Two Polyhedral Combinatorics Problems from Network Information Theory

Tie Liu

Joint work with Amir Salimi (Texas A&M), Shuguang Cui (Texas A&M), Chao Tian (AT&T Labs), and Jun Chen (McMaster)

Polyhedral combinatorics

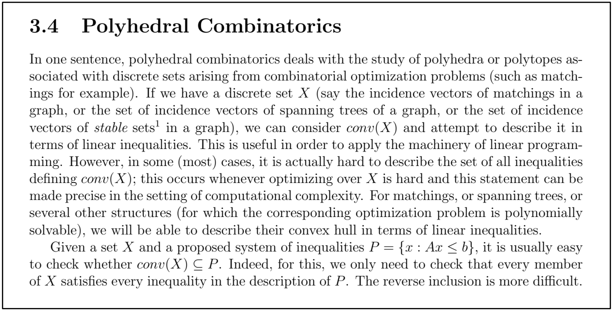
3.4 Polyhedral Combinatorics

In one sentence, polyhedral combinatorics deals with the study of polyhedra or polytopes associated with discrete sets arising from combinatorial optimization problems (such as matchings for example). If we have a discrete set X (say the incidence vectors of matchings in a graph, or the set of incidence vectors of spanning trees of a graph, or the set of incidence vectors of *stable* sets[1] in a graph), we can consider $conv(X)$ and attempt to describe it in terms of linear inequalities. This is useful in order to apply the machinery of linear programming. However, in some (most) cases, it is actually hard to describe the set of all inequalities defining $conv(X)$; this occurs whenever optimizing over X is hard and this statement can be made precise in the setting of computational complexity. For matchings, or spanning trees, or several other structures (for which the corresponding optimization problem is polynomially solvable), we will be able to describe their convex hull in terms of linear inequalities.

Given a set X and a proposed system of inequalities $P = \{x : Ax \leq b\}$, it is usually easy to check whether $conv(X) \subseteq P$. Indeed, for this, we only need to check that every member of X satisfies every inequality in the description of P. The reverse inclusion is more difficult.

- M. X. Goemans, *Lecture Notes on Linear Programming and Polyhedral Combinatorics*. Massachusetts Institute of Technology, 2009. Available online at `http://www-math.mit.edu/~goemans/`

Polyhedral combinatorics



3.4 Polyhedral Combinatorics

In one sentence, polyhedral combinatorics deals with the study of polyhedra or polytopes associated with discrete sets arising from combinatorial optimization problems (such as matchings for example). If we have a discrete set X (say the incidence vectors of matchings in a graph, or the set of incidence vectors of spanning trees of a graph, or the set of incidence vectors of *stable* sets[1] in a graph), we can consider $conv(X)$ and attempt to describe it in terms of linear inequalities. This is useful in order to apply the machinery of linear programming. However, in some (most) cases, it is actually hard to describe the set of all inequalities defining $conv(X)$; this occurs whenever optimizing over X is hard and this statement can be made precise in the setting of computational complexity. For matchings, or spanning trees, or several other structures (for which the corresponding optimization problem is polynomially solvable), we will be able to describe their convex hull in terms of linear inequalities.

Given a set X and a proposed system of inequalities $P = \{x : Ax \leq b\}$, it is usually easy to check whether $conv(X) \subseteq P$. Indeed, for this, we only need to check that every member of X satisfies every inequality in the description of P. The reverse inclusion is more difficult.

- M. X. Goemans, *Lecture Notes on Linear Programming and Polyhedral Combinatorics*. Massachusetts Institute of Technology, 2009. Available online at `http://www-math.mit.edu/~goemans/`
- More generally, to see whether a parametric representation (P-rep) and a canonical half-space representation (H-rep) give rise to the same polyhedron

This talk

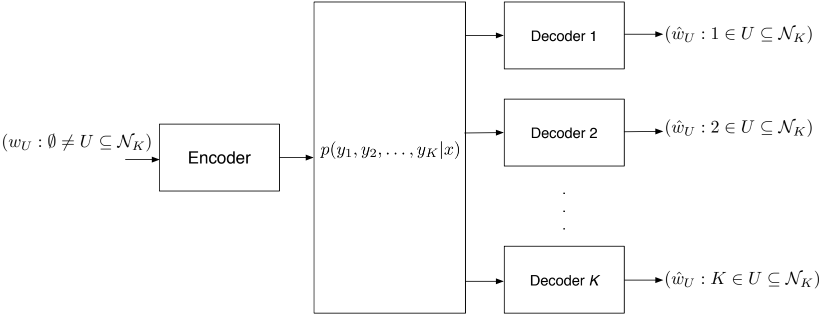
- Goal: To demonstrate that network information theory
  - is not only an ample source for polyhedral combinatorics
  - but also provides new ways of solving them

This talk

- Goal: To demonstrate that network information theory
  - is not only an ample source for polyhedral combinatorics
  - but also provides new ways of solving them
- Two examples:
  - Latency capacity region of broadcast channels
  - Symmetric projections of entropy regions

Latency capacity region of broadcast channels

Broadcast channel with a complete message set

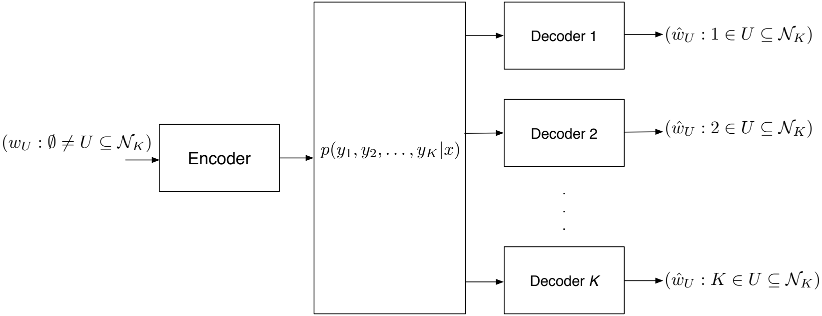


- $2^K - 1$ independent messages at the transmitter:

$$(w_U : \emptyset \neq U \subseteq \mathcal{N}_K)$$

where w_U is a multicast message intended for all receivers $k \in U$

Broadcast channel with a complete message set



- $2^K - 1$ independent messages at the transmitter:

$$(w_U : \emptyset \neq U \subseteq \mathcal{N}_K)$$

  where w_U is a multicast message intended for all receivers $k \in U$

- A computable characterization of the capacity region remains unknown for $K \geq 2$

Latency capacity region

- Assume that a rate tuple

$$\mathbf{R}^* := (R_U^* : \emptyset \neq U \subseteq \mathcal{N}_K)$$

is known to be achievable. What are the other rate tuples whose achievability can be inferred solely from the achievability of $\mathbf{R}^*$?

Latency capacity region

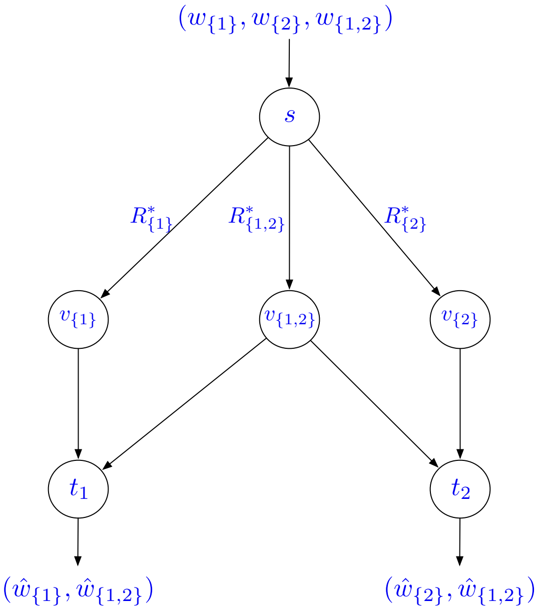
- Assume that a rate tuple

$$\mathbf{R}^* := (R_U^* : \emptyset \neq U \subseteq \mathcal{N}_K)$$

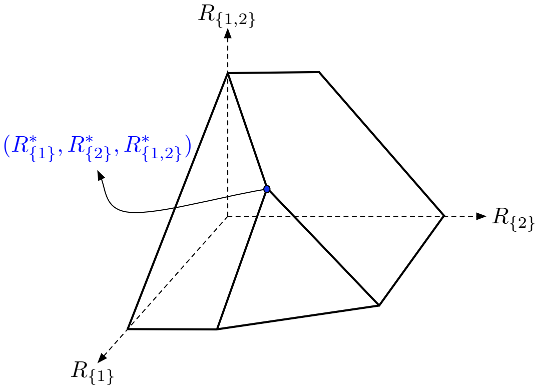
  is known to be achievable. What are the other rate tuples whose achievability can be inferred solely from the achievability of $\mathbf{R}^*$?

- Claim: This is (essentially) a combination-network coding problem

$K = 2$

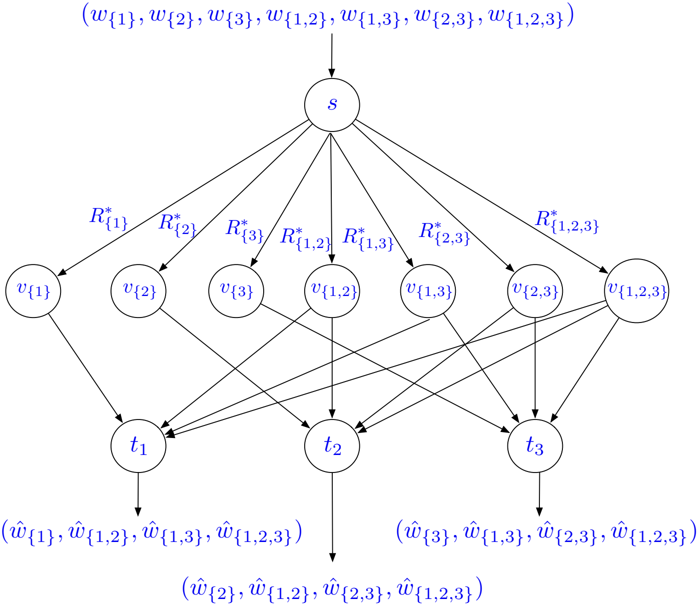


Capacity region



1) $R_{\{1\}}+R_{\{1,2\}} \leq R^*_{\{1\}} + R^*_{\{1,2\}}$
2) $R_{\{2\}}+R_{\{1,2\}} \leq R^*_{\{2\}} + R^*_{\{1,2\}}$
3) $R_{\{1\}}+R_{\{2\}} + R_{\{1,2\}} \leq R^*_{\{1\}} + R^*_{\{2\}} + R^*_{\{1,2\}}$

$K = 3$


$(w_{\{1\}}, w_{\{2\}}, w_{\{3\}}, w_{\{1,2\}}, w_{\{1,3\}}, w_{\{2,3\}}, w_{\{1,2,3\}})$
s
$R^*_{\{1\}}$
$R^*_{\{2\}}$
$R^*_{\{3\}}$
$R^*_{\{1,2\}}$
$R^*_{\{1,3\}}$
$R^*_{\{2,3\}}$
$R^*_{\{1,2,3\}}$
$v_{\{1\}}$
$v_{\{2\}}$
$v_{\{3\}}$
$v_{\{1,2\}}$
$v_{\{1,3\}}$
$v_{\{2,3\}}$
$v_{\{1,2,3\}}$
t_1
t_2
t_3
$(\hat{w}_{\{1\}}, \hat{w}_{\{1,2\}}, \hat{w}_{\{1,3\}}, \hat{w}_{\{1,2,3\}})$
$(\hat{w}_{\{3\}}, \hat{w}_{\{1,3\}}, \hat{w}_{\{2,3\}}, \hat{w}_{\{1,2,3\}})$
$(\hat{w}_{\{2\}}, \hat{w}_{\{1,2\}}, \hat{w}_{\{2,3\}}, \hat{w}_{\{1,2,3\}})$

Capacity region (Grokop-Tse 2008)

1) $R_{\{1\}} + R_{\{1,2\}} + R_{\{1,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{1\}} + R^*_{\{1,2\}} + R^*_{\{1,3\}} + R^*_{\{1,2,3\}}$

2) $R_{\{2\}} + R_{\{1,2\}} + R_{\{2,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{2\}} + R^*_{\{1,2\}} + R^*_{\{2,3\}} + R^*_{\{1,2,3\}}$

3) $R_{\{3\}} + R_{\{1,3\}} + R_{\{2,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{3\}} + R^*_{\{1,3\}} + R^*_{\{2,3\}} + R^*_{\{1,2,3\}}$

4) $R_{\{1\}} + R_{\{2\}} + R_{\{1,2\}} + R_{\{2,3\}} + R_{\{1,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{1\}} + R^*_{\{2\}} + R^*_{\{1,2\}} + R^*_{\{2,3\}} + R^*_{\{1,3\}} + R^*_{\{1,2,3\}}$

5) $R_{\{2\}} + R_{\{3\}} + R_{\{1,2\}} + R_{\{2,3\}} + R_{\{1,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{2\}} + R^*_{\{3\}} + R^*_{\{1,2\}} + R^*_{\{2,3\}} + R^*_{\{1,3\}} + R^*_{\{1,2,3\}}$

6) $R_{\{1\}} + R_{\{3\}} + R_{\{1,2\}} + R_{\{2,3\}} + R_{\{1,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{1\}} + R^*_{\{3\}} + R^*_{\{1,2\}} + R^*_{\{2,3\}} + R^*_{\{1,3\}} + R^*_{\{1,2,3\}}$

7) $R_{\{1\}} + R_{\{2\}} + R_{\{3\}} + R_{\{1,2\}} + R_{\{2,3\}} + R_{\{1,3\}} + R_{\{1,2,3\}}$
$\leq R^*_{\{1\}} + R^*_{\{2\}} + R^*_{\{3\}} + R^*_{\{1,2\}} + R^*_{\{2,3\}} + R^*_{\{1,3\}} + R^*_{\{1,2,3\}}$

8) $R_{\{1\}}+R_{\{2\}}+R_{\{3\}}+2R_{\{1,2\}}+R_{\{2,3\}}+R_{\{1,3\}}+2R_{\{1,2,3\}}$
$\leq R^*_{\{1\}}+R^*_{\{2\}}+R^*_{\{3\}}+2R^*_{\{1,2\}}+R^*_{\{2,3\}}+R^*_{\{1,3\}}+2R^*_{\{1,2,3\}}$

9) $R_{\{1\}}+R_{\{2\}}+R_{\{3\}}+R_{\{1,2\}}+2R_{\{2,3\}}+R_{\{1,3\}}+2R_{\{1,2,3\}}$
$\leq R^*_{\{1\}}+R^*_{\{2\}}+R^*_{\{3\}}+R^*_{\{1,2\}}+2R^*_{\{2,3\}}+R^*_{\{1,3\}}+2R^*_{\{1,2,3\}}$

10) $R_{\{1\}}+R_{\{2\}}+R_{\{3\}}+R_{\{1,2\}}+R_{\{2,3\}}+2R_{\{1,3\}}+2R_{\{1,2,3\}}$
$\leq R^*_{\{1\}}+R^*_{\{2\}}+R^*_{\{3\}}+R^*_{\{1,2\}}+R^*_{\{2,3\}}+2R^*_{\{1,3\}}+2R^*_{\{1,2,3\}}$

11) $R_{\{1\}}+R_{\{2\}}+R_{\{3\}}+2R_{\{1,2\}}+2R_{\{2,3\}}+2R_{\{1,3\}}+2R_{\{1,2,3\}}$
$\leq R^*_{\{1\}}+R^*_{\{2\}}+R^*_{\{3\}}+2R^*_{\{1,2\}}+2R^*_{\{2,3\}}+2R^*_{\{1,3\}}+2R^*_{\{1,2,3\}}$

12) $R_{\{1\}}+2R_{\{2\}}+2R_{\{3\}}+2R_{\{1,2\}}+2R_{\{2,3\}}+2R_{\{1,3\}}+3R_{\{1,2,3\}}$
$\leq R^*_{\{1\}}+2R^*_{\{2\}}+2R^*_{\{3\}}+2R^*_{\{1,2\}}+2R^*_{\{2,3\}}+2R^*_{\{1,3\}}+3R^*_{\{1,2,3\}}$

13) $2R_{\{1\}}+R_{\{2\}}+2R_{\{3\}}+2R_{\{1,2\}}+2R_{\{2,3\}}+2R_{\{1,3\}}+3R_{\{1,2,3\}}$
$\leq 2R^*_{\{1\}}+R^*_{\{2\}}+2R^*_{\{3\}}+2R^*_{\{1,2\}}+2R^*_{\{2,3\}}+2R^*_{\{1,3\}}+3R^*_{\{1,2,3\}}$

14) $2R_{\{1\}}+2R_{\{2\}}+R_{\{3\}}+2R_{\{1,2\}}+2R_{\{2,3\}}+2R_{\{1,3\}}+3R_{\{1,2,3\}}$
$\leq 2R^*_{\{1\}}+2R^*_{\{2\}}+R^*_{\{3\}}+2R^*_{\{1,2\}}+2R^*_{\{2,3\}}+2R^*_{\{1,3\}}+3R^*_{\{1,2,3\}}$

15) $2R_{\{1\}}+2R_{\{2\}}+2R_{\{3\}}+2R_{\{1,2\}}+2R_{\{2,3\}}+2R_{\{1,3\}}+3R_{\{1,2,3\}}$
$\leq 2R^*_{\{1\}}+2R^*_{\{2\}}+2R^*_{\{3\}}+2R^*_{\{1,2\}}+2R^*_{\{2,3\}}+2R^*_{\{1,3\}}+3R^*_{\{1,2,3\}}$

$K > 3$

- Capacity region is unknown in general

$K > 3$

- Capacity region is unknown in general
- Symmetrical setting:

$$R_U = R_k, \quad \forall U \text{ s.t. } |U| = k$$

Capacity region (Tian 2011)

A P-rep of the capacity region:

$$0 \leq R_j \leq \sum_{i=1}^{K} \phi_{i,j} r_{i,j}, \quad \forall j \in \mathcal{N}_K$$

for some nonnegative reals $(r_{i,j} : i, j \in \mathcal{N}_K)$ satisfying

$$\sum_{j=1}^{K} r_{i,j} = R_i^*, \quad \forall i \in \mathcal{N}_K$$

where

$$\phi_{i,j} := \begin{cases} \binom{i}{j}^{-1} \binom{K-j}{i-j}, & \text{if } i \geq j \\ \binom{K-i}{j-i}^{-1} \binom{j-1}{i-1}, & \text{if } i < j \end{cases}$$

Sketched proof

- Achievability:
  - Think of each $i \in \mathcal{N}_K$ as a currency

Sketched proof

- Achievability:
  - Think of each $i \in \mathcal{N}_K$ as a currency
  - The initial amount of currency i is R_i^*

Sketched proof

- Achievability:
  - Think of each $i \in \mathcal{N}_K$ as a currency
  - The initial amount of currency i is R_i^*
  - Split R_i^* into K parts $(r_{i,1}, r_{i,2}, \ldots, r_{i,K})$

Sketched proof

- Achievability:
  - Think of each $i \in \mathcal{N}_K$ as a currency
  - The initial amount of currency i is R_i^*
  - Split R_i^* into K parts $(r_{i,1}, r_{i,2}, \ldots, r_{i,K})$
  - Convert $r_{i,j}$ amount of currency i into $\phi_{i,j} r_{i,j}$ amount of currency j using MDS codes

Sketched proof

- Achievability:
  - Think of each $i \in \mathcal{N}_K$ as a currency
  - The initial amount of currency i is R_i^*
  - Split R_i^* into K parts $(r_{i,1}, r_{i,2}, \ldots, r_{i,K})$
  - Convert $r_{i,j}$ amount of currency i into $\phi_{i,j} r_{i,j}$ amount of currency j using MDS codes
- The converse is akin to the rate region of the symmetrical multi-level diversity coding problem (Yeung-Zhang 1999):
  - Relies on an implicit characterization of the supporting hyperplanes rather than an explicit inequality description of the rate region

Capacity region (Salimi-L-Cui 2013)

An H-rep of the capacity region:

$$\sum_{j=1}^{K} d_Q(j) R_j \leq \sum_{j=1}^{K} d_Q(j) R_j^*, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}$$

where

$$d_Q(j) := \binom{K}{j} \sum_{r=1}^{j} \beta_Q(r)$$

$$\beta_Q(r) := \begin{cases} \prod_{\{q \in Q : q < r\}} (q-1) \prod_{\{q \in Q : q > r\}} q, & \text{if } r \notin Q \\ 0, & \text{if } r \in Q \end{cases}$$

Proof strategy

- Mathematically, it suffices to show that

$$\text{P-rep} = \text{H-rep}$$

using standard polyhedral combinatorics techniques

Proof strategy

- Mathematically, it suffices to show that

$$\text{P-rep} = \text{H-rep}$$

  using standard polyhedral combinatorics techniques

  - Appears to be difficult

Proof strategy

- Mathematically, it suffices to show that

$$\text{P-rep} = \text{H-rep}$$

  using standard polyhedral combinatorics techniques

  - Appears to be difficult

- Our strategy: To show that the H-rep is indeed the capacity region (by proving both achievability and the converse) and hence matching these two representations indirectly

The converse

- Follows directly from the generalized cut-set bounds for broadcast networks (Salimi-L-Cui 2012)

Achievability

- Recall that the H-rep is given by

$$\left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{R} \leq \mathbf{d}_Q^t \mathbf{R}^*, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\}$$

Achievability

- Recall that the H-rep is given by

$$\left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{R} \leq \mathbf{d}_Q^t \mathbf{R}^*, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\}$$
$$= \left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t (\mathbf{R} - \mathbf{R}^*) \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\}$$

Achievability

- Recall that the H-rep is given by

$$\begin{aligned}
&\left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{R} \leq \mathbf{d}_Q^t \mathbf{R}^*, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\
&\quad = \left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t (\mathbf{R} - \mathbf{R}^*) \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\
&\quad = \left\{\mathbf{x} + \mathbf{R}^* \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{x} \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\}
\end{aligned}$$

Achievability

- Recall that the H-rep is given by

$$\begin{aligned}&\left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{R} \leq \mathbf{d}_Q^t \mathbf{R}^*, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\ &\quad = \left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t (\mathbf{R} - \mathbf{R}^*) \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\ &\quad = \left\{\mathbf{x} + \mathbf{R}^* \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{x} \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\ &\quad = \{\mathbf{x} \geq -\mathbf{R}^* : \mathbf{x} \in \mathcal{C}\} + \mathbf{R}^*\end{aligned}$$

  where

$$\mathcal{C} := \left\{\mathbf{x} : \mathbf{d}_Q^t \mathbf{x} \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\}$$

  is a polyhedral cone

Achievability

- Recall that the H-rep is given by

$$\begin{aligned}
&\left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{R} \leq \mathbf{d}_Q^t \mathbf{R}^*, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\
&\quad = \left\{\mathbf{R} \geq \mathbf{0} : \mathbf{d}_Q^t (\mathbf{R} - \mathbf{R}^*) \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\
&\quad = \left\{\mathbf{x} + \mathbf{R}^* \geq \mathbf{0} : \mathbf{d}_Q^t \mathbf{x} \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\} \\
&\quad = \{\mathbf{x} \geq -\mathbf{R}^* : \mathbf{x} \in \mathcal{C}\} + \mathbf{R}^*
\end{aligned}$$

  where

$$\mathcal{C} := \left\{\mathbf{x} : \mathbf{d}_Q^t \mathbf{x} \leq 0, \quad \forall Q \subseteq \mathcal{N}_K \setminus \{1\}\right\}$$

  is a polyhedral cone

- It suffices to prove the achievability of $\mathbf{R}$ which are maximal in the H-rep, which can be written as $\mathbf{x} + \mathbf{R}^*$ for some $\mathbf{x} \geq -\mathbf{R}^*$ which are maximal in $\mathcal{C}$

Characterization of maximal vectors

- First note that if $\mathbf{x}$ is maximal in $\mathcal{C}$, then there must exist a $Q \subseteq \mathcal{N}_K \setminus \{1\}$ such that

$$\mathbf{d}_Q^t \mathbf{x} = 0$$

Characterization of maximal vectors

- First note that if $\mathbf{x}$ is maximal in $\mathcal{C}$, then there must exist a $Q \subseteq \mathcal{N}_K \setminus \{1\}$ such that

$$\mathbf{d}_Q^t \mathbf{x} = 0$$

- For each $j \in \mathcal{N}_{K-1}$, define the exchange vectors between currencies j and $j+1$ as

$$\begin{aligned} \mathbf{v}_j^+ &:= \phi_{j+1,j}\mathbf{e}_j - \mathbf{e}_{j+1} \quad (j+1 \to j) \\ \mathbf{v}_j^- &:= \phi_{j,j+1}\mathbf{e}_{j+1} - \mathbf{e}_j \quad (j \to j+1) \end{aligned}$$

Facts

- Fact 1: For each $Q \subseteq \mathcal{N}_K \setminus \{1\}$ and $j \in \mathcal{N}_{K-1}$, we have

$$\mathbf{d}_Q^t \mathbf{v}_j^+ \begin{cases} = 0, & \text{if } \ j+1 \in Q \\ < 0, & \text{if } \ j+1 \notin Q \end{cases}$$

$$\text{and} \quad \mathbf{d}_Q^t \mathbf{v}_j^- \begin{cases} < 0, & \text{if } \ j+1 \in Q \\ = 0, & \text{if } \ j+1 \notin Q \end{cases}$$

Facts

- Fact 1: For each $Q \subseteq \mathcal{N}_K \setminus \{1\}$ and $j \in \mathcal{N}_{K-1}$, we have

$$\mathbf{d}_Q^t \mathbf{v}_j^+ \begin{cases} = 0, & \text{if } j+1 \in Q \\ < 0, & \text{if } j+1 \notin Q \end{cases}$$

$$\text{and} \quad \mathbf{d}_Q^t \mathbf{v}_j^- \begin{cases} < 0, & \text{if } j+1 \in Q \\ = 0, & \text{if } j+1 \notin Q \end{cases}$$

- Fact 2: Fix $Q \subseteq \mathcal{N}_K \setminus \{1\}$ and let $(\mathbf{v}_j^* : j \in \mathcal{N}_{K-1})$ be the set of vectors such that

$$\mathbf{d}_Q^t \mathbf{v}_j^* = 0, \quad \forall j \in \mathcal{N}_{K-1}$$

  where $*$ equals either $+$ or $-$. Then, $(\mathbf{v}_j^* : j \in \mathcal{N}_{K-1})$ are linearly independent

Characterization of maximal vectors

- Any $\mathbf{x} \in \mathcal{C}$ such that $\mathbf{d}_Q^t \mathbf{x} = 0$ can be written as a conic combination of $(\mathbf{v}_j^* : j \in \mathcal{N}_{K-1})$, i.e.,

$$\mathbf{x} = \sum_{j=1}^{K-1} \lambda_j \mathbf{v}_j^*$$

for some $(\lambda_j \geq 0 : j \in \mathcal{N}_{K-1})$

Characterization of maximal vectors

- Any $\mathbf{x} \in \mathcal{C}$ such that $\mathbf{d}_Q^t \mathbf{x} = 0$ can be written as a conic combination of $(\mathbf{v}_j^* : j \in \mathcal{N}_{K-1})$, i.e.,

$$\mathbf{x} = \sum_{j=1}^{K-1} \lambda_j \mathbf{v}_j^*$$

  for some $(\lambda_j \geq 0 : j \in \mathcal{N}_{K-1})$

- Any $\mathbf{R}$ which is maximal in the H-rep can be written as

$$\mathbf{R} = \sum_{j=1}^{K-1} \lambda_j \mathbf{v}_j^* + \mathbf{R}^*$$

  for some $(\lambda_j \geq 0 : j \in \mathcal{N}_{K-1})$ such that

$$\sum_{j=1}^{K-1} \lambda_j \mathbf{v}_j^* \geq -\mathbf{R}^*$$

Transaction graph

- Each arc between vertices j and $j+1$ represent the exchange between currencies j and $j+1$

Successive encoding

$$\mathbf{R}^{(0)} = \mathbf{R}^*$$

Successive encoding

$$\mathbf{R}^{(0)} = \mathbf{R}^*$$

$$\mathbf{R}^{(1)} = \mathbf{R}^{(0)} + \lambda_1 \mathbf{v}_1^*$$

Successive encoding

$$\mathbf{R}^{(0)} = \mathbf{R}^*$$

$$\mathbf{R}^{(1)} = \mathbf{R}^{(0)} + \lambda_1 \mathbf{v}_1^*$$

$$\mathbf{R}^{(2)} = \mathbf{R}^{(1)} + \lambda_2 \mathbf{v}_2^*$$

Successive encoding

1 $\mathbf{R}^{(0)} = \mathbf{R}^*$

2 $\mathbf{R}^{(1)} = \mathbf{R}^{(0)} + \lambda_1 \mathbf{v}_1^*$

3 $\mathbf{R}^{(2)} = \mathbf{R}^{(1)} + \lambda_2 \mathbf{v}_2^*$

$\vdots$

K $\mathbf{R}^{(K-1)} = \mathbf{R}^{(K-2)} + \lambda_{K-1} \mathbf{v}_{K-1}^*$

Loan-free scheduling

- Caveat: To implement the exchanges using MDS codes, we need

$$\mathbf{R}^{(k)} \geq \mathbf{0}, \quad \forall k \in \mathcal{N}_{K-1}$$

not just

$$\mathbf{R}^{(K-1)} = \mathbf{R} \geq \mathbf{0}$$

as guaranteed by the choices of $(\lambda_j : j \in \mathcal{N}_{K-1})$

Loan-free scheduling

- Caveat: To implement the exchanges using MDS codes, we need

$$\mathbf{R}^{(k)} \geq \mathbf{0}, \quad \forall k \in \mathcal{N}_{K-1}$$

not just

$$\mathbf{R}^{(K-1)} = \mathbf{R} \geq \mathbf{0}$$

as guaranteed by the choices of $(\lambda_j : j \in \mathcal{N}_{K-1})$

- Loan-free scheduling: Need to find a permutation π on $\mathcal{N}_{K-1}$ such that

$$\mathbf{R}^{(k)} := \mathbf{R}^{(k-1)} + \lambda_{\pi(k)} \mathbf{v}^*_{\pi(k)} \geq \mathbf{0}, \quad \forall k \in \mathcal{N}_{K-1}$$

Observations

- Fix $j \in \mathcal{N}_K$. Then each transaction can either increase, decrease, or retain the amount of currency j

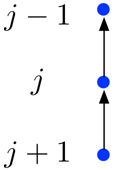
Observations

- Fix $j \in \mathcal{N}_K$. Then each transaction can either increase, decrease, or retain the amount of currency j
- On the other hand, each currency j can involve at most two transactions

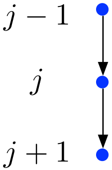
Observations

- Fix $j \in \mathcal{N}_K$. Then each transaction can either increase, decrease, or retain the amount of currency j
- On the other hand, each currency j can involve at most two transactions
- Two concerning scenarios:

Case 1: $\pi(j-1) < \pi(j)$



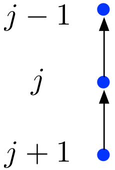
Case 2: $\pi(j) < \pi(j-1)$



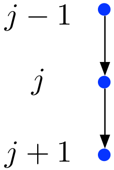
Observations

- Fix $j \in \mathcal{N}_K$. Then each transaction can either increase, decrease, or retain the amount of currency j
- On the other hand, each currency j can involve at most two transactions
- Two concerning scenarios:

Case 1: $\pi(j-1) < \pi(j)$



Case 2: $\pi(j) < \pi(j-1)$



- Main challenge: To find a single permutation π to avoid the above two scenarios for every $j \in \mathcal{N}_K$

Loan-free scheduling

- First order the currencies $j \in \mathcal{N}_K$ according to a topological order of the graph (which is obviously acyclic)

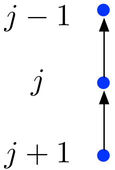
Loan-free scheduling

- First order the currencies $j \in \mathcal{N}_K$ according to a topological order of the graph (which is obviously acyclic)
- Next, order the acs of the graph (each representing a transaction) based on the order of their starting vertices:
  - Arbitrarily break the tie if two arcs share the same starting vertex

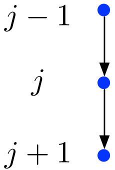
Loan-free scheduling

- First order the currencies $j \in \mathcal{N}_K$ according to a topological order of the graph (which is obviously acyclic)
- Next, order the acs of the graph (each representing a transaction) based on the order of their starting vertices:
  - Arbitrarily break the tie if two arcs share the same starting vertex
- Validation:

Case 1: $\pi(j) < \pi(j-1)$



Case 2: $\pi(j-1) < \pi(j)$



Summary

- A P-rep (Tian 2011):
  - Established via the rate-splitting scheme
  - A converse-centric approach

Summary

- A P-rep (Tian 2011):
  - Established via the rate-splitting scheme
  - A converse-centric approach
- An H-rep (Salimi-L-Cui 2013):
  - Established via the generalized cut-set bounds for broadcast networks
  - An achievability-centric approach

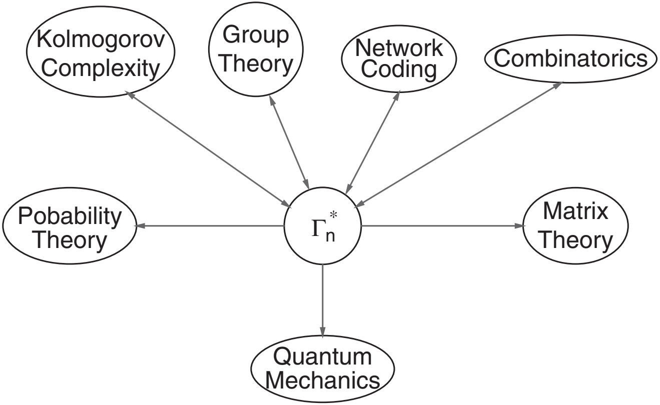
Summary

- A P-rep (Tian 2011):
  - Established via the rate-splitting scheme
  - A converse-centric approach
- An H-rep (Salimi-L-Cui 2013):
  - Established via the generalized cut-set bounds for broadcast networks
  - An achievability-centric approach
- The mathematical output is an information-theoretic solution to a polyhedral combinatorics problem

A. Salimi, T. Liu, and S. Cui, "Polyhedral description of latency capacity region of broadcast channels," in *Proc. 2014 IEEE Int. Sym. Inf. Theory*, Honolulu, HI, June–July 2014

Symmetric projections of entropy regions

Facets of entropy (Yeung 2009)



Entropy region

- Fix $n \in \mathcal{N}$. A vector $\mathbf{h}$ indexed by

  $$\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$$

  is called *entropic* if

  $$h_U = H(X_i : i \in U), \quad \emptyset \neq U \subseteq \mathcal{N}_n$$

  for some jointly distributed discrete random vector $(X_1, \ldots, X_n)$

Entropy region

- Fix $n \in \mathcal{N}$. A vector $\mathbf{h}$ indexed by

$$\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$$

is called *entropic* if

$$h_U = H(X_i : i \in U), \quad \emptyset \neq U \subseteq \mathcal{N}_n$$

for some jointly distributed discrete random vector $(X_1, \ldots, X_n)$

- The collection of all entropic vectors (over n variables) is called the *entropy region* and is usually denoted by Γ_n^*

Entropy region

- Fix $n \in \mathcal{N}$. A vector $\mathbf{h}$ indexed by

$$\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$$

  is called *entropic* if

$$h_U = H(X_i : i \in U), \quad \emptyset \neq U \subseteq \mathcal{N}_n$$

  for some jointly distributed discrete random vector $(X_1, \ldots, X_n)$

- The collection of all entropic vectors (over n variables) is called the *entropy region* and is usually denoted by Γ_n^*

- For the purposes of studying network coding capacities and unconstrained information inequalities, it suffices to study $cl(\Gamma_n^*)$, which is known to be a convex cone (Zhang-Yeung 1997)

Two concerns from the application viewpoint

- Dimensionality:
  - The dimension of $cl(\Gamma_n^*)$ is $2^n - 1$

Two concerns from the application viewpoint

- Dimensionality:
  - The dimension of $cl(\Gamma_n^*)$ is $2^n - 1$
- Descriptive complexity:
  - The number of independent Shannon-type inequalities (elemental inequalities) is

$$n + \binom{n}{2} 2^{n-2}$$

Two concerns from the application viewpoint

- Dimensionality:
  - The dimension of $cl(\Gamma_n^*)$ is $2^n - 1$
- Descriptive complexity:
  - The number of independent Shannon-type inequalities (elemental inequalities) is

$$n + \binom{n}{2} 2^{n-2}$$

  - For $n \geq 4$, there are infinite independent non-Shannon-type inequalities (Matúš 2007)

Dimension reduction via symmetric projection

- Sometimes it suffices to consider the entropies averaged over the subsets of $\mathcal{N}_n$

Dimension reduction via symmetric projection

- Sometimes it suffices to consider the entropies averaged over the subsets of $\mathcal{N}_n$
- For example, to solve the symmetrical multilevel diversity coding problem, it suffices to consider Han's subset inequality:

$$H_1 \geq \frac{H_2}{2} \geq \cdots \geq \frac{H_n}{n}$$

where

$$H_k := \frac{1}{\binom{n}{k}} \sum_{U \subseteq \mathcal{N}_n : |U| = k} H(X_i : i \in U)$$

Dimension reduction via symmetric projection

- Sometimes it suffices to consider the entropies averaged over the subsets of $\mathcal{N}_n$
- For example, to solve the symmetrical multilevel diversity coding problem, it suffices to consider Han's subset inequality:

$$H_1 \geq \frac{H_2}{2} \geq \cdots \geq \frac{H_n}{n}$$

where

$$H_k := \frac{1}{\binom{n}{k}} \sum_{U \subseteq \mathcal{N}_n : |U| = k} H(X_i : i \in U)$$

- Question: What are the other information inequalities that relate $H_1, \ldots, H_n$ (Han 1978, Chen-He-Jiang-Wang 2009)?

Average entropy region

- Average entropy region:

$$P\Gamma_n^* := \left\{ (H_1, \ldots, H_n) : H_k = \frac{1}{\left(\begin{array}{c} n \\ \alpha \end{array} \right)} \sum_{U \subseteq \mathcal{N}_n : |U| = \alpha} h_U \right.$$

$$\left. \text{for some } (h_U : \emptyset \neq U \subseteq \mathcal{N}_n) \in \Gamma_n^* \right\}$$

Average entropy region

- Average entropy region:

$$P\Gamma_n^* := \left\{ (H_1, \ldots, H_n) : H_k = \frac{1}{\left(\begin{array}{c} n \\ \alpha \end{array}\right)} \sum_{U \subseteq \mathcal{N}_n : |U| = \alpha} h_U \right.$$
$$\left. \text{for some } (h_U : \emptyset \neq U \subseteq \mathcal{N}_n) \in \Gamma_n^* \right\}$$

- Goal: To characterize $cl(P\Gamma_n^*)$

Average entropy region

- Average entropy region:

$$P\Gamma_n^* := \left\{(H_1, \ldots, H_n) : H_k = \frac{1}{\begin{pmatrix} n \\ \alpha \end{pmatrix}} \sum_{U \subseteq \mathcal{N}_n : |U| = \alpha} h_U \right.$$

$$\left. \text{for some } (h_U : \emptyset \neq U \subseteq \mathcal{N}_n) \in \Gamma_n^* \right\}$$

- Goal: To characterize $cl(P\Gamma_n^*)$

  1) Characterize $P\Gamma_n$ (which is an outer bound for $cl(P\Gamma_n^*)$)

Average entropy region

- Average entropy region:

$$P\Gamma_n^* := \Big\{(H_1, \dots, H_n) : H_k = \frac{1}{\binom{n}{\alpha}} \sum_{U \subseteq \mathcal{N}_n : |U| = \alpha} h_U$$

$$\text{for some } (h_U : \emptyset \neq U \subseteq \mathcal{N}_n) \in \Gamma_n^* \Big\}$$

- Goal: To characterize $cl(P\Gamma_n^*)$
  1) Characterize $P\Gamma_n$ (which is an outer bound for $cl(P\Gamma_n^*)$)
  2) Check whether $P\Gamma_n = cl(P\Gamma_n^*)$?

Average entropy region

- Average entropy region:

$$P\Gamma_n^* := \left\{ (H_1, \ldots, H_n) : H_k = \frac{1}{\binom{n}{\alpha}} \sum_{U \subseteq \mathcal{N}_n : |U| = \alpha} h_U \right.$$
$$\left. \text{for some } (h_U : \emptyset \neq U \subseteq \mathcal{N}_n) \in \Gamma_n^* \right\}$$

- Goal: To characterize $cl(P\Gamma_n^*)$
  1) Characterize $P\Gamma_n$ (which is an outer bound for $cl(P\Gamma_n^*)$)
  2) Check whether $P\Gamma_n = cl(P\Gamma_n^*)$?
  3) Add non-Shannon-type inequalities (all permutation included) to Γ_n and repeat Step 1)

Step 1) Characterizing $P\Gamma_n$

- Fact: For any convex, permutation symmetric set Θ of length-$(2^n - 1)$ vectors $\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$, we have

$$P\Theta = P\Theta'$$

where

$$\Theta' := \left\{ \mathbf{h} : h_U = h_{U'},\ \forall |U| = |U'| \right\}$$

Step 1) Characterizing $P\Gamma_n$

- Fact: For any convex, permutation symmetric set Θ of length-$(2^n - 1)$ vectors $\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$, we have

$$P\Theta = P\Theta'$$

where

$$\Theta' := \left\{\mathbf{h} : h_U = h_{U'},\ \forall |U| = |U'|\right\}$$

- Thus, setting

$$h_U = H_k, \quad \forall U \subseteq \mathcal{N}_n \text{ s.t. } |U| = k$$

in the elemental inequalities, we conclude that $P\Gamma_n$ is given by all $(H_1, \ldots, H_n)$ satisfying:

$$2H_k - H_{k-1} - H_{k+1} \geq 0, \quad \forall k \in \mathcal{N}_{n-1}$$
$$H_n - H_{n-1} \geq 0$$

Step 2) $P\Gamma_n = cl(P\Gamma_n^*)$?

- First compute the extreme rays of $P\Gamma_n$ as:

$$\mathbf{r}_k = (1\ 2\ \cdots\ k\ \cdots\ k), \quad k \in \mathcal{N}_n$$

Step 2) $P\Gamma_n = cl(P\Gamma_n^*)$?

- First compute the extreme rays of $P\Gamma_n$ as:

$$\mathbf{r}_k = (1\ 2\ \cdots\ k\ \cdots\ k), \quad k \in \mathcal{N}_n$$

- Note that for any $k \in \mathcal{N}_n$, $\mathbf{r}_k$ is the rank profile of an (n, k) MDS code. We thus have

$$\mathbf{r}_k \in P cl(\Gamma_n^*) \subseteq cl(P\Gamma_n^*)$$

Step 2) $P\Gamma_n = cl(P\Gamma_n^*)$?

- First compute the extreme rays of $P\Gamma_n$ as:

$$\mathbf{r}_k = (1\ 2\ \cdots\ k\ \cdots\ k), \quad k \in \mathcal{N}_n$$

- Note that for any $k \in \mathcal{N}_n$, $\mathbf{r}_k$ is the rank profile of an (n, k) MDS code. We thus have

$$\mathbf{r}_k \in Pcl(\Gamma_n^*) \subseteq cl(P\Gamma_n^*)$$

- We thus conclude that

$$P\Gamma_n \subseteq cl(P\Gamma_n^*)$$

and hence

$$P\Gamma_n = cl(P\Gamma_n^*)$$

i.e., there are no non-Shannon-type inequalities that relate $H_1, \ldots, H_n$

Complexity reduction via symmetric projection

- Entropy region Γ_n^*:
  - Dimension $= 2^n - 1$
- Symmetrical projection $P\Gamma_n^*$:
  - Dimension $= n$

Complexity reduction via symmetric projection

- Entropy region Γ_n^*:
  - Dimension $= 2^n - 1$
  - Non-polyhedral for $n \geq 4$
- Symmetrical projection $P\Gamma_n^*$:
  - Dimension $= n$
  - Completely characterized by n Shannon-type inequalities

Partially symmetric projections

- Let G be a group of permutations over $\mathcal{N}_n$. Consider the group action on the nonempty subsets of $\mathcal{N}_n$. Then, the orbits of G forms a partition of all $2^n - 1$ nonempty subsets of $\mathcal{N}_n$

Partially symmetric projections

- Let G be a group of permutations over $\mathcal{N}_n$. Consider the group action on the nonempty subsets of $\mathcal{N}_n$. Then, the orbits of G forms a partition of all $2^n - 1$ nonempty subsets of $\mathcal{N}_n$
- Let $O_1, \ldots, O_m$ be the collection of all distinct orbits of G. For any length-$(2^n - 1)$ vector $(h_S : \emptyset \neq U \subseteq \mathcal{N}_n)$, the *orbit averages* are defined as

$$H_k := \frac{1}{|O_k|} \sum_{U \in O_k} h_U, \quad \forall k \in \mathcal{N}_m$$

Partially symmetric projections

- Let G be a group of permutations over $\mathcal{N}_n$. Consider the group action on the nonempty subsets of $\mathcal{N}_n$. Then, the orbits of G forms a partition of all $2^n - 1$ nonempty subsets of $\mathcal{N}_n$
- Let $O_1, \ldots, O_m$ be the collection of all distinct orbits of G. For any length-$(2^n - 1)$ vector $(h_S : \emptyset \neq U \subseteq \mathcal{N}_n)$, the *orbit averages* are defined as

$$H_k := \frac{1}{|O_k|} \sum_{U \in O_k} h_U, \quad \forall k \in \mathcal{N}_m$$

- We shall call the above projection from $\boldsymbol{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$ to $\boldsymbol{H} = (H_k : k \in \mathcal{N}_m)$ the projection *induced* by G and denote it by P_G

Classification of permutation groups

- When $G = \{(1)\}$,
  - $P\Gamma_n^* = \Gamma_n^*$

Classification of permutation groups

- When $G = \{(1)\}$,
  - $P\Gamma_n^* = \Gamma_n^*$
- When $G = S_n$,
  - $O_k = \{U \subseteq \mathcal{N}_n : |U| = k\}$
  - $cl(P\Gamma_n^*) = P\Gamma_n$

Classification of permutation groups

- When $G = \{(1)\}$,
  - $P\Gamma_n^* = \Gamma_n^*$
- When $G = S_n$,
  - $O_k = \{U \subseteq \mathcal{N}_n : |U| = k\}$
  - $cl(P\Gamma_n^*) = P\Gamma_n$
- When $G \subseteq S_n$,
  - $cl(P\Gamma_n^*) = P\Gamma_n?$

Classification of permutation groups

- When $G = \{(1)\}$,
  - $P\Gamma_n^* = \Gamma_n^*$
- When $G = S_n$,
  - $O_k = \{U \subseteq \mathcal{N}_n : |U| = k\}$
  - $cl(P\Gamma_n^*) = P\Gamma_n$
- When $G \subseteq S_n$,
  - $cl(P\Gamma_n^*) = P\Gamma_n$?
  - Is $cl(P\Gamma_n^*)$ polyhedral?

Challenges

- Characterizing $P_G\Gamma_n$:
  - Let G be a subgroup of S_n. For any convex, permutation symmetric set Θ of length-(2^n-1) vectors $\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$, we have

$$P_G\Theta = P_G\Theta'$$

where

$$\Theta' := \{\mathbf{h} : h_U = h_{U'},\ \forall U, U' \text{ in the same orbit of } G\}$$

Challenges

- Characterizing $P_G\Gamma_n$:
  - Let G be a subgroup of S_n. For any convex, permutation symmetric set Θ of length-$(2^n - 1)$ vectors $\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$, we have

$$P_G\Theta = P_G\Theta'$$

    where

$$\Theta' := \{\mathbf{h} : h_U = h_{U'},\ \forall U, U' \text{ in the same orbit of } G\}$$

- $P\Gamma_n = cl(P\Gamma_n^*)$:
  - Need to "compute" the extreme rays of $P\Gamma_n$ (polyhedral combinatorics)

Challenges

- Characterizing $P_G\Gamma_n$:
  - Let G be a subgroup of S_n. For any convex, permutation symmetric set Θ of length-$(2^n - 1)$ vectors $\mathbf{h} = (h_U : \emptyset \neq U \subseteq \mathcal{N}_n)$, we have

$$P_G\Theta = P_G\Theta'$$

    where

$$\Theta' := \{\mathbf{h} : h_U = h_{U'},\ \forall U, U' \text{ in the same orbit of } G\}$$

- $P\Gamma_n = cl(P\Gamma_n^*)$:
  - Need to "compute" the extreme rays of $P\Gamma_n$ (polyhedral combinatorics)
  - Need to verify wether the extreme rays are almost entropic or not (representable matroids)

Q. Chen and R. W. Yeung, "Two-partition-symmetrical entropy function regions," in *Proc. 2013 IEEE Inf. Th. Workshop*, Sevilla, Spain, Sept. 2013, pp. 1–5

A. Salimi, T. Liu, S. Cui, C. Tian, and J. Chen, "Symmetric projections of entropy regions," in preparation