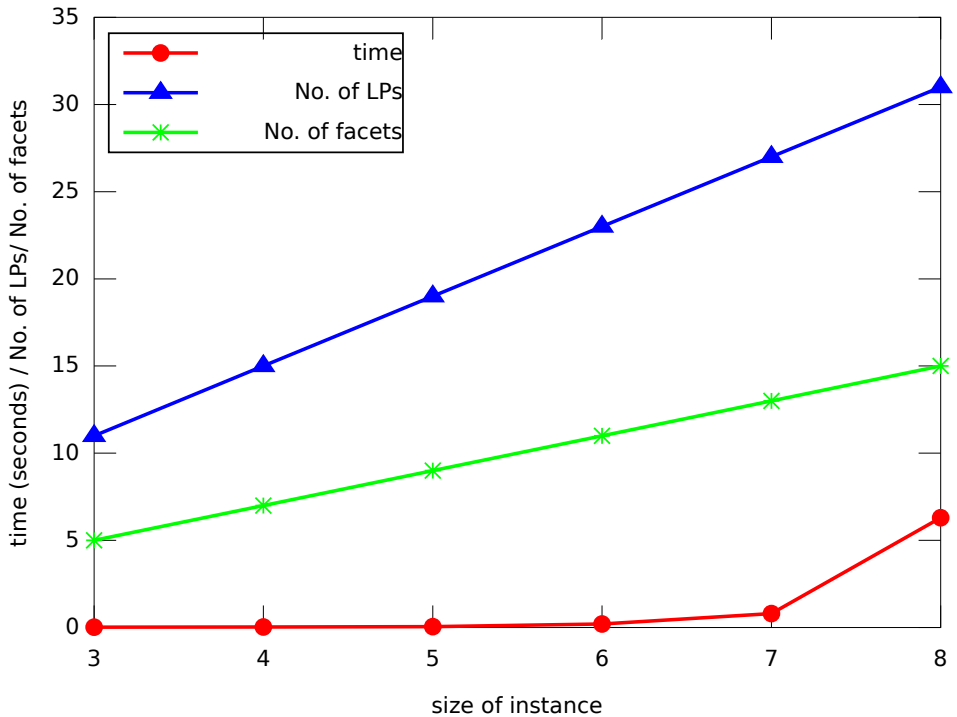
How are the inner bounds updated?

- Maintains a *Double Description (DD) Pair* of the inner bound
- First DD pair is computed using a $k+1 \times k+1$ matrix inversion
- Later inner bounds are computed by augmenting the existing inner bound by a single vertex

Input: DD pair of an inner bound, a new boundary point of projection,
Output: DD pair new inner bound obtained by augmenting current inner bound with new point,
How: An iteration of the Double Description Method [FP96] of polyhedral representation conversion.
(Lassez et. al. [LL93] used combinatorial search instead)

Example: Uniform Matroidal Networks

- A uniform matroidal network of size $k \geq 3$ is constructed from a uniform matroid U_k^2 of rank 2 on k elements [DFZ07]
- Possibly the simplest family of networks (in terms of sizes of rate region descriptions)



- Runtime grows exponentially in problem size (projection dimension), reflecting exponential growth in the size of polytope being projected

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

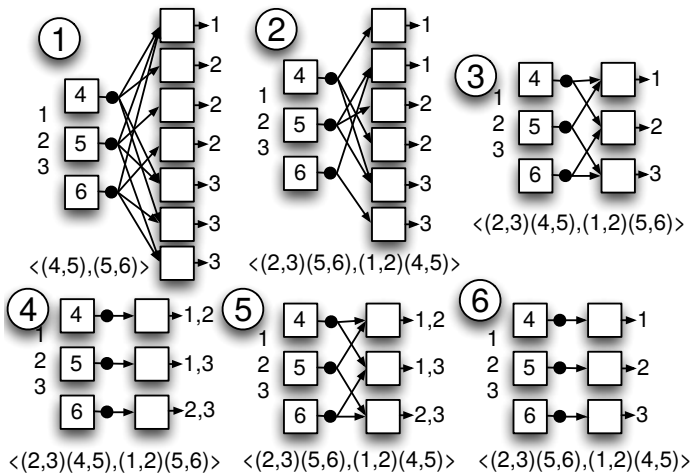
Polyhedral Symmetries

Let $\mathcal{P} \subseteq \mathbb{R}_d$ be a polytope.

- **Combinatorial Symmetries**: Automorphisms of the face lattice of polytope $\mathcal{P}$.
- **Affine Symmetries (Restricted Symmetries)**: Members of $GL_d(\mathbb{R})$ ($GL_{d+1}(\mathbb{R})$) that leave $\mathcal{P}$ (embedding of $\mathcal{P}$ in $\mathbb{R}^{d+1}$ called homog($\mathcal{P}$)) setwise fixed. Form a group called Affine (Restricted) symmetry Group, ASG (RSG).
- **Permutations of Co-ordinate dimensions**: Affine symmetries arising from permutation matrices

Network Symmetry Groups (NSGs)

- For a HMSNC instance of size N, its NSG contains the permutations of message labels $[N]$ under which the network constraints are stabilized setwise.



- NSG is always a product group $G_1 \times G_2 \leq S_{[k]} \times S_{[N]\setminus[k]}$
- [AW15] defines NSGs and considers their computation using algorithms for computing automorphism groups of graphs.

NSGs and EPOBs

- NSGs correspond to symmetry groups of permutations of co-ordinates, that stabilize $\Gamma_{\text{out}} \cap \mathscr{L} \cap \mathscr{L}'$ and its projection $\mathcal{R}_{\text{out}}$ setwise.
- In general, we can assume we know a subgroup of the ASG of the projection polytope $\text{proj}_k(\mathcal{P})$.
- How can we exploit these symetries?

Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

Exploiting symmetry to solve less LPs

- Solving LPs exactly using rational arithmetic is much more burdonsome than solving them with floats.[2]
- Let G be the specified subgroup of ASGs of $\text{proj}_k(\mathcal{P})$.

How can we reduce the number of LPs solved?

- Test the terminality of a facet $\mathbf{f}$ of the inner bound.
- If $\mathbf{f}$ is terminal, so are the facets $\mathbf{f}^G \setminus \{\mathbf{f}\}$, and we save on $|\mathbf{f}^G| - 1$ LPs.
- Otherwise, we find a new boundary point $\mathbf{v}$ of the projection, and compute its orbit $\mathbf{v}^G$ under the action of G on $\mathbb{R}^k$.
- We trade $|\mathbf{v}^G| - 1$ LPs for one orbit computation.
- This way, we end up maintaining only the symmetric inner bounds on $\text{proj}_k(\mathcal{P})$. (inner bounds whose symmetry group is also G)

[2] David L. Applegate, William Cook, Sanjeeb Dash, and Daniel G. Espinoza. 2007. Exact solutions to linear programming problems. Oper. Res. Lett. 35, 6 (November 2007), 693-699.

Exploiting Symmetry for lower complexity inner bound updates

Input: DD pair of the lth symmetric inner bound $\mathcal{P}^l$ and a new boundary point $\mathbf{v}$,
Output DD pair of the $l+1$th symmetric inner bound $\mathcal{P}^{l+1}$,
How:

- Augment the current inner bound $\mathcal{P}$ with new point $\mathbf{v}$.
- Use the incidence decomposition framework of Bremner et. al. to compute facets of $\mathcal{P}^{l+1}$ incident to $\mathbf{v}$
- Takes as many k dimensional DD steps as there members of $|\mathbf{v}^G|$ that are neighbors of $\mathbf{v}$.

Illustration: projection of a hypercube in $\mathbb{R}^d$ to $\mathbb{R}^3$

- DD = Double description steps in $(\mathbb{R}^4)^\circ$

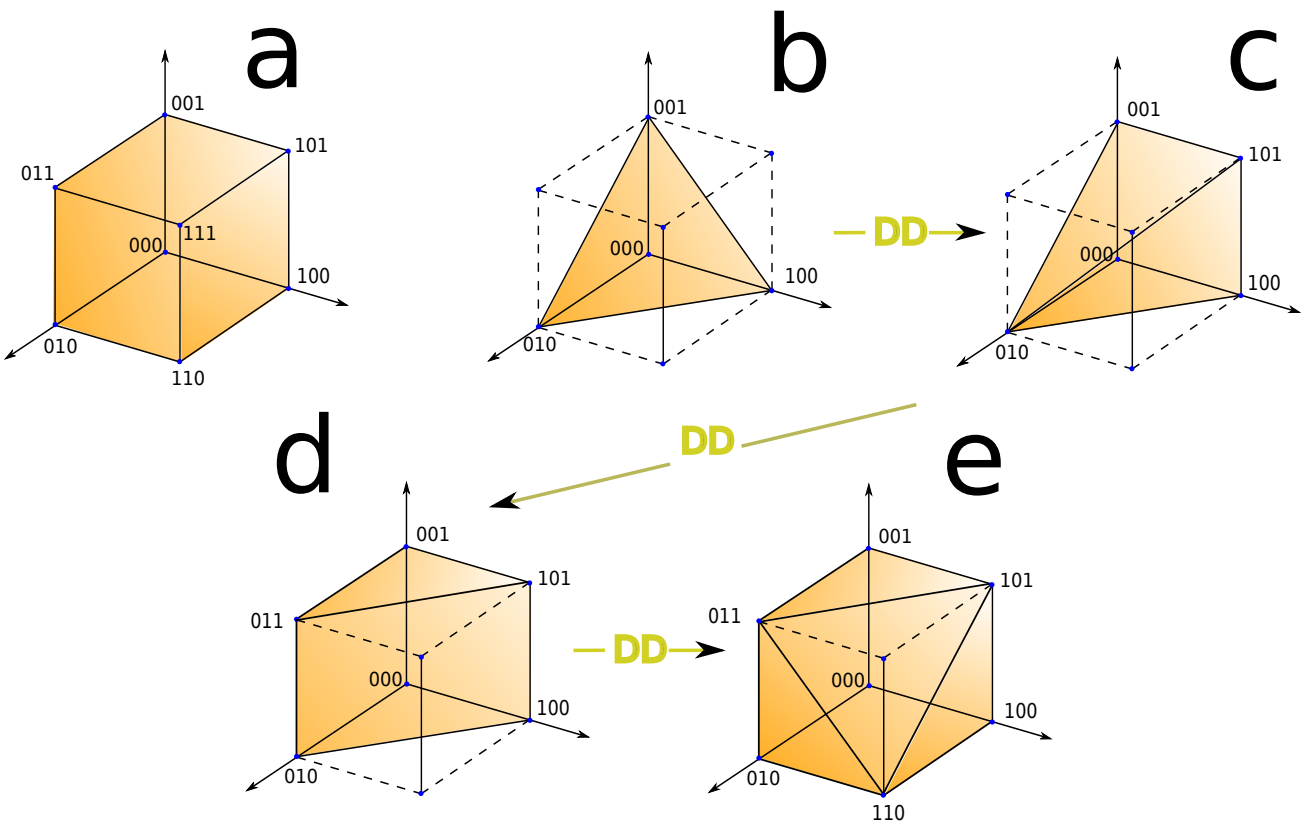
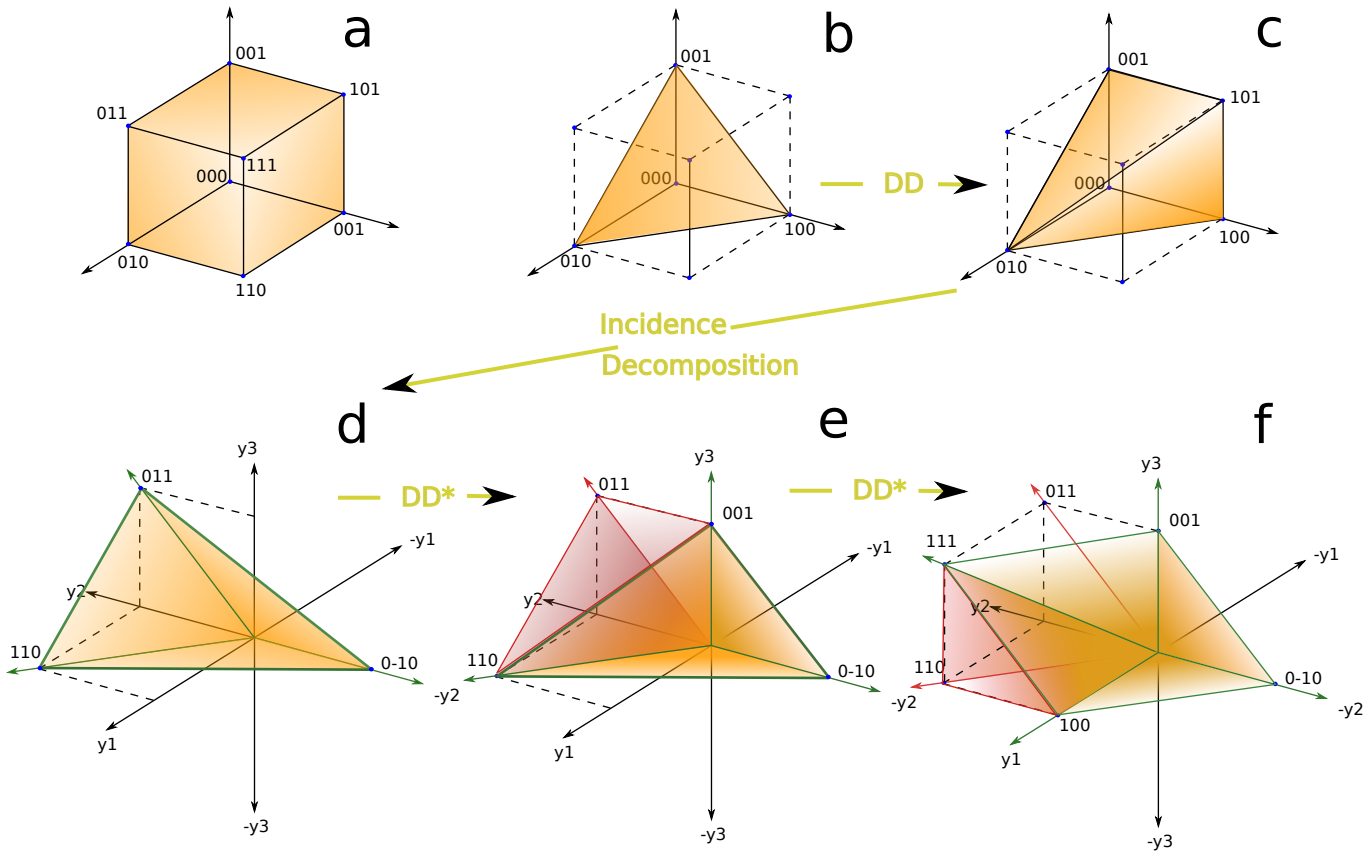


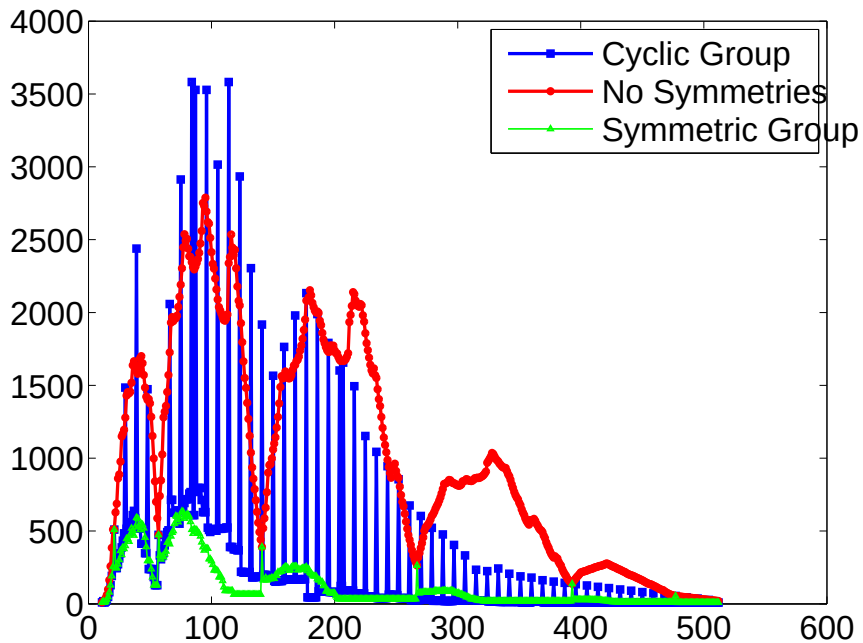
Illustration: projection of a hypercube in $\mathbb{R}^d$ to $\mathbb{R}^3$

- DD = Double description steps in $(\mathbb{R}^4)^\circ$
- DD* = Double description steps in $(\mathbb{R}^3)^\circ$



Sizes of DD steps for projecting a 12-dimensional hypercube to $\mathbb{R}^9$

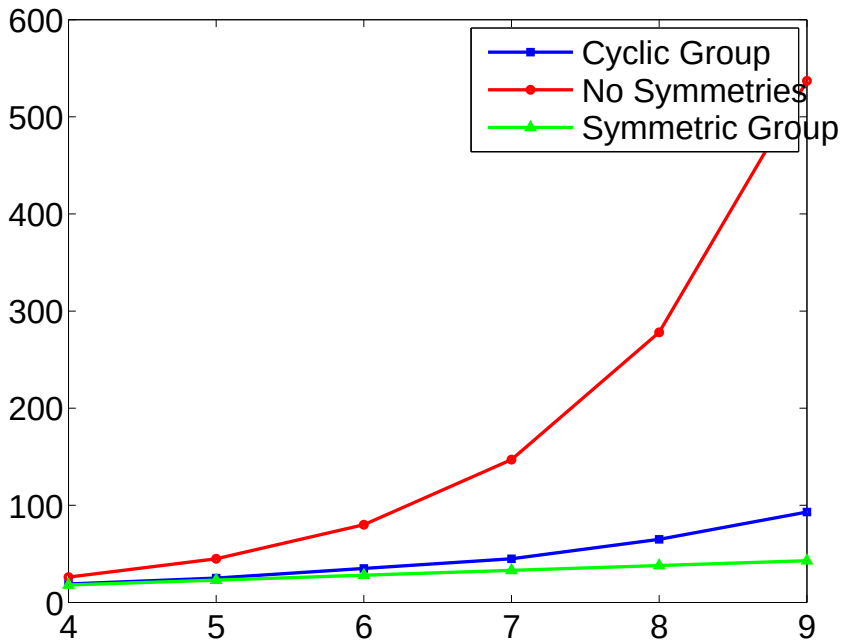
- DD stepsize = Number of extreme rays of the cone input to the DD subroutine
- Figure: DD stepsize for augmenting by ith vertex vs i



Average stepsizes under knowledge of no symmetries, cyclic group C_9 and symmetric group S_9 are 978.97, 245.38 and 120.54 respectively.

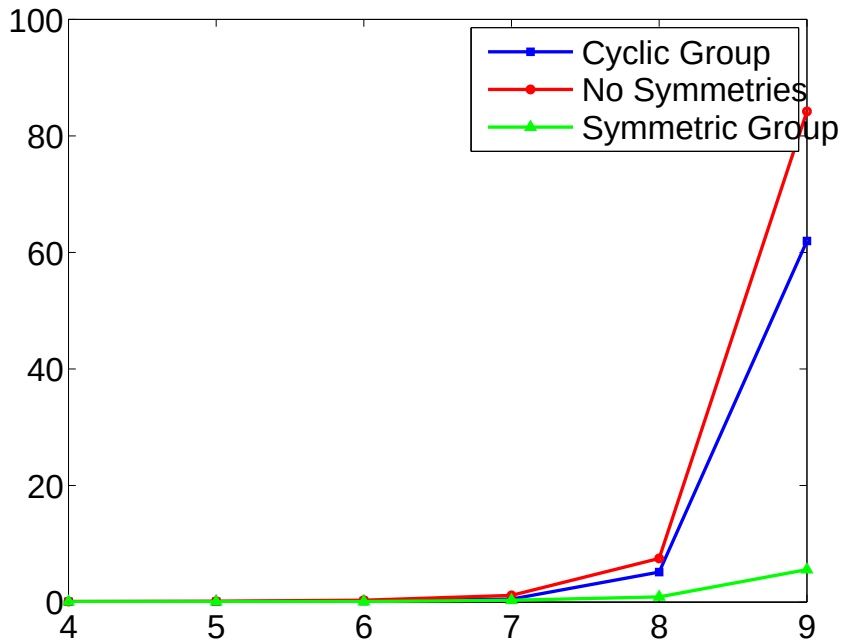
Number of LPs solved for projecting a 12-dimensional hypercube

- Number of LPs solved vs projection dimension



Runtimes for projection of a 12-dimensional hypercube

- Runtime in seconds vs projection dimension



Outline

1. Introduction
2. Inner bound Algorithms
   - Linear polymatroids
   - Constrained Linear Representability Problems
   - $p\mathcal{I}$-polymatroids
   - Orderly generation for solving CLRP$_q$-EN
   - Computing with ITAP
3. Outer Bound Algorithms
   - Introduction to EPOBs
   - Convex Hull Method
   - Polyhedral symmetries and Network Symetries
   - symCHM: Symmetry Exploiting CHM
   - Computing with ITCP

Drexel UNIVERSITY

This Thesis

Information Theoretic Converse Prover (ITCP)

- Generate statements of rate region converses using symCHM.
- Supports weighted sum rate bounds (HMSNC), information ratio lower bounds (secret sharing), and guessing number upper bounds (guessing games) via an interface to QSopt exact LP solver[DWSD09].

Computing with ITCP: NSGs

- We consider a 3-source, 5-encoder IDSC instance with $N = 8$.

```
gap> # Define a size 8 IDSC instance
> idsc:=[ [ [ [ 1, 2, 3 ], [ 1, 2, 3, 4, 5, 6, 7, 8 ] ],\
>       [ [ 4, 5 ], [ 1, 2, 4, 5 ] ], [ [ 5, 6 ], [ 1, 2, 5, 6 ] ],\
>       [ [ 6, 7 ], [ 1, 2, 6, 7 ] ], [ [ 7, 8 ], [ 1, 2, 7, 8 ] ],\
>       [ [ 4, 8 ], [ 1, 2, 4, 8 ] ], [ [ 4, 6 ], [ 3, 4, 6 ] ],\
>       [ [ 5, 8 ], [ 3, 5, 8 ] ], [ [ 4, 7 ], [ 3, 4, 7 ] ],\
>       [ [ 5, 7 ], [ 3, 5, 7 ] ], [ [ 6, 8 ], [ 3, 6, 8 ] ] ], 3, 8 ];
gap> G:=NetSymGroup(idsc);
Group([ (5,8)(6,7), (4,5)(6,8), (4,6)(7,8), (1,2) ])
gap> Size(G);
20
```

- NSG is isomorphic to $S_2 \times D_5$, where D_5 is the dihedral group.

Computing with ITCP: EPOBs

- **Stats**: 94 inequalities, 18 equivalence classes
  109 LPs with symmetries, 207 LPs without symmetries
  Time: 43.91 sec with symmetries and 67.72 without symmetries.

```
gap> rlist1:=NCRateRegionOB2(idsc,true,[]);;
gap> Display(rlist1[2]);
0 >= -w2
0 >= -w3
+R4 >= 0
+R4 +R6 >= +w3
+R4 +R5 >= +w1 +w2
+R4 +1/2 R5 +1/2 R8 >= +w1 +w2 +1/2 w3
+1/2 R4 +1/2 R5 +1/2 R6 +1/2 R7 >= +w1 +w2 +1/2 w3
+2/3 R4 +2/3 R5 +1/3 R6 +1/3 R8 >= +w1 +w2 +2/3 w3
+2/3 R4 +1/3 R5 +1/3 R6 +1/3 R7 +1/3 R8 >= +w1 +w2 +2/3 w3
+1/2 R4 +1/2 R5 +1/2 R6 +1/4 R7 +1/4 R8 >= +w1 +w2 +3/4 w3
+R4 +1/2 R5 +1/2 R6 +1/2 R7 >= +w1 +w2 +w3
+R4 +1/2 R5 +1/2 R6 +1/2 R8 >= +w1 +w2 +w3
+R4 +1/3 R5 +1/3 R6 +1/3 R7 +1/3 R8 >= +w1 +w2 +w3
+2/3 R4 +2/3 R5 +1/3 R6 +2/3 R7 +1/3 R8 >= +w1 +w2 +4/3 w3
+R4 +1/2 R5 +1/2 R6 +R7 >= +w1 +w2 +3/2 w3
+R4 +1/2 R5 +1/2 R6 +1/2 R7 +1/2 R8 >= +w1 +w2 +3/2 w3
+2 R4 +R6 +R7 >= +w1 +w2 +2 w3
+R4 +R5 +R6 +R7 >= +w1 +w2 +2 w3
```

Computing with ITCP: EPOBs

- Fano network is a HMSNC instance with size $N = 7$.

```
gap> # define a network instance (in this case, Fano network)
> F:=[ [ [ [ 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:=NCRateRegionOB(F,true,[]);;
gap> Display(rlist[2]);
0 >= -w2
0 >= -w1
0 >= -w3
+R6 >= +w3
+R5 >= +w3
+R7 >= +w1
+R4 >= +w1
+R6 +R7 >= +w2 +w3
+R4 +R6 >= +w2 +w3
+R4 +R5 >= +w2 +w3
+R6 +R7 >= +w1 +w2
+R4 +R6 >= +w1 +w2
+R4 +R5 >= +w1 +w2
```

- Substituting edge capacities $= 1$, we recover the achievable source rate region computed by Dougherty, Freiling and Zeger [DFZ15], which is a cube in $\mathbb{R}^3$.

Summary of Contributions

- Algorithms to solve important problems related to HMSNC with an enumerative flavour, applicable to a variety of related problems,
- Finite terminating algorithms for computing achievable rate regions over a specified class of linear codes, that can also be used for solving verification problems,
- Finite terminating algorithms for generating statements of converse proofs,
- Software implementations:
  - ITAP,ITCP, symCHM, Qsopt_ex-interface in GAP, and
  - Rational arithmetic C implementation chm.
- Impact:
  - The techniques developed in this thesis have been used to prove thousands of rate regions, and make general non-trivial statements about the HMSNC problem [Con].
  - The techniques developed in this thesis have been used to understand the structure of entropy function region [ACW16].

Drexel UNIVERSITY

Jayant's Publications

Jayant Apte and John MacLaren Walsh.

Constrained Linear Representability of Polymatroids and Algorithms for computing Network Coding Achievability Proofs.
submitted to *IEEE Transactions on Information Theory, May 15, 2016.*

Jayant Apte and John MacLaren Walsh.

Explicit Polyhedral Outer Bounds on Network Coding Rate Regions via Entropy Function Region: Algorithms, Symmetry and Computation.
submitted to IEEE Transactions on Information Theory, July 22, 2016.

Qi Chen, Jayant Apte and John MacLaren Walsh.

Symmetries in the Entropy Space.
in preparation.

Jayant Apte and John MacLaren Walsh.

Symmetry in Network Coding.
in International Symposium on Information Theory, Hong Kong, pages 376-380, June 2015.

Jayant Apte and John MacLaren Walsh.

Exploiting Symmetry in Computing Polyhedral Bounds on Network Coding Rate Regions.
in International Symposium on Network Coding, Sydney, Australia, June 22-24, 2015, pages 76-80, 2015.

Jayant Apte, Congduan Li and John MacLaren Walsh.

Algorithms for Computing Network Coding Rate Regions via Single Element Extensions of Matroids.
in International Symposium on Informtion Theory, Honolulu, Hawaii, pages 2306-2310, June 2014.

Jayant Apte, Congduan Li and John MacLaren Walsh.

Exact Rpair Problems with Multiple Sources.
in Conference on Information Sciences and Systems (CISS), Princeton, NJ, pages 1-6, 2014

Drexel UNIVERSITY

Thank You!

Questions?

References I

Rudolf Ahlswede, Ning Cai, S-YR Li, and Raymond W Yeung, *Network information flow*, IEEE Transactions on information theory **46** (2000), no. 4, 1204–1216.

Jayant Apte, Qi Chen, and John MacLaren Walsh, *Symmetries in the entropy space*, 2016, to appear, IEEE Information Theory Workshop, Cambridge, UK.

Jayant Apte, *chm-An Implementation of Convex Hull Method*, 2014, http://www.ece.drexel.edu/walsh/aspitrg/software.html.

J. Apte and J. M. Walsh, *Symmetry in network coding*, 2015 IEEE International Symposium on Information Theory (ISIT), June 2015, pp. 376–380.

References II

A. Betten, M. Braun, H. Fripertinger, 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.

David Bremner, *Incremental convex hull algorithms are not output sensitive*, pp. 26–35, Springer Berlin Heidelberg, Berlin, Heidelberg, 1996.

M. Costantini and W. de Graaf, *singular, the gap interface to singular, Version 12.04.28*, Apr 2012, GAP package.

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.

L. Csirmaz, *Information inequalities for four variables*, Avaible Online: https://www.eprints.renyi.hu/65/1/benson.pdf, 2013.

References III

Randall Dougherty, Christopher Freiling, and Kenneth Zeger, *Insufficiency of linear coding in network information flow*, IEEE Transactions on Information Theory **51** (2005), no. 8, 2745–2759.

R. Dougherty, C. Freiling, and K. Zeger, *Networks, matroids, and non-shannon information inequalities*, Information Theory, IEEE Transactions on **53** (2007), no. 6, 1949–1969.

R. Dougherty, C. Freiling, and K. Zeger, *Non-shannon information inequalities in four random variables*, CoRR **abs/1104.3602** (2011).

Randall Dougherty, Chris Freiling, and Kenneth Zeger, *Achievable rate regions for network coding*, IEEE Transactions on Information Theory **61** (2015), no. 5, 2488–2509.

Drexel UNIVERSITY

References IV

- David Applegate, William Cook, Sanjeeb Dash, and Daniel Espinoza, *Qsopt-exact rational lp solver*, 2009, http://www.math.uwaterloo.ca/~bico/qsopt/ex/.
- F. Matúš, *Infinitely Many Information Inequalities*, IEEE International Symposium on Information Theory (ISIT), June 2007, pp. 41–44.
- K. Fukuda and A. Prodon, *Double description method revisited*, Combinatorics and computer science (1996), 91–111.
- S. Fujishige, *Polymatroidal dependence structure of a set of random variables*, Information and Control **39** (1978), 55–72.
- Tracey Ho, Muriel Médard, Ralf Koetter, David R Karger, Michelle Effros, Jun Shi, and Ben Leong, *A random linear network coding approach to multicast*, IEEE Transactions on Information Theory **52** (2006), no. 10, 4413–4430.

Drexel UNIVERSITY

References V

D. Hammer, A. Romashchenko, and N. Vereshchagin A. Shen, *Inequalities for shannon entropy and kolmogorov complexity*, Journal of Computer and System Science **60** (2000), no. 2, 442–464.

S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, *Polynomial time algorithms for multicast network code construction*, IEEE Transactions on Information Theory **51** (2005), no. 6, 1973–1982.

R. Koetter and M. Medard, *An algebraic approach to network coding*, IEEE/ACM Transactions on Networking **11** (2003), no. 5, 782–795.

C. Lassez and J-L. Lassez, *Quantifier elimination for conjunctions of linear constraints via a convex hull algorithm*, Symbolic and Numerical Computation for Artificial Intelligence (Donald, Kapur, and Mundy, eds.), Academic Press, 1993.

References VI

April Rasala Lehman and Eric Lehman, *Complexity classification of network information flow problems*, Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (Philadelphia, PA, USA), SODA '04, Society for Industrial and Applied Mathematics, 2004, pp. 142–150.

R. Pulikkoonattu, E. Perron, and S. Diggavi, *X-information theoretic inequality prover(xitip)*, 2008, http://xitip.epfl.ch/.

Abhay T. Subramanian and Andrew Thangaraj, *Path gain algebraic formulation for the scalar linear network coding problem*, IEEE Transactions on Information Theory **56** (2010), no. 9, 4520–4531.

Chao Tian, *Characterizing the rate region of the (4, 3, 3) exact-repair regenerating codes*, IEEE Journal on Selected Areas in Communications **32** (2014), no. 5, 967–975.

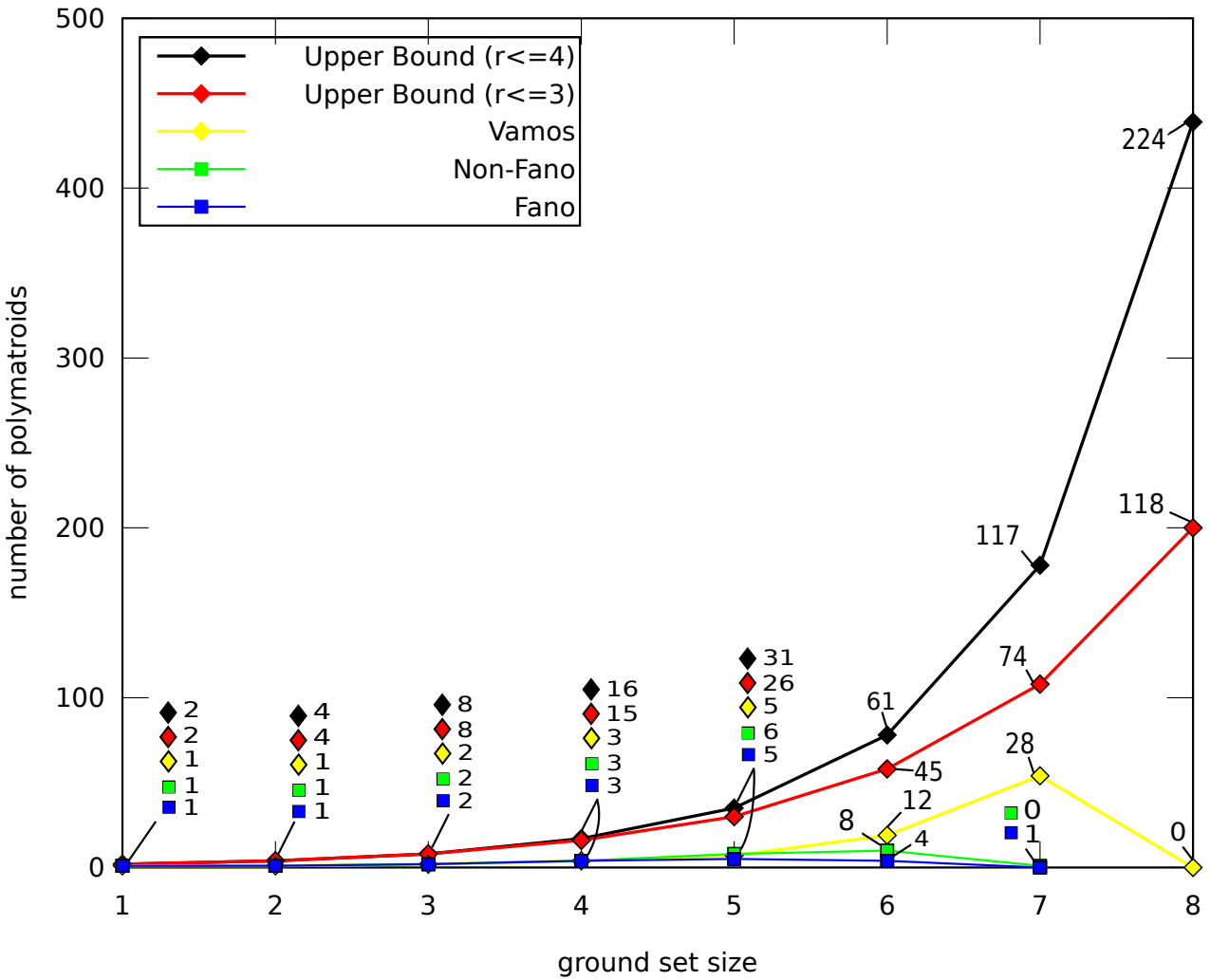
References VII

- W. Xu, J. Wang, J. Sun, *A projection method for derivation of non-Shannon-type information inequalities*, IEEE International Symposium on Information Theory (ISIT), 2008, pp. 2116 – 2120.
- R. W. Yeung, *Information theory and network coding*, Springer, 2008.
- Ying-On Yan and Raymond Yeung, *Itip-information theoretic inequality prover*, 2008, http://user-www.ie.cuhk.edu.hk/ ITIP/.
- 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** (2012), no. 9, 5625–5639.
- Z. Zhang and R W. Yeung, *On Characterization of Entropy Function via Information Inequalities*, IEEE Transactions on Information Theory **44** (1998), no. 4.
- G.M. Ziegler, *Lectures on polytopes*, Springer-Verlag, 1995.

Drexel UNIVERSITY

Combinatorial generation for solving CLRP$_q$-EX

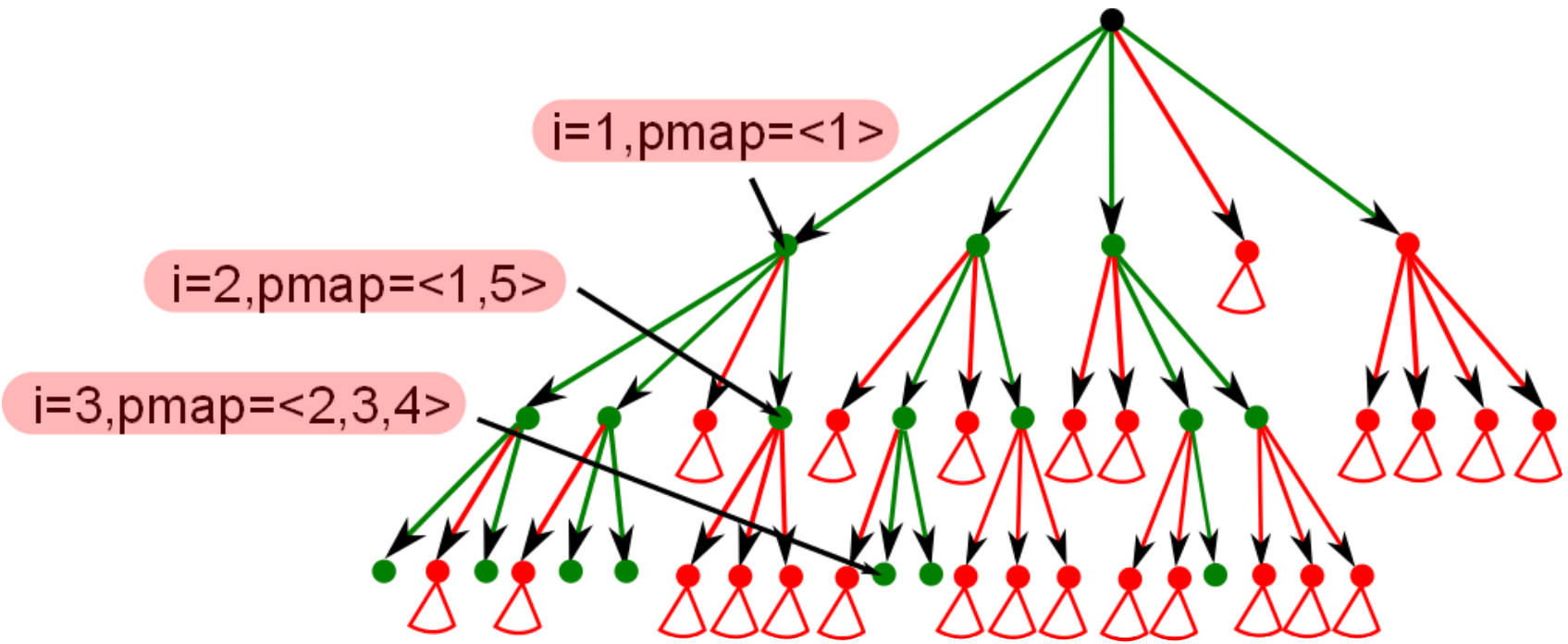
Number matroid representations over $\mathbb{F}_2$ maintained by ITAP at different iterations for Fano (blue), Non-Fano (green) and Vámos (yellow) networks along with upper bounds.



CHM complexity

- McMullen's upper bound on the no. of vertices of a k dimensional polytope specified by m inequalities [Zie95].

$$\mathcal{O}(m^{\lfloor \frac{k}{2} \rfloor})$$

- Simplex method has exponential worst case complexity in d.
- Assuming that the only points of projection obtained during the course are the extreme points of projection, CHM could solve $\mathcal{O}(m^{\lfloor \frac{k}{2} \rfloor}) + m$ linear programs, one per vertex and facet of projection, with each having exponential runtime, given that the projection has m facets.
- The double description method does not have an output sensitive time complexity [Bre96],as it is known to be susceptible to the insertion order of inequalities.
- DD updates are susceptible to the order in which we find new points in CHM.

How to augment partially feasible polymatroids