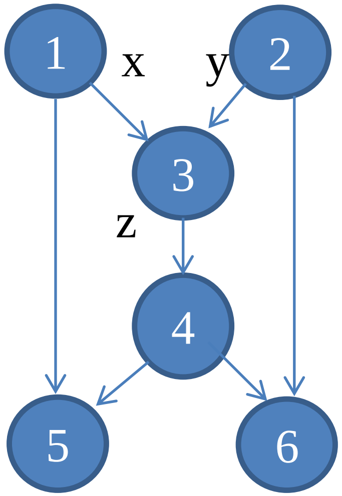
Multisource Multisink Network coding Capacities region found from the Region of entropic vectors.

Presented by :
Alexander Erick Trofimoff
PhD student
ECE department
Drexel University

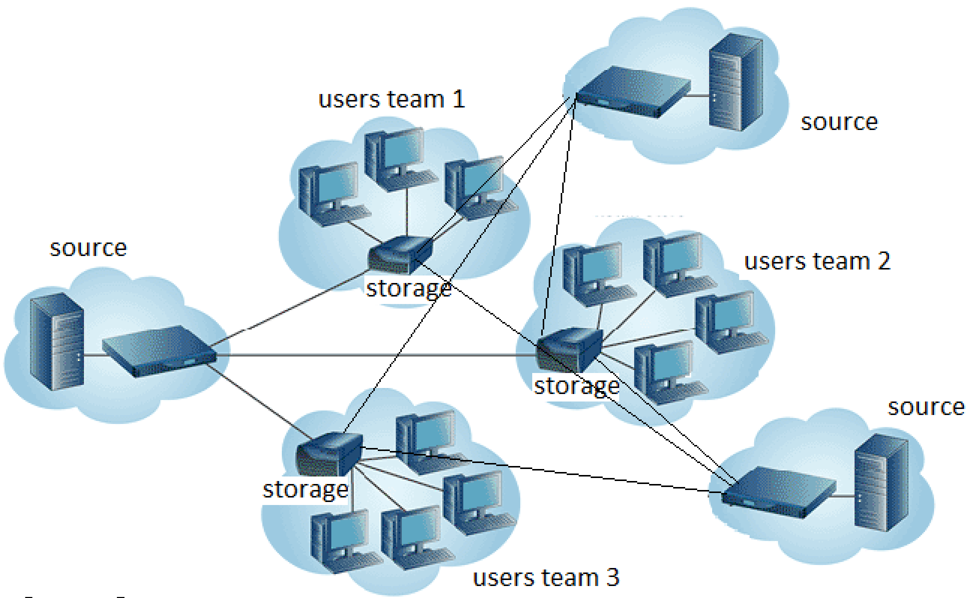
Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



Application Problems :

- ✓ Distributed Storage
- ✓ Max flow



Aspects of interest :

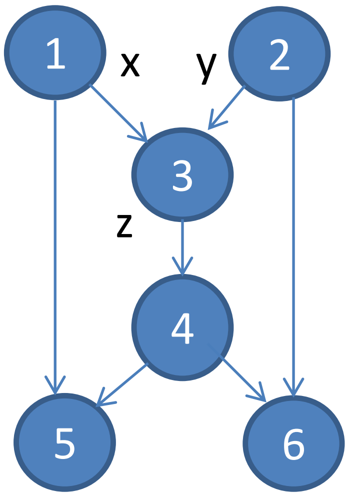
✓ How much can be communicated ?:
Links capacities & encoding nodes.

✓ Variables of interest
original source rates & the capacities of the edges.

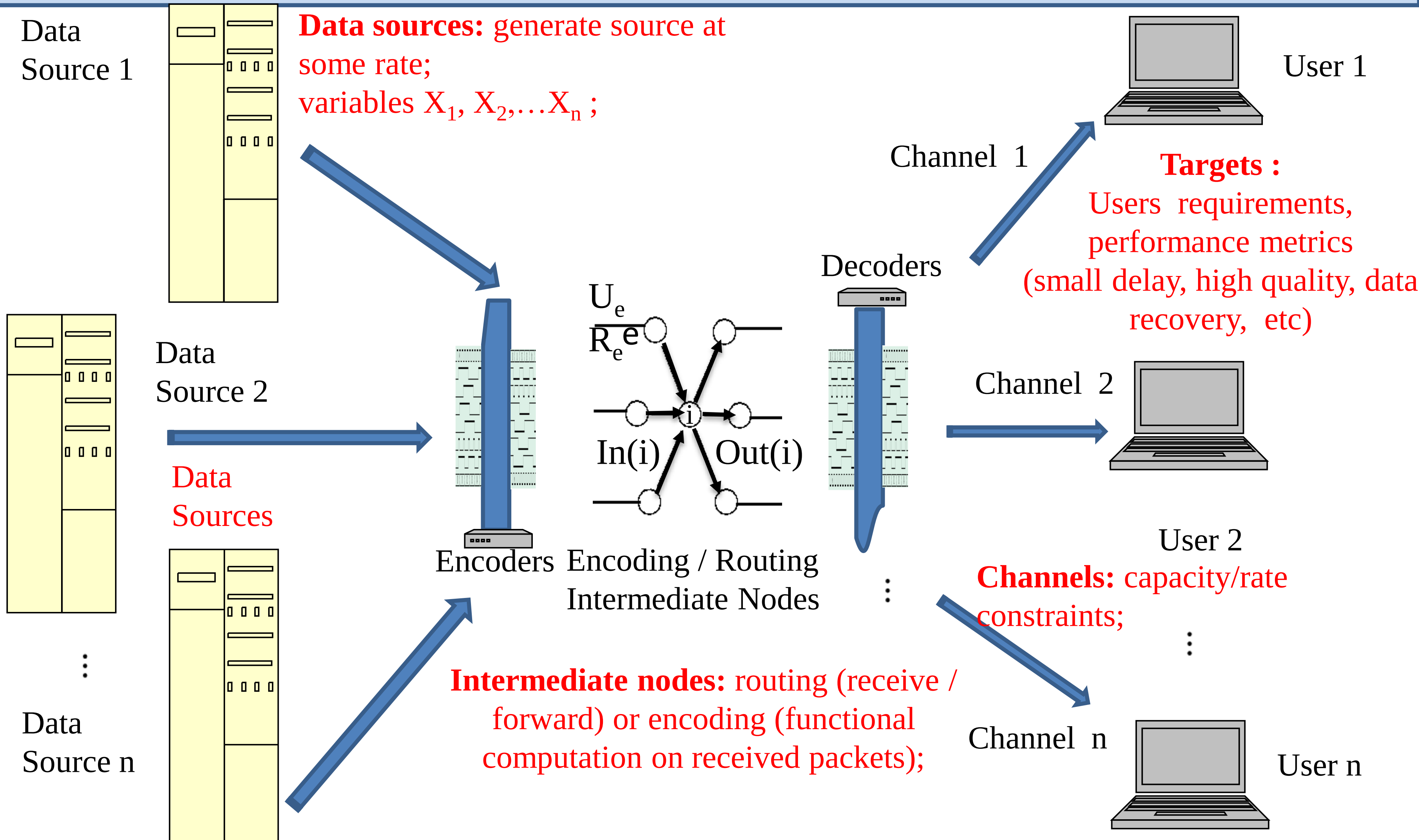
✓ Aspects to consider
The upper bounds of edge capacities,
over all possible ways of encoding messages on
intermediate nodes.

Presentation Outline

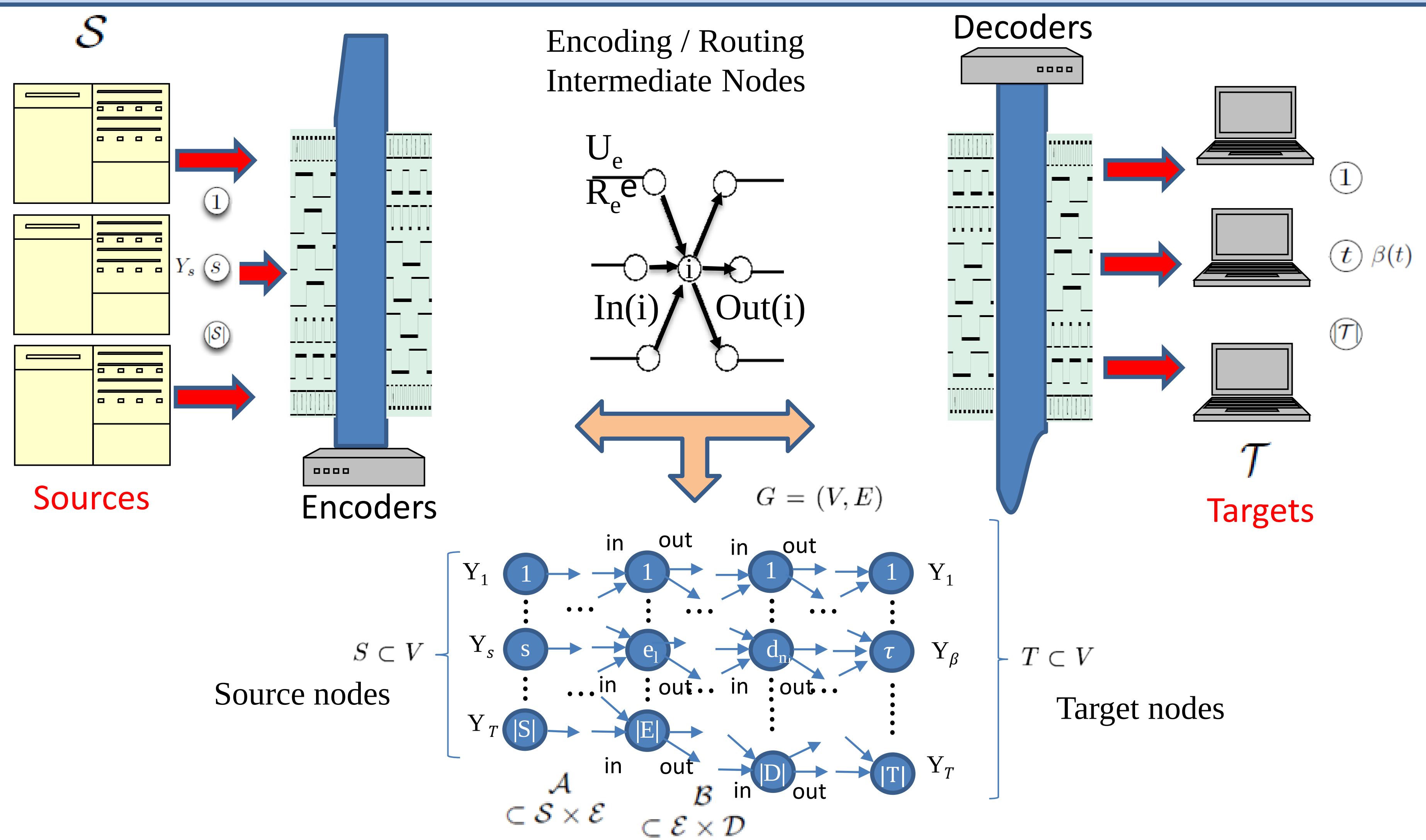
1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



1.General Acyclic Mutisource Multisink Network coding framework

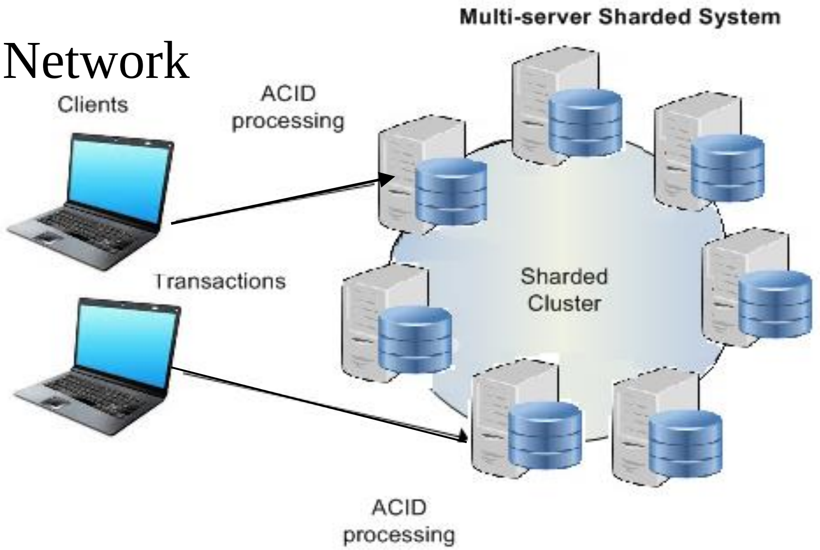


1.General Acyclic Mutisource Multisink Network coding framework



Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



The Region of capabilities in a distributed storage system

- ✓ **Parallel processing:** data distributed to speed computations.
- ✓ **Fault Tolerance:** Data distributed using secret sharing analysis techniques, originally developed to assure privacy.
- ✓ Using **Galois field and Network flow theories**, information can be stored at different sites with minimum of redundancy.
- ✓ This **prevents loss of data** if several sites become inaccessible.

Problem: Protection of multiple sites failures minimizing the storage used.

$$(V_1, \ldots, V_k) = (U_1, \ldots, U_k) \overbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_k^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_k^{k-1} \end{pmatrix}}^{A}$$

$\alpha_j \in GF(q^t)$ $\quad V_j \in GF(2^{C_k})$

$t = C_k$ (the number of bits per disk) $\quad q = 2$ (binary alphabet)

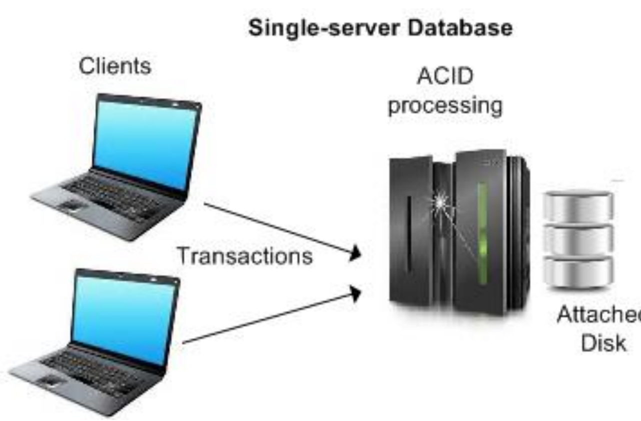
Distributed information Storage, J R Roche, Department of Statistics, Stanford U., Technical report No.79, 1992

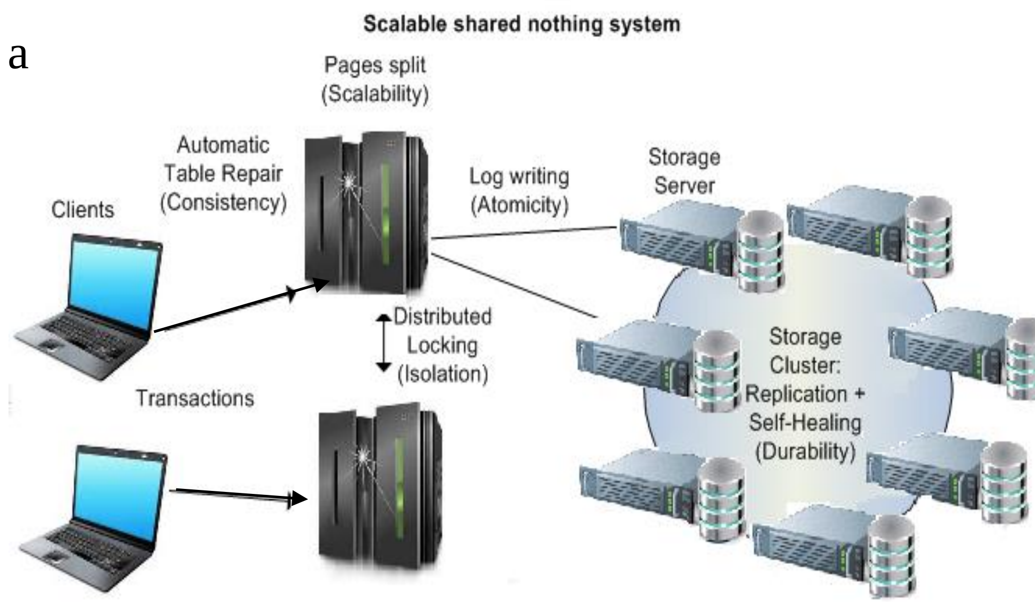
The Region of capabilities in a distributed storage system

Problem : Distributed storage Backup systems to **restore information** from Disk failures.

Scenario: large **distributed storage system**, when disk failures,

Goal : Need to **repair itself** without requiring a whole lot of bandwidth to fix a disk? ,





Distributed information Storage, J R Roche, Department of Statistics, Stanford U., Technical report No.79, 1992

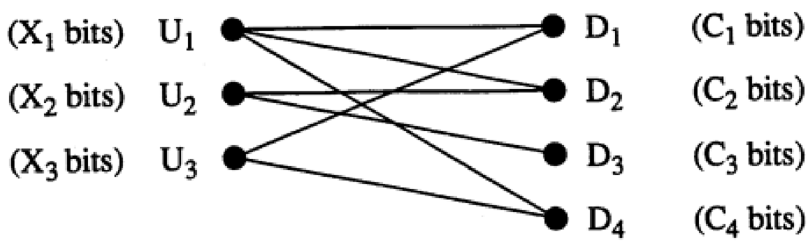
The Region of capabilities in a distributed storage system

Requirements : The disk when it is repaired be exactly **as it was before**.

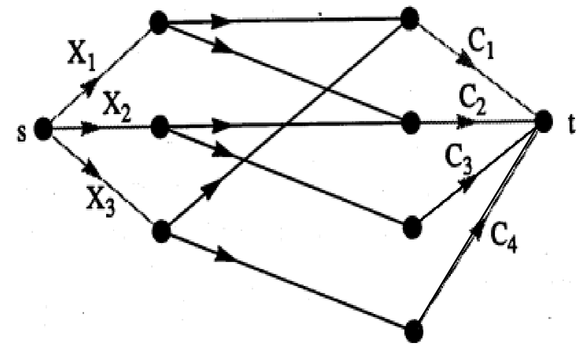
Read the data from this way **without having to pull too much**.

Motivation:

The **fundamental limits** of this problem are **instances of network codes**.



Storage Network



Equivalent flow Network

$$C_1 \leq C_2 \leq \ldots \leq C_n$$

$$C_{\max} = C_1 + \ldots + C_k$$

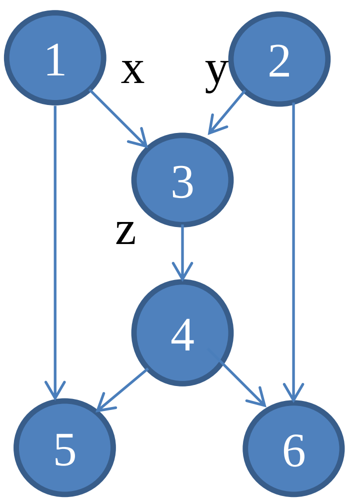
$$V_j = U_1 + \alpha_j U_2 + \alpha_j^2 U_3 + \ldots + \alpha_j^{k-1} U_k$$

$$1 \leq j \leq k$$

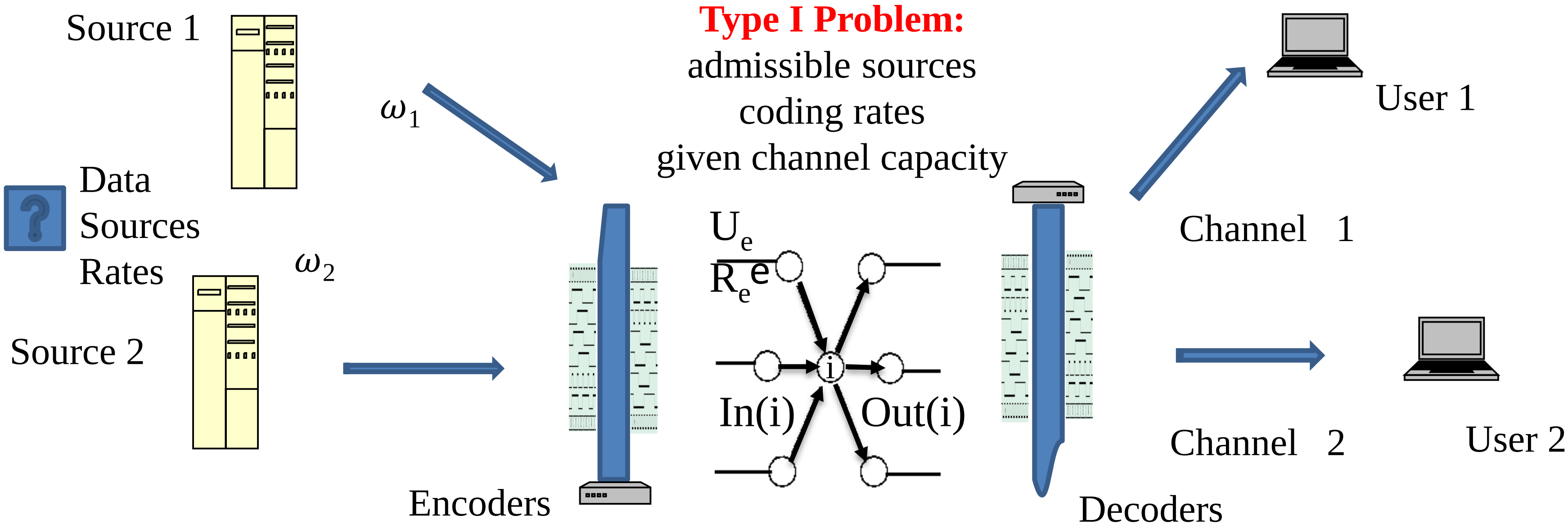
Distributed information Storage, J R Roche, Department of Statistics, Stanford U., Technical report No.79, 1992

Presentation Outline

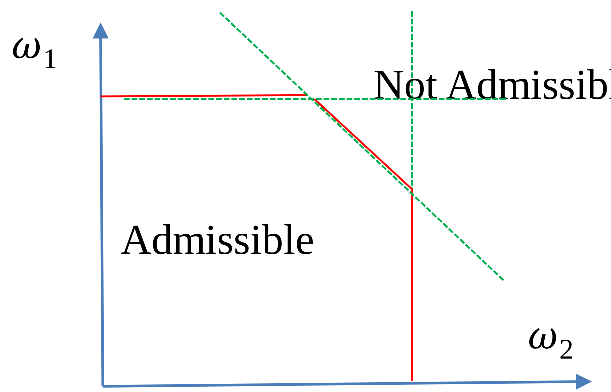
1. Motivation : Acyclic Multisource Multisink Network coding
   Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



The rate regions for Information flow on communication Wireless Network



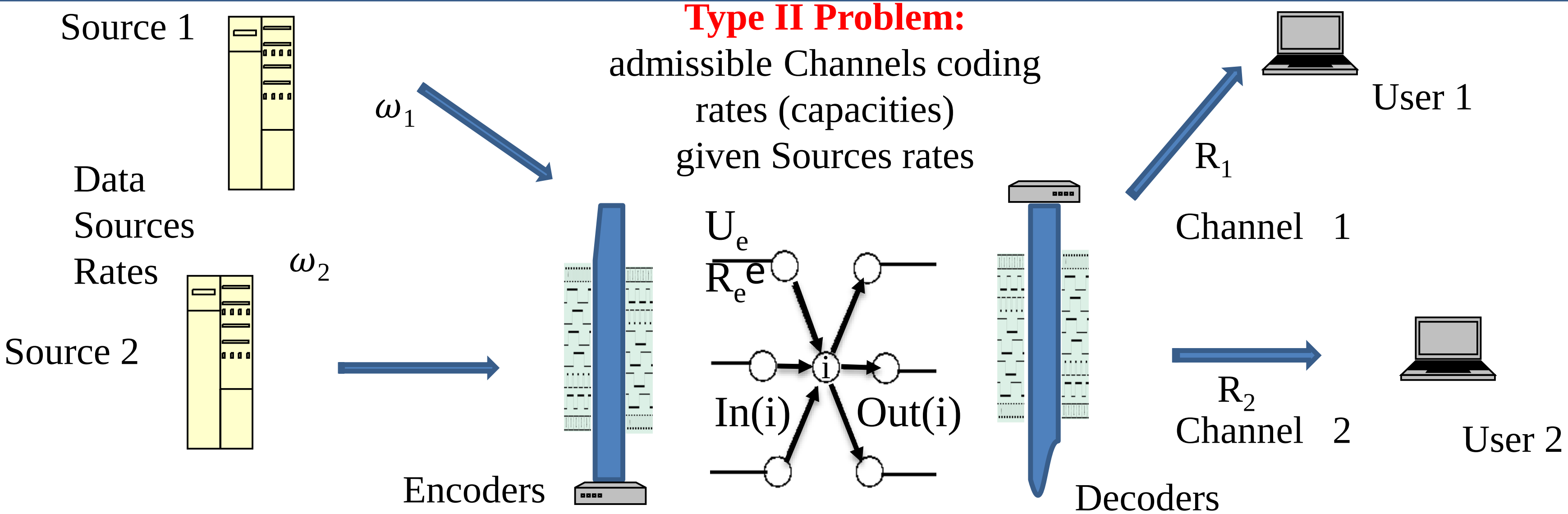
S. R. Region **W** Optimizing over all Codes



If ω is admissible, and $\omega' \leq \omega \rightarrow \omega'$ is admissible.

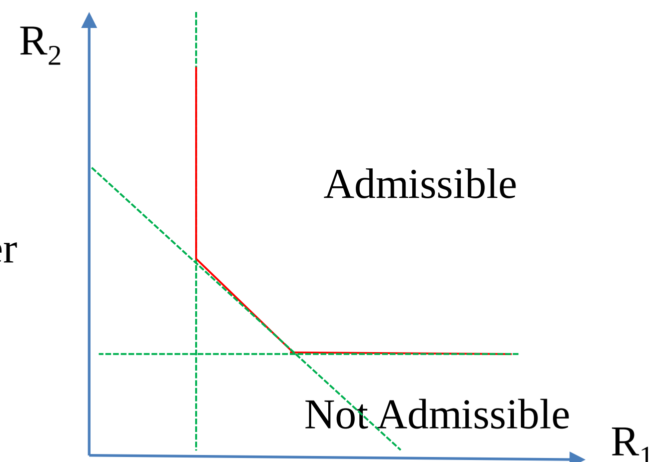
The rate regions for Information flow on Wireless Network Communication

Type II Problem:
admissible Channels coding rates (capacities) given Sources rates



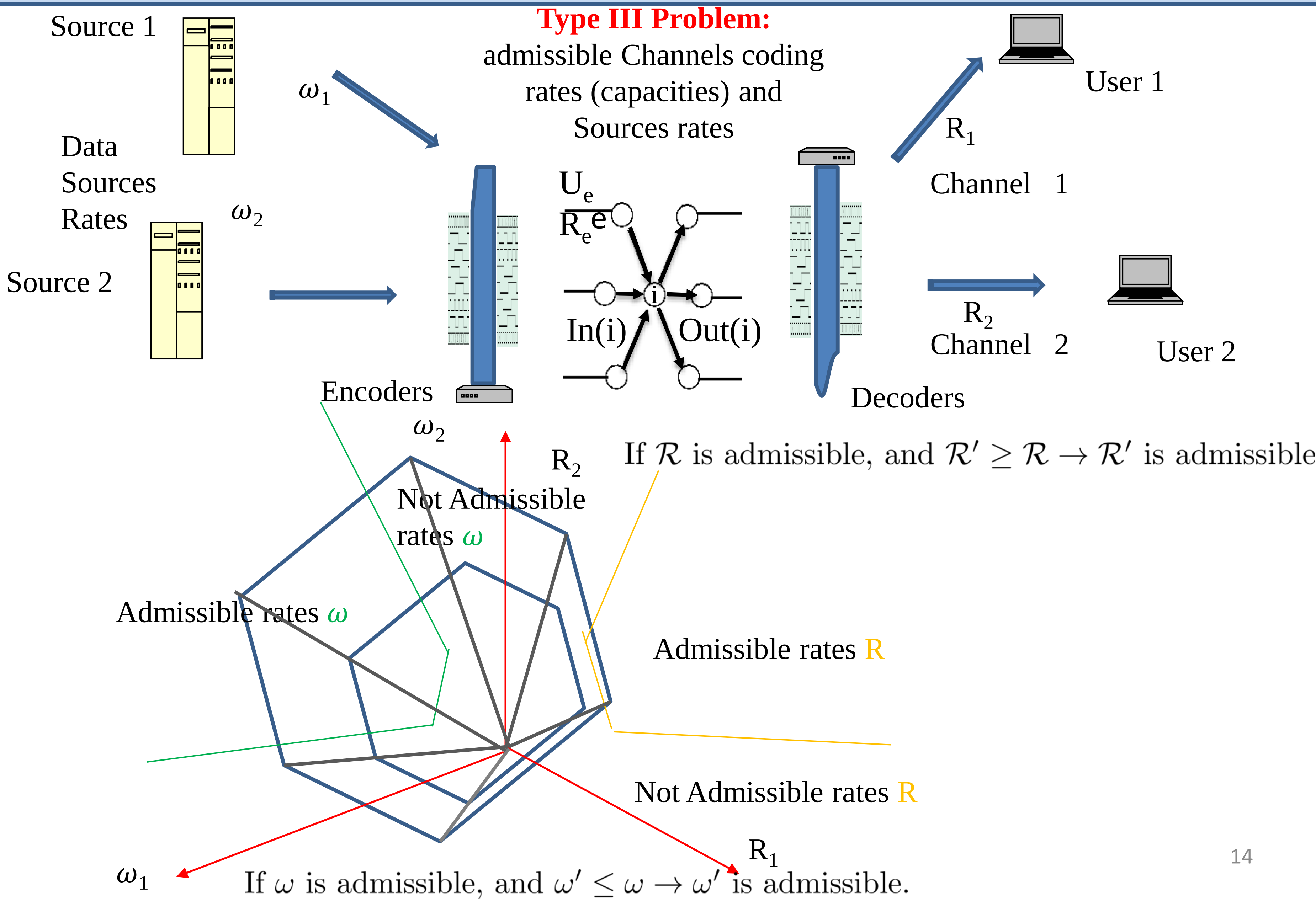
Channel Capacities

C. R. Region **R** Optimizing over all Codes



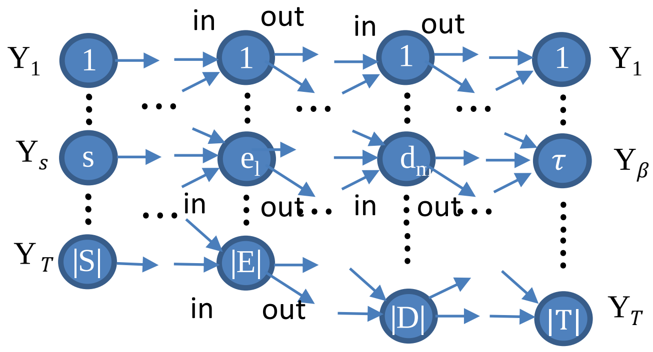
$$\text{If } \mathcal{R} \text{ is admissible, and } \mathcal{R}' \geq \mathcal{R} \rightarrow \mathcal{R}' \text{ is admissible}$$

The rate regions for Information flow on Wireless Network Communication



Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



Shannon Information measures

Shannon Entropy

- Measure of the uncertainty in a r.v.
- Average unpredictability in a r.v.,
- Information content

$$h_A = H(X_A) = -\sum_{X_A} p_{X_A}(X_A) \log p_{X_A}(X_A)$$

absolute limit on best possible
lossless encoding of any communication

Joint S. Entropy $$h_{12} = H(X_1, X_2) = -\sum_{X_1 X_2} p_{X_1 X_2}(X_1, X_2) \log p_{X_1 X_2}(X_1, X_2)$$

Conditional S. Entropy $$h_{2|1} = H(X_2|X_1) = -\sum_{X_1 X_2} p_{X_1 X_2}(X_1, X_2) \log p_{X_2|X_1}(X_2|X_1)$$

Mutual Information $$I(X_1, X_2) = \sum_{X_1 X_2} p_{X_1 X_2}(X_1, X_2) \log \frac{p_{X_1 X_2}(X_1, X2)}{p_{X_1}(X_1) p_{X_2}(X_2)}$$

2. Rate Region Implicit Characterization by Yan, Yeung & Zhang.

Joint entropies are vectors.

$$h_A = H(X_A) = -\sum_{X_A} p_{X_A}(X_A) \log p_{X_A}(X_A)$$

$$\bar{h} = (h_A | A \subseteq \mathcal{N}) \in \mathbb{R}^{2^N - 1}$$

$$\mathcal{N} = 2 : \bar{h} = (h_1, h_2, h_{12})$$

$$\mathcal{N} = 3 : \bar{h} = (h_1, h_2, h_{12}, h_3, h_{13}, h_{23}, h_{123})$$

2. Rate Region Implicit Characterization by Yan, Yeung & Zhang.

Consider

$Y_s, s \in S$
$U_e, e \in E$

$\mathcal{N} = \{Y_s; U_e\}$
$\mathcal{P}_{\mathcal{N}} = 2^{\mathcal{N}} \backslash \{\emptyset\}$

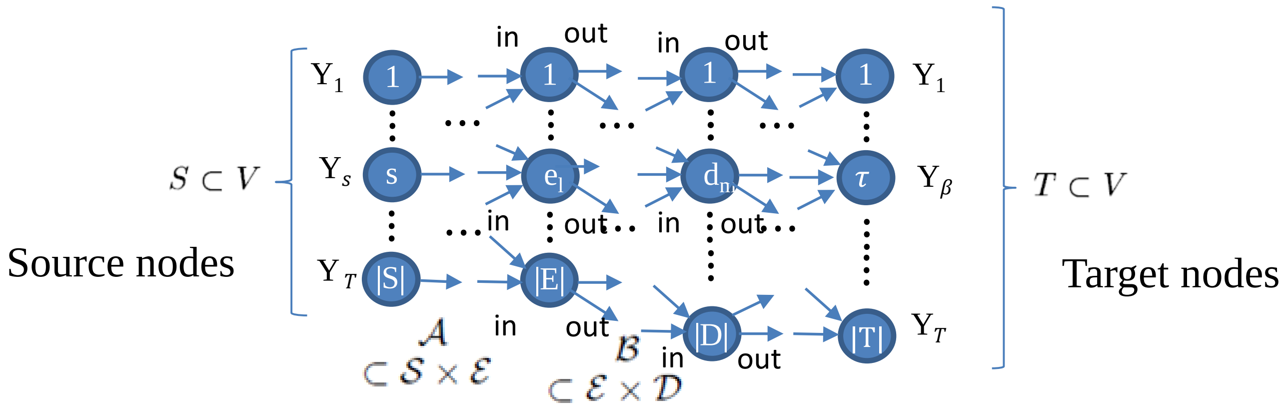
$h = (h_A : A \in \mathcal{P}_{\mathcal{N}}\}$
h is entropic if $h_A = H(X_A), A \in \mathcal{P}_{\mathcal{N}}$
$\mathcal{H}_{\mathcal{N}} = \mathbb{R}^{2^{\mathcal{N}}-1}$

$$\Gamma^*_{\mathcal{N}} = \{h \in \mathcal{H}_{\mathcal{N}} : h \text{ is entropic}\}$$

Entropic Region

Yan X., Yeung R.W., Zhang Z. An implicit Characterization of the Achievable rate region for acyclic multisource multisink network conding, IEEE transactions on Information Theory, Vol 58, No. 9 2012

$G = (V, E)$



Entropic Subregions

$$\mathcal{L}_0 = \{h \in \mathcal{H}_\mathcal{N} : h_{Y_s} \geq \omega_s \;, \; s \in S\}$$

$$\mathcal{L}_1 = \{h \in \mathcal{H}_\mathcal{N} : h_{Y_S} = \textstyle\sum_{s \in S} h_{Y_s}\}$$ → C_1

$$\mathcal{L}_2 = \left\{h \in \mathcal{H}_\mathcal{N} : h_{U_{Out(s)}|Y_s} = 0, s \in S\right\}$$ → C_2

$$\mathcal{L}_3 = \left\{h \in \mathcal{H}_\mathcal{N} : h_{U_{Out(i)}|U_{In(i)}} = 0, i \in V \setminus (S \cup T)\right\}$$ → C_3

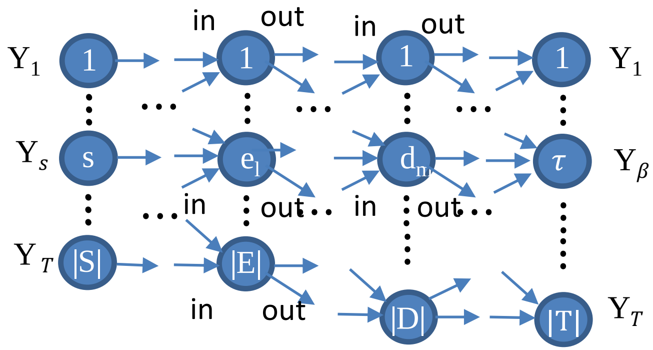
$$\mathcal{L}_4 = \{h \in \mathcal{H}_\mathcal{N} : h_{U_e} \leq R_e, e \in E\}$$ → C_4

$$\mathcal{L}_5 = \left\{h \in \mathcal{H}_\mathcal{N} : h_{Y_{\beta(t)}|U_{In(t)}} = 0, t \in T\right\}$$ → C_5

Yan X., Yeung R.W., Zhang Z. An implicit Characterization of the Achievable rate region for acyclic multisource multisink network conding, IEEE transactions on Information Theory, Vol 58, No. 9 2012

Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



2. Yan, Yeung & Zhang Exact Characterizing of Rate Region.

Some important conventions

$$\text{For } \mathbf{h} \in \mathcal{H}_{\mathcal{N}} \longrightarrow \mathbf{h}_{Y_{\mathcal{S}}} = (h_{Y_s} : s \in \mathcal{S})$$
$$\text{For } \mathbf{h} \in \mathcal{H}_{\mathcal{N}} \longrightarrow \mathbf{h}_{U_{\mathcal{E}}} = (h_{U_e} : e \in \mathcal{E})$$

$$\text{For } \mathcal{B} \subset \mathcal{H}_{\mathcal{N}} \longrightarrow \text{proj}_{Y_{\mathcal{S}}}(\mathcal{B}) = \{\mathbf{h}_{Y_{\mathcal{S}}} : \mathbf{h} \in \mathcal{B}\}$$
$$\text{For } \mathcal{A} \subset \mathcal{H}_{\mathcal{N}} \longrightarrow \text{proj}_{U_E}(\mathcal{A}) = \{\mathbf{h}_{U_{\mathcal{E}}} : \mathbf{h} \in \mathcal{A}\}$$

$$\text{If } \mathbf{h}' \in \mathcal{B} \rightarrow \Lambda(\mathcal{B}) = \{\mathbf{h} \in \mathcal{H}_{\mathcal{N}} : 0 \leq \mathbf{h} \leq \mathbf{h}'\}$$

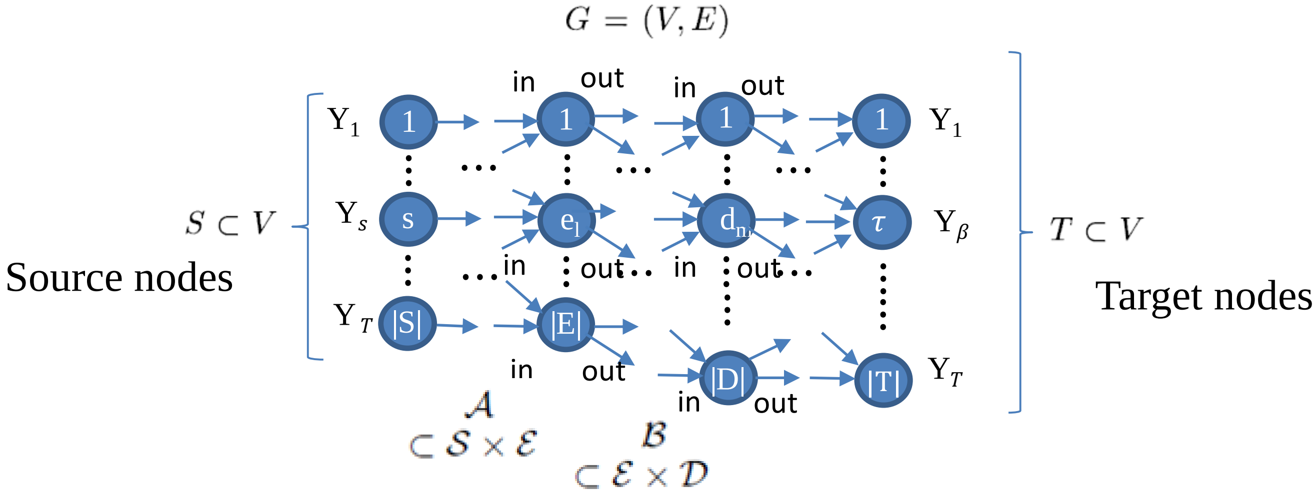
$$\text{Ex}(\mathcal{B}) = \{\mathbf{h} \in \mathcal{H}_{\mathcal{N}} : \mathbf{h} \geq \mathbf{h}', \mathbf{h}' \in \mathcal{B}\}$$

Let $\text{con}(\mathcal{B})$ be the convex hull of $\mathcal{B}$.
Let $\overline{\mathcal{B}}$ be the closure of $\mathcal{B}$.

$$\mathcal{W}' = \Lambda\left(\text{proj}_{Y_{\mathcal{S}}}\left(\overline{\text{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{123})} \cap \mathcal{L}_4 \cap \mathcal{L}_5\right)\right)$$
$$\mathcal{R}' = \overline{\text{Ex}\left(\text{proj}_{U_{\mathcal{E}}}\left(\text{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{0123})\right)\right)}$$

Yan X., Yeung R.W., Zhang Z. An implicit Characterization of the Achievable rate region for acyclic multisource multisink network conding, IEEE transactions on Information Theory, Vol 58. No. 9 2012

2. Yan, Yeung & Zhang Exact Characterizing of Rate Region.



Exact Rate Region expressions

$$\mathcal{W}' = \Lambda(\mathrm{proj}_{Y_S}(\overline{\mathrm{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{123})} \cap \mathcal{L}_4 \cap \mathcal{L}_5))$$

$$\mathcal{R}' = \mathcal{R} \subset \mathcal{R}' = \overline{\mathrm{Ex}\left(\mathrm{proj}_{U_\mathcal{E}}\left(\mathrm{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{0123}\right)\right)}$$

Theorem I

Theorem I

$\mathcal{W} = \mathcal{W}'$ ⟺ $\mathcal{R} = \mathcal{R}'$

Converse Theorem I

Converse Theorem I

$$\mathcal{W} \subset \Lambda(\mathrm{proj}_{Y_S}(\overline{\mathrm{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{123})} \cap \mathcal{L}_4 \cap \mathcal{L}_5)) = \mathcal{W}'$$

$$\mathcal{R} \subset \mathcal{R}' = \overline{\mathrm{Ex}\left(\mathrm{proj}_{U_\mathcal{E}}\left(\mathrm{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{0123}\right)\right)}$$

Yan X., Yeung R.W., Zhang Z. An implicit Characterization of the Achievable rate region for acyclic multisource multisink network conding, IEEE transactions on Information Theory, Vol 58, No. 9 2012

Calculation of rate regions which are projections of the entropic vectors region .

.

Information Th.

Solving Maxflow or
Distributed Storage Systems

For any liner objective we require
to determine the Rate region.

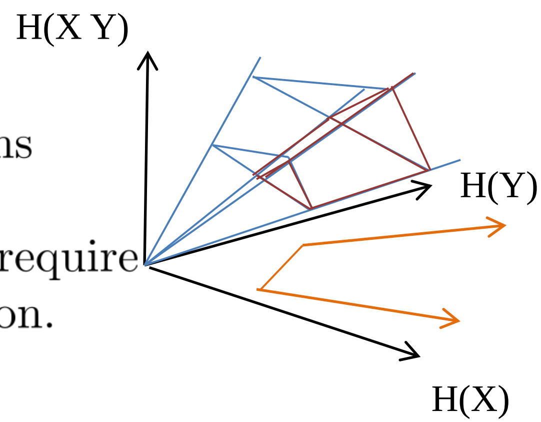
Binary Matroids Entropic
region Inner bound
⇓

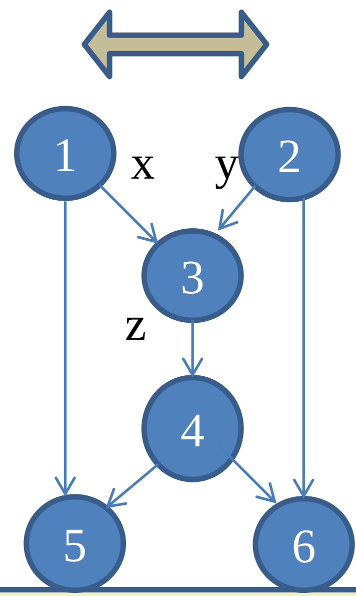
Characterize Rate region
in terms of Entropic Region s.t.

⇓

Binary linear codes suffice with
$\oplus$ as the most complex operation

Projection





Network Codes Solutions

Codes Achieving Inf. Rate Region
at extreme points
Network Topology
⇓

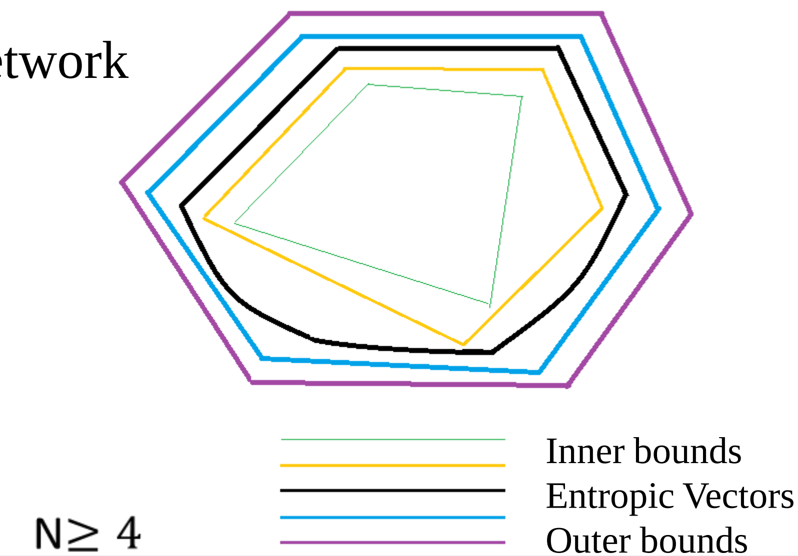
Sources Indep.Constr.
Encoder Constr. on S.Var. & Aux.Var.
Decoder Constr. on Aux.Var & Rec.Var.
Add rate inequalities
Project over variables of interest s.t.

⇓

Efficiently use of Channels
for higher throughput
Minimum efficient Backup Support
for Distributed Storage system

Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



3. The Polymatroid Axioms

Given a r.v. X_n, finite Alphabet,

$$h : \alpha \subseteq \{1, 2, \ldots, n\} = \mathcal{N} \to \mathbb{R}^+$$

Each $X_\alpha \to h(X_\alpha) \in \mathbb{R}^{\mathcal{P}(\mathcal{N})}$

$\forall h$ we have:

1. $h(\emptyset) = 0$
2. $h(i) \leq h(j) \ \forall i \subseteq j \subseteq \mathcal{N}$
3. $h(i) + h(j) \geq h(i \cup j) + h(i \cap j) \ \forall i, j \subseteq \mathcal{N}$

$$\Gamma_N = \{h | h : 2^E \to Z^+\}$$

Recent Progresses in Characterising Information Inequalities, Terence Chan, Entropy 2011, 13, 379-401
doi:10.3390/e13020379

4. Entropic Region, its Closure and Polymatroid functions region.

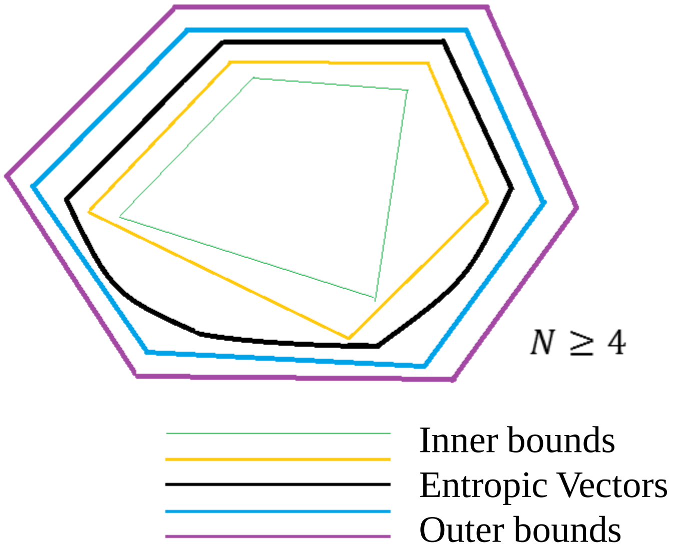
The Entropic Region & its Closure

$$\overline{\Gamma_2^*} = \Gamma_2 \text{ Polyhedral C.}$$

$$\overline{\Gamma_3^*} = \Gamma_3 \text{ Polyhedral C.}$$

$$\overline{\Gamma_4^*} \neq \Gamma_4 \text{ Convex C.}$$

$$\overline{\Gamma_N^*} \neq \Gamma_N \text{ Unknown.}$$



$$\overline{\Gamma_2^*} = \Gamma_2 \text{ Th. Z. Zhang \& R.Yeung 1997}$$

$$\overline{\Gamma_3^*} = \Gamma_3 \text{ Th. Z. Zhang \& R.Yeung 1997}$$

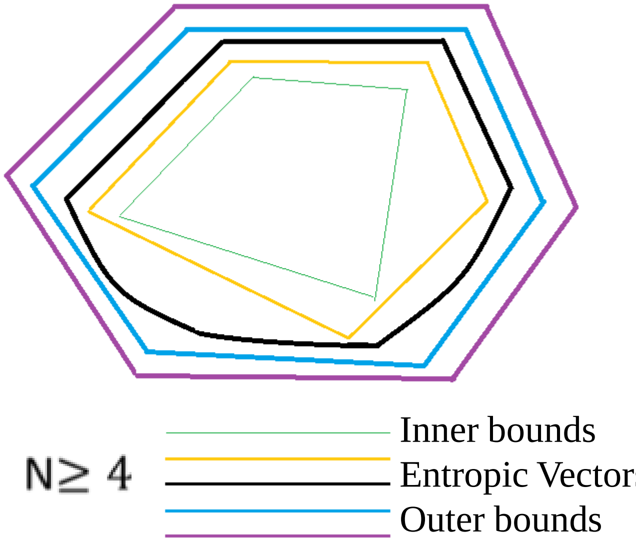
$$\overline{\Gamma_4^*} \neq \Gamma_4 \text{ Th. Z. Zhang \& R.Yeung 1998}$$

$$\text{For } N \geq 4,\ \overline{\Gamma_N^*} \neq \Gamma_N \text{ Th. Z. Zhang \& R.Yeung 1998}$$

A non Shannon type Conditional Inequality of information Quantities, Zhen Zhang, Raymond Yeung. IEEE trans. Inf. Th. Vol 43 No 6, Nov. 1997
On Characterization of Entropy function via Information Inequalities, Zhen Zhang, Raymond Yeung. IEEE trans. Inf. Th. Vol 44 No 4, Jul. 1998

Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bound
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



Entropic Region, its Closure and Properties.

Entropy vector of N variables: Shannon entropy of all possible subset of N variables

Case N<4

Origin is entropic

If a vector $\mathbf{h}$ is entropic, $\alpha\mathbf{h}, \alpha \geq 0$ is also entropic.

Hence, the region is a cone.

Completly determined for $N < 4$, (Polyhedral cone)

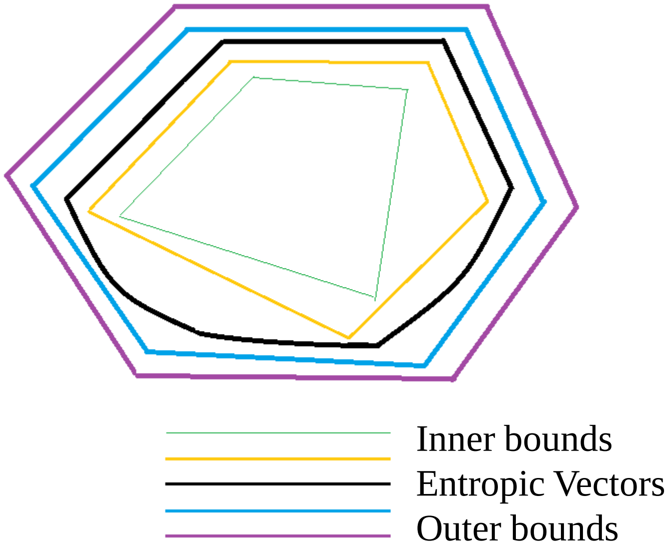
Region of Entropic Vectors

For $N < 4$, the region (or closure) is a polyhedral convex cone.

Not known for $N \geq 4$, non-polyhedra cone,

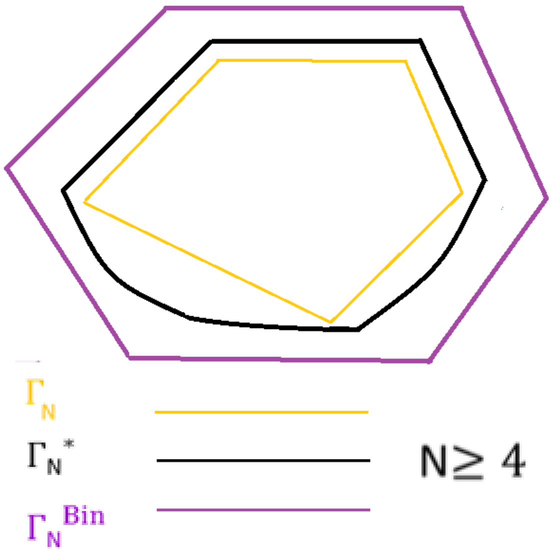
outer bound and inner bound

Case N≥4



Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms, Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



4. Matroid Axioms

(E, r) be a matroid $\to E$ finite set, function $r : 2^E \to Z^+$

r obey Polymatroid Axioms, $\forall \alpha, \beta \subset E$

$$r(\emptyset) = 0$$
$$\alpha \subseteq \beta \to r(\alpha) \leq r(\beta)$$
$$r(\alpha \cup \beta) + r(\alpha \cap \beta) \leq r(\alpha) + r(\beta)$$

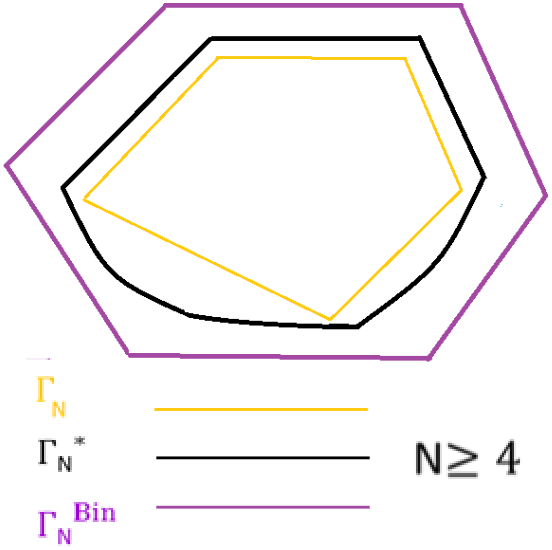
$$\Gamma_N = \{r | r : 2^E \to Z^+\}$$

Integer valued Polymatroids r, s.t. $r(\mathcal{A}) \leq |\mathcal{A}|$ are matroids, $\mathcal{A} \subset E$

Linear representable Matroids are all matroids r s.t. $r(\mathcal{A}) \propto |v|, v \subseteq R^n$ for some $n \in Z^+$

Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms , Matroids, **Representable** & entropic **matroids**, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region

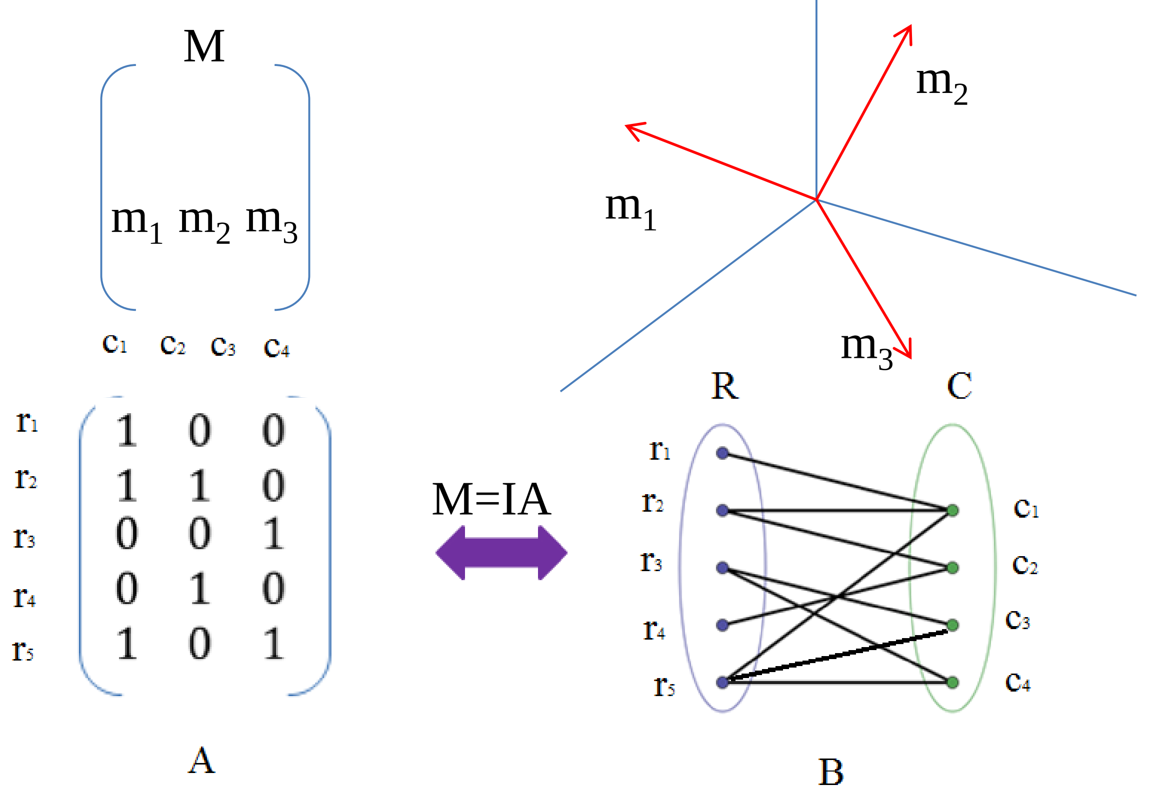


Representable Matroids

M is representable if (E, r) can be rep. by $V \in F^r$

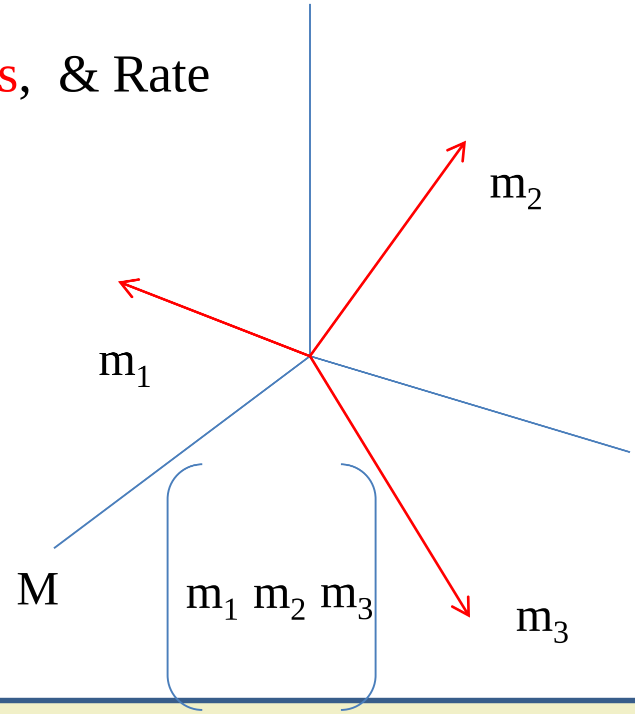
$\exists\, V \in F^r$ and $f : E \to V$ s.t. $r(V) \geq dim f(X)\ \forall X \subseteq E$

if $|E| = N, \exists A \in F^{r \times N}\ s.t. r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y)\ \forall X, Y \in Col(A)$



Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Rate region Shannon inequalities Outer bound
4. Matroid Axioms, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
5. Entropic vectors enumeration: Analytical enumeration of binary linear codes
6. Algorithm to evaluate codes that achieve Network Rate region



Representable Matroids & Entropic Matroids

Not all Entropic Matroid $\Rightarrow$ Rep. Matroid,

but All Rep.Matroid $\Rightarrow$ Entropic Matroid.

If $h \in \Gamma^*$ is rep. $\Rightarrow$ Assoc. Network Prob.has Optimal sol.
$\therefore$, $\exists$ linear Network code over F that achieve rate region.

All Representable Matroids are Entropic Matroids

Given (E, r) Matroid, $|E| = N$, $r(E) = k$ rep. over F_q , $|F| = q$, rep. by $A \in F_q^{k \times N}$ s.t. $\forall B \subseteq E$, $r(B) = rank(A :,_B)$.

Conic hull, Γ_N^q are all Matroid rank functions with N elements, rep. in F_q.
$\Gamma_N^q \subseteq \overline{\Gamma_N^*}$, since any extremal $r \in \Gamma_N^q$ is rep. assoc. to $A \in F^{K \times N}$,

Def. r.v. $(X_1, \ldots, X_N) = uA$, $u \sim U(F_q^k)$, $X_n = \sum_i^k u_i a_{in}$,
$h_B = r(B) \log_2 q, \forall B \subseteq E$; $r(B) = rank(A :,_B)$, all extremal rays of Γ_N^q are entropic, $\Gamma_N^q \subseteq \overline{\Gamma_N^*}$

Presentation Outline

1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds
4. Entropic vectors enumeration: Analytic enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region

$$b(n, \leq r) = \frac{\sum_{(A,\pi) \in GL_r^2 \times S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

A new technique to find Best tied Inner bound for the Region of entropic vectors

For every representable matroid there is an entropic vector.

we want to list isomorphic classes of representable matroids .

how many are needed to list?

we can enumerate them without generating all of them,
(Marcel Wild 1993,) .

An efficient procedure is required, since **the number usually is extremely large.**

Abstract algebra approach can **actually list all of them** (A.Kerber, H.Fripertinger, Laue , Bayreuth University, Germany 1994)

- ✓ **binary linear codes- Abstract Algebra Perspective – Dr. Marcel Wild research.**

1st step: From **counting of orbits** to **averaging fix points.**

- ✓ Groups
- ✓ Cauchy-Frobenius Counting Lemma
- ✓ Orbits enumeration – fix points Average.
- ✓ Groups for binary linear matroid isomorphic classes enumeration .

$$b(n, \leq r) = \frac{\sum_{(A,\pi) \in GL_r^2 \times S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

6. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Cauchy-Frobenius Burnside Counting theorem

Lemma: The orbit-counting theorem,
result in group theory useful in taking account of symmetry
when counting mathematical objects.

$\lrcorner$ G be finite group acts on a set X. For each $g \in G$,
$\lrcorner X_g$ be set $x \in X$ that are fixed by g.
It states that $|G \setminus \setminus X| = \frac{1}{|G|} \sum_{g \in G} |X_g|$

$\therefore$ number of orbits $(\in \mathbb{N}$ or $+\infty) = \bar{x}$ of points fixed by $g \in G$.

Defining groups involved in the enumeration of the isomorphic classes of binary r rank matroids on n elements

To find $b(n,r)$,
consider the group $GL_r^2 \times S_n$,

GL_r^2 general linear group
S_n is the symmetric group on $1, 2, ..., n$.

The group acts on the set of matrices $M := (a_1, a_2, ..., a_n) \in GF(2)^{r \times n}$

$$(A, \pi) * (a_1, ..., a_n) := (Aa_{\pi^{-1}1}, \dots, Aa_{\pi^{-1}n})$$

Permutation group that change the order of the columns , moving columns with their Respective labels.

Non singular matrix
General Linear Group
elementary row Operations (change of basis)

Double Group Action

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

5. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Number of orbits equals the average of fix points

The orbits ${}_{G}(x) \Leftrightarrow$ isomorphism classes of binary matroids of n elements with rank $\leq r$

$$\lrcorner Z(A,\pi) := \{M \in Z : (A,\pi) * M = M\}$$

Main Result of Wild: Using Burnside lemma , number of orbits is

$$b(n, \leq r) = \frac{\sum_{(A,\pi)\in GL_r^2 \times S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

number of orbits = average of fix points.

Also $b(n,r) = b(n, \leq r) - b(n, \leq r-1)$

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

5. Entropic vectors enumeration: Analytical enumeration of binary linear codes

To evaluate $\sum_{(A,\pi)\in GL_r^2\times S_n} |Z_{A,\pi}|$ is difficult, since the so large number of summands.

Hence, equivalently,

$$b(n, \leq r) = \frac{\sum\limits_{(A,\pi)\in GL_r^2\times S_n} \prod\limits_{i=1}^{n} |Y_{A^i}|^{a_i(\pi)}}{|GL^2||S_n|}$$

Instead of matrices $M \in GF(2)^{r\times n}$, consider mappings $f : 1, 2, \ldots, n \to GF(2)^r$.

A ,π act on $X := 1, 2, \ldots, n$ and $Y := GF(2)^r$,through maps f, $Y^X := \{f | f : X \to Y\}$ by

$$(A, \pi) * f := A \circ f \circ \pi^{-1}$$

Y_{A^i} : points fixed by $A^i \in GL_r^2$, s.t. $A^i.M = 1.M = M$

$a_i(\pi)$: $|$ cycles of length $i|$ in the cycle decomposition of $\pi (1 \leq i \leq n)$

Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

5. Entropic vectors enumeration: Analytical enumeration of binary linear codes

- ✓ **Analytical approach for binary linear codes- Abstract Algebra – from Dr. Marcel Wild research.**

2nd step:
Averaging
Sym group fix points from points fixed by a canonical representative of Conjugacy classes Times size of the class.

- ✓ Computing fix points through conjugacy classes.
- ✓ Burnside Lemma expression in terms of Conjugation

$$b(n, \leq r) = \frac{\sum_{(A,\pi) in GL_r^2 \times S_n} \prod_{i=1}^{n} |Y_{A^i}|^{a_i(\pi)}}{|GL^2||S_n|}$$

5. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Averaging

Matrices fixed in Y by elementary row operations under the action of exponential linear group H^x

and

Matrices fixed on column labels permutations on X under the action of symmetric subgroup G

through

Product of

fix points induced by canonical representatives of equivalences classes of

Conjugation of the two groups

Times

Cardinalities of the Sets of all such Conjugacy equivalence classes of groups G and H^x

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

Conjugacy classes of Matrices

$\lrcorner D$ is conjugacy class $\in GL_r^2$.

$D^i = \{A^i | A \in D\}$ is also a conjugacy class.

$D_1, D_2, \ldots, D_{k(r)}$, conjugacy classes of GL_r^2 enumerated in arbitrary order.

$\forall 1 \leq \mu \leq k(r)$ and $\forall 1 \leq i \leq n$,
D_μ , is a similar class of invertible matrices
$fix(\mu, i)$ be common number of fixpoints $\forall A^i \in D^i_\mu$,
the number of eigenvectors (including zero)
$\forall A \in D_\mu$.

5. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Summarizing these concepts,
the orbits counting expression found from Burnside Lemma
we get:

Sym classes Cardinality group conjugacy

GL_2 group conjugacy classes Cardinality

Type of permutation is associated with a Sym group Conjugacy class, parametrized by λ.

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu,i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Points fixed by representative of GL_2 group Conjugacy Class parametrized by μ

λ parametrize the conjugacy classes C_λ of the group S_n.

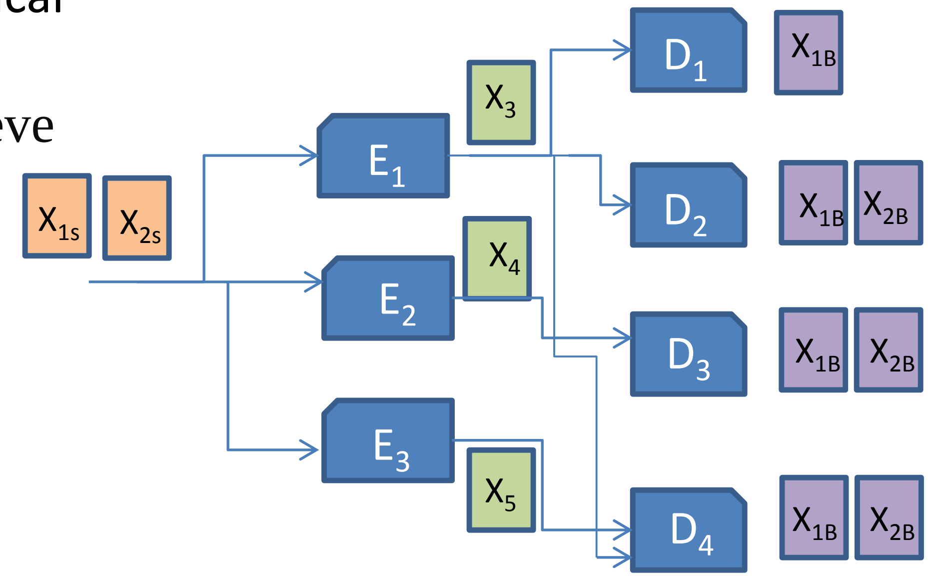
To Average points fixed under the double group Action
It suffices to count
the fix points of just only one representative of
Their conjugacy classes
and multiply the result by
the cardinality of sets of conjugacy classes.

Considering Conjugacy classes and number of points fixed by representatives of them.

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

Presentation Outline

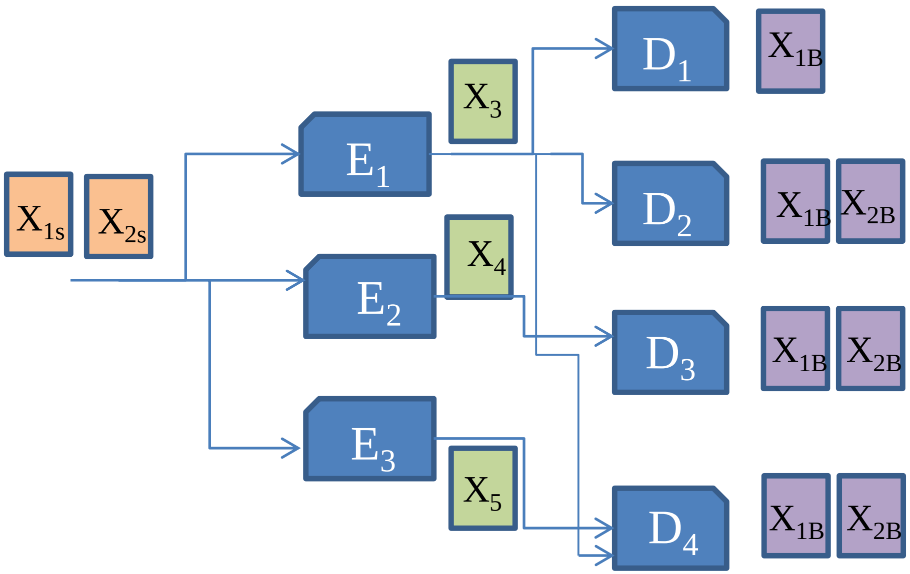
1. Motivation : Acyclic Multisource Multisink Network coding Region of capabilities: Max flow framework & Data Storage Scenario
2. Rate Region Implicit & exact Characterization
3. Polymatroid axioms & Matroids & Rate region Entropic Vectors Inner bounds, Representable matroids are Entropic
4. Entropic vectors enumeration: Analytical enumeration of binary linear codes
5. Algorithm to evaluate codes that achieve Network Rate region



$N \geq 4$

6.Algorithm to Evaluate Codes that Achieve Rate region of a Given Network

Variables and Constraints from Network Topology



Source Variables

$X_{1s} = [X^1{}_1, X^1{}_2]$

$X_{2s} = [X^2{}_1, X^2{}_2, X^2{}_3, X^2{}_4]$

Auxiliary Variables

$X_3 = U_1 = [X^3{}_1, X^3{}_2, X^3{}_3]$

$X_4 = U_2 = [X^4{}_1, X^4{}_2, X^4{}_3]$

$X_5 = U_3 = [X^5{}_1, X^5{}_2, X^5{}_3]$

Encoder Constraints

$h_{12}=h_{123}$

$h_{12}=h_{124}$

$h_{12}=h_{125}$

Decoder Constraints

$h_3=h_{13}$

$h_{34}=h_{1234}$

$h_{35}=h_{1235}$

$h_{45}=h_{1245}$

Demanded Variables

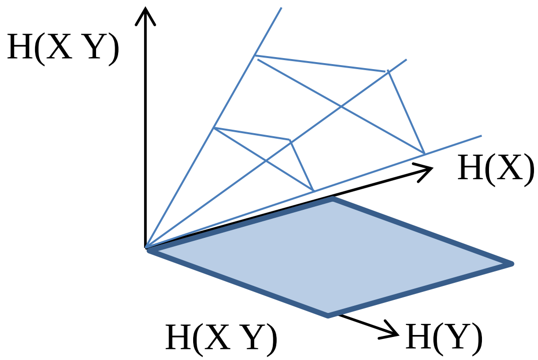
$X_{1B} = [X^1{}_1, X^1{}_2]$

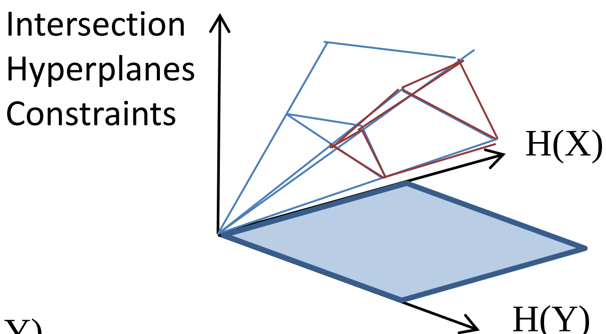
$X_{2B} = [X^2{}_1, X^2{}_2, X^2{}_3, X^2{}_4]$

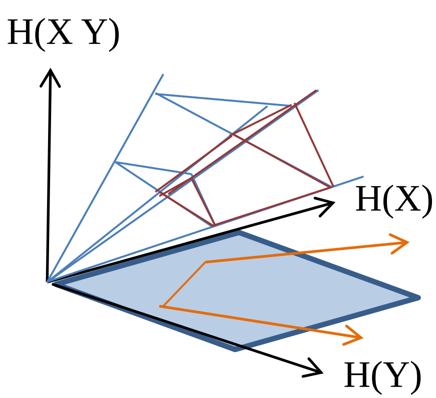
Var X_1 and X_2 must be full rank

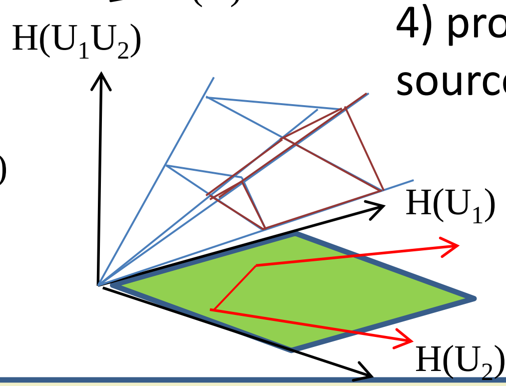
Solution: How to find rate region of a Network using Entropic Vectors.

Algorithm to evaluate codes that achieve Network Rate region.









- ✓ The algorithm is based on the exact characterization of the Rate region using the region of entropic vectors.

- ✓ The fundamental steps are :

1) getting entropics vectors data,
2) intersecting it with hyperplanes constraints and finally
3) adding rate variables
4) projecting the result downward to Network source variables/ capacities plane.

Solution: How to find rate region of a Network using Entropic Vectors.

Algorithm to evaluate codes that achieve Network Rate region.

1. We extract entropies from the non isomorphic binary linear codes for all possible values we can assign to source and auxiliary variables from each of the codes looping for different possible bits per variable.
2. The constraints depend on the Topology of the Network, they represent hyperplanes that cut it.
3. We need to add the rates that we are interested into optimize.
4. Final we need to project into the corresponding rates plane to find the polymatroids that inequalities representation of the rate region.

intersect $\overline{\Gamma_N}^*$ with

$$h_{U_{out(s)}|Y_s} = 0, \quad s \in S$$

$$h_{U_{out(i)}|U_{in(i)}} = 0, \quad i \in V(S \cup T)$$

$$h_{Y_{\beta(t)}|U_{in(t)}} = 0, \quad t \in T$$

$$h_{Y_S} = \sum_{s \in S} h_{Y_s}$$

$$h_{Y_s} \ge \omega_s \,, \quad s \in S$$

or

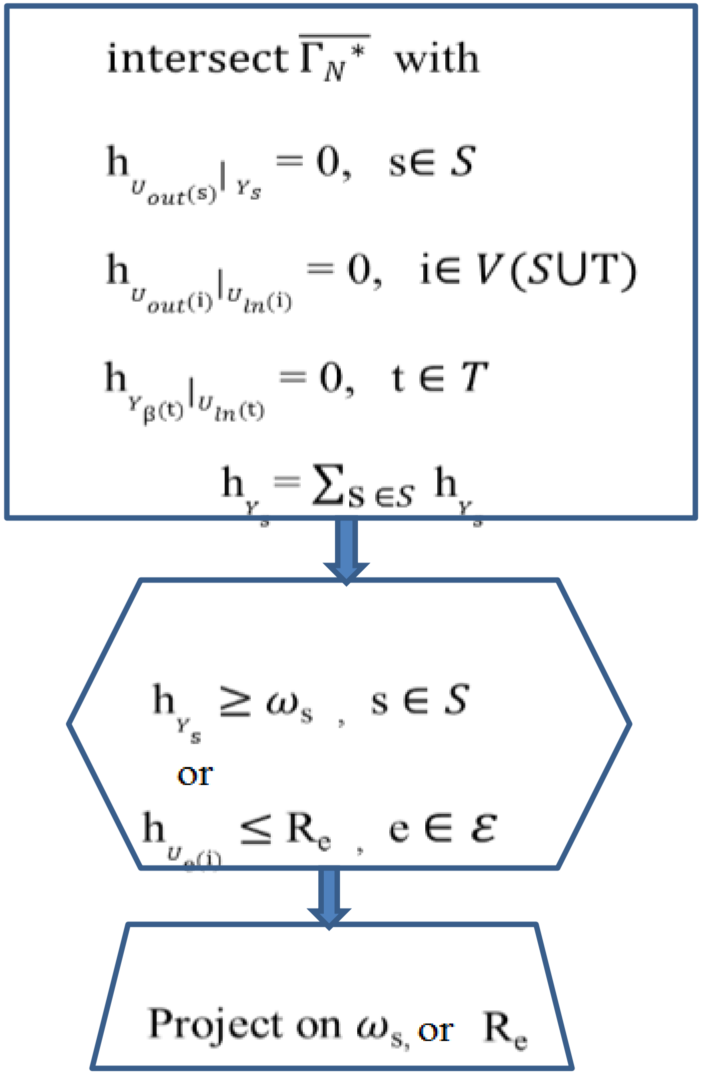
$$h_{U_{e(i)}} \le R_e \,, \quad e \in \mathcal{E}$$

Project on ω_s, or R_e

Solution: How to find rate region of a Network using Entropic Vectors.

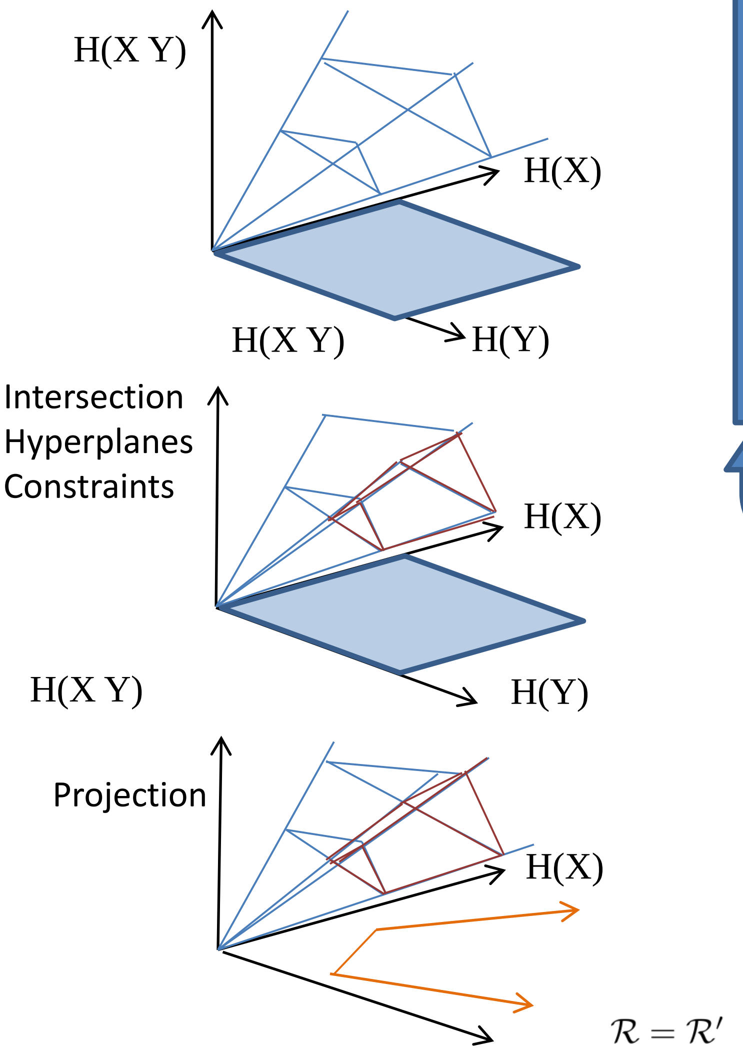
Algorithm to evaluate codes that achieve Network Rate region.

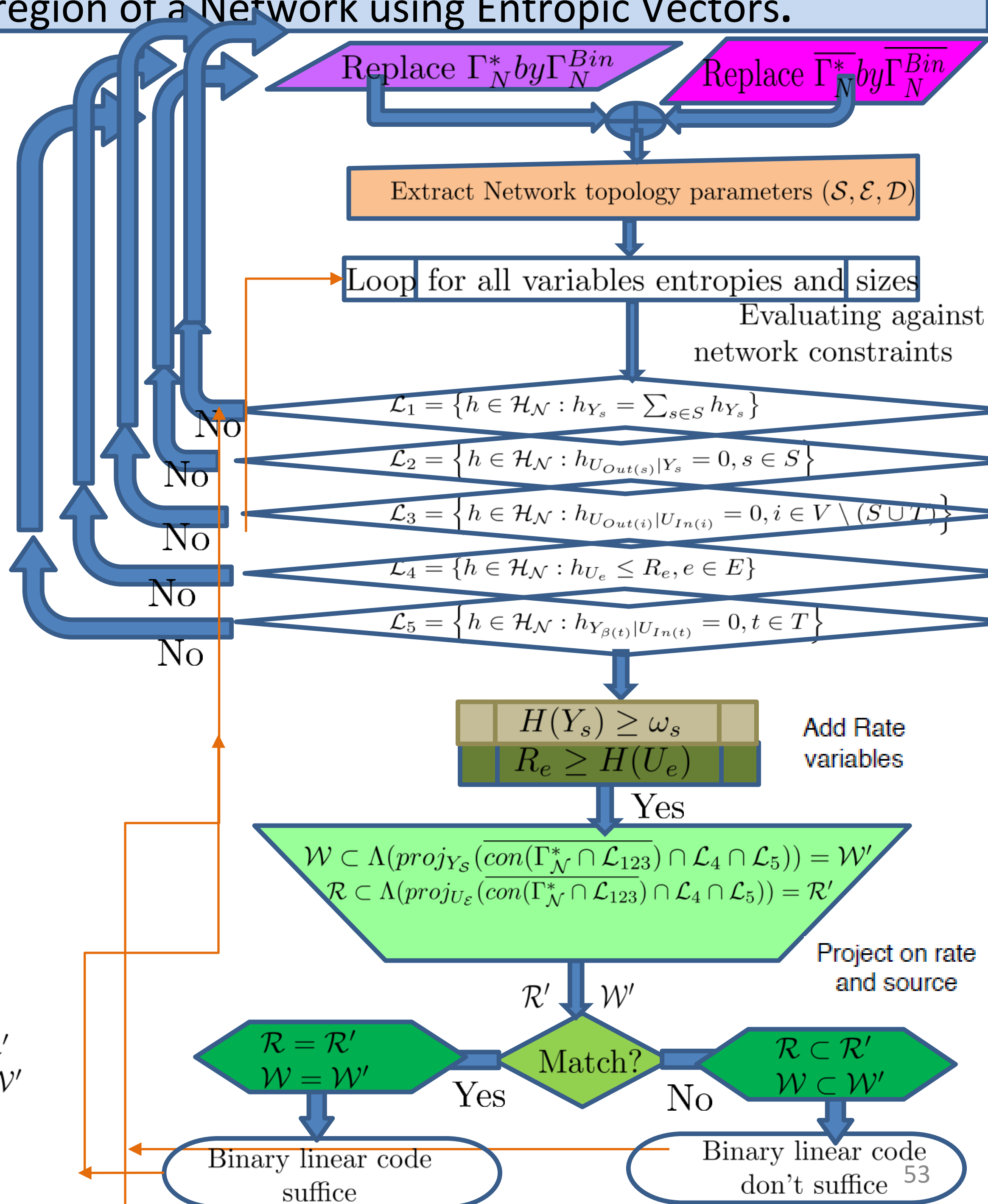
- ✓ Exploring every ray to see if it is included.
- ✓ Looping for different combinations of entropies and bits per variable ,
- ✓ Every time we need to eliminate Redundancies w.r.t to other variables.
- ✓ Evaluate encoding and decoding constraints for all possible entropies and bits,
- ✓ considering that the source variables must be linearly independent.
- ✓ Our strategy is to find at least one binary linear code satisfying constraints, per each selection of entropies and bits , per ray, this will determine the form of the convex cone of the region of entropic vectors.



Solution: How to find rate region of a Network using Entropic Vectors.

Practical Algorithm compute
General Rate region





Solution: How to find rate region of a Network using Entropic Vectors.

Algorithm Description:

Combinations of all variable sizes are computed between 1 and A_n−number of variables −1,

(No variable can have zero bits and when the variable is at its maximum size, bits must be reserved for the remaining other variables).

The inputs of the functions are:

1. Combinations structure called comb,
2. The ray that is at that particular stage being explored
3. The code it is checked to be possibly achieving the rate region.

Solution: How to find rate region of a Network using Entropic Vectors**.**

A ray is defined as a tuple of entropies (source and auxiliary variables), is a vector.

For each variable, the program loop from its entropy to $A_n - \sum_{v \in Notyetselected} h_v - \sum_{u \in Alreadyselected} bits_u$,

where A_n is the number of columns, code length.

Size of variable can't be less than its entropy and can't be so large such that one or more of the other variables become of size smaller than their respective entropies.

Solution: How to find rate region of a Network using Entropic Vectors**.**

Given a variable size, loop through all combinations that are stored in the structure comb of that same size.

Along every loop redundancies are checked w.r.t. the variables previously fixed and the entropies are checked against network constraints.

If conditions are not satisfied, then move to next possible combination, otherwise it is moved to the next variable.

A constrained permutation approach is applied, if we find that for some entropies assigned to some variables there are constraints not matched , we don't continue exploring on permutations that are derived from that assignation of entropies. We prune that branch from the tree of permutations.

6.Algorithm to Evaluate Codes that Achieve Rate region of a Given Network

X   Y U_1 U_2 U_3

10 11 12 13 14 15 1 5 9 2 3 6 4 7 8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	1	0	0	0	0
1	1	0	0	1	1	0	0	0	0	0	1	0	0	0
1	0	1	0	1	0	1	0	0	0	0	0	1	0	0
0	1	0	1	0	1	1	0	0	0	0	0	0	1	0
1	0	1	1	1	1	0	1	0	0	0	0	0	0	1

X   Y U_1 U_2 U_3

10 11 12 13 14 15 2 6 9 1 3 5 4 7 8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	1	0	0	0	0
1	1	0	0	1	1	0	0	0	0	0	1	0	0	0
1	0	1	0	1	0	1	0	0	0	0	0	1	0	0
0	1	0	1	0	1	1	0	0	0	0	0	0	1	0
0	0	1	1	1	0	0	1	0	0	0	0	0	0	1

X   Y U_1 U_2 U_3

10 15 11 12 13 14 3 8 9 1 4 5 2 6 7

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	1	0	0	0	0
1	1	0	0	1	1	0	0	0	0	0	1	0	0	0
1	0	1	0	1	0	1	0	0	0	0	0	1	0	0
0	1	0	1	0	1	1	0	0	0	0	0	0	1	0
1	1	1	0	1	0	0	1	0	0	0	0	0	0	1

3 codes that were tested and achieved a ray (2 4 3 3 3) of the rate region .

6.Algorithm to Evaluate Codes that Achieve Rate region of a Given Network

RRrep3
V-representation
begin
5 6 integer
0 1 1 1 1 2
0 1 1 1 1 3
0 1 1 1 1 4
0 2 4 3 3 3
0 1 2 2 1 4
end

RRrep3Rd
*row 2 was redundant and removed
V-representation
begin
4 6 rational
0 1 1 1 1 2
0 1 1 1 1 4
0 2 4 3 3 3
0 1 2 2 1 4
end
*Input had 5 rows and 6 columns: 1 row(s) redundant*redund:lrslib v.4.3 2012.6.1(32bit,lrsmp.h) max digits=8/100*0.000u 0.015s 4324Kb 1147 flts 0 swaps 0 blks-in 0 blks-out

6.Algorithm to Evaluate Codes that Achieve Rate region of a Given Network

RRrep3Rd
H-representation
linearity 1 1
begin
***** 6 rational
0 -1 -1 1 1 0
0 4 -5 5 0 -1
0 -1 -1 2 0 0
0 0 3 -5 0 1
0 0 1 -1 0 0
end
*Totals: facets=4 bases=1 linearities=1
facets+linearities=5*lrs:lrslib v.4.3
2012.6.1(32bit,lrsmp.h) max
digits=8/100*0.015u 0.000s 4324Kb 1147 flts 0
swaps 0 blks-in 0 blks-out

6.Algorithm to Evaluate Codes that Achieve Rate region of a Given Network

```
RRrep3Rd
H-representation
begin
11 9 rational
0 -1 -1  1  1  0  0 0 0
0  4 -5  5  0 -1  0 0 0
0 -1 -1  2  0  0  0 0 0
0  0  3 -5  0  1  0 0 0
0  0  1 -1  0  0  0 0 0
0  0  0 -1  0  0  1 0 0
0  0  0  0 -1  0  0 1 0
0  0  0  0  0  -1  0 0 1
0  0  0  0  0  0  1 0 0
0  0  0  0  0  0  0 1 0
0  0  0  0  0  0  0 0 1
```

$X_1 X_2 U_1 U_2 U_3 R_1 R_2 R_3$

```
end
*Totals: facets=4 bases=1 linearities=1
facets+linearities=5*lrs:lrslib v.4.3
2012.6.1(32bit,lrsmp.h) max digits=8/100*0.015u
0.000s 4324Kb 1147 flts 0 swaps 0 blks-in 0 blks-out
```

Conclusions

Integrating the research carried out in Network coding of Z.Zheung, X.Yan and R.Yeung,
under the information theory most recent progresses reported by T.Chan
with the methods developed for the enumeration construction of binary linear codes of M.Wild and R.Laue,
a suitable method of finding the rate region for
acyclic multisink multisources Networks was proposed.

The method is based on the use of results of analytic enumeration of binary linear codes
carried out with Computational Group theory and
an algorithm designed to test them against all the constraints of a network using constrained permutation.

Conclusions

The exact characterization of the Network coding Rate region w.r.t
the entropic region (under bounding this one)
was used to develop a General strategy of its computation.
based on representable matroids.

In particular, this is an approach that can be used to find
solution of two importantnet Network coding problems
as the Max flow and the Distributive storage.

Appendix. Entropic Region, its Closure and Properties.
(Convex Hull)

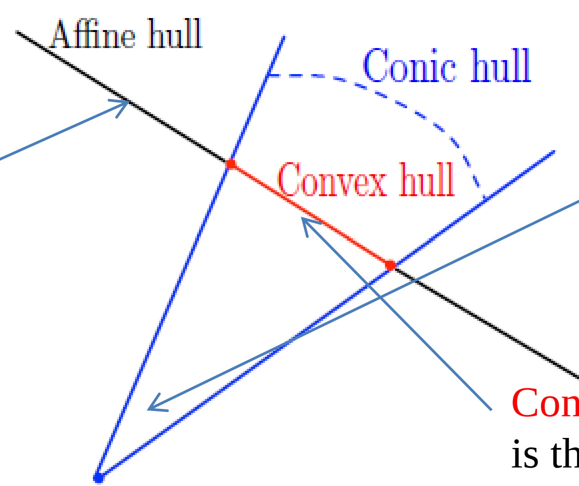
Entropic region Closure is a Polyhedral Cone

The **affine hull** of S : $$\operatorname{aff}(S) = \left\{ \sum_{i=1}^{k} \alpha_i x_i \,\middle|\, k > 0,\ x_i \in S,\ \alpha_i \in \mathbb{R},\ \sum_{i=1}^{k} \alpha_i = 1 \right\}.$$

The **convex hull of S** : $$\operatorname{Conv}(S) = \left\{ \sum_{i=1}^{|S|} \alpha_i x_i \,\middle|\, (\forall i : \alpha_i \geq 0) \wedge \sum_{i=1}^{|S|} \alpha_i = 1 \right\}.$$

The **conic hull of S**: $$\operatorname{cone}(S) = \left\{ \sum_{i=1}^{k} \alpha_i x_i \,\middle|\, x_i \in S,\ \alpha_i \in \mathbb{R},\ \alpha_i \geq 0, i, k = 1, 2, \ldots \right\}.$$

Conic hull of 2 pts., union of all rays, emanating from origin, intersecting convex hull



Affine hull of 2 pts.
is the line through them

Convex hull of 2 pts .
is the line segment between them

Appendix. Matroid Axioms, Representable & entropic matroids, & Rate region Entropic Vectors Inner bounds

Entropic Region includes all Valid Entropic vectors

$$\mathcal{H}_{\mathcal{N}} = \mathbb{R}^{2^N - 1}$$

$$\Gamma_N^* = \{h \in \mathcal{H}_{\mathcal{N}} : \text{h is entropic}\}$$

$\overline{\Gamma_N^*}$ is a convex cone.

Not All the Euclidean Space is Entropic

Recent Progresses in Characterising Information Inequalities, Terence Chan, Entropy 2011, 13, 379-401
doi:10.3390/e13020379

2. Rate Region Implicit Characterization by Yan & Yeung.

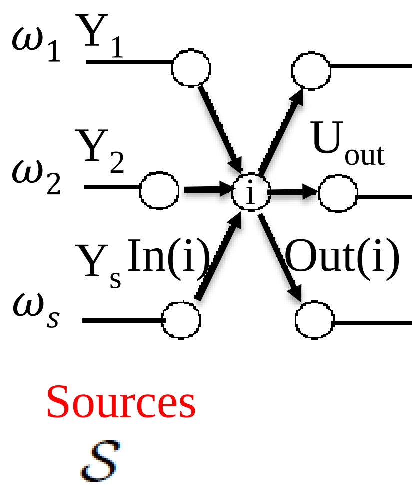
Network sources Rate Region

Source rate

$H(Y_s) \geq \omega_s$

Sources Independence

$H(Y_S) = \sum_{s \in S} H(Y_s)$



Source Encoding

$H(U_{out(s)}|Y_s) = 0$

$$\mathcal{W} = \{\text{ W: W is admissible, where W} = \{\omega_s, s \in \mathcal{S}\}\}$$

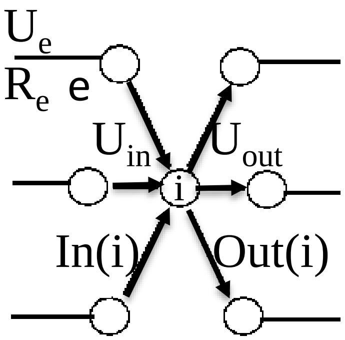
Admissible Rate Region

Admissible Rate Vectors

Network coding Rate Region

Channels encoding rates
vs
entropies of Aux.Var.

$$\mathcal{R}_e \geq H(U_e)$$
$$e \in \mathcal{E}$$



Int. nodes

encoding constraints

$$H(U_{out(i)}|U_{In(i)}) = 0$$
$$i \in \mathcal{V} \backslash (\mathcal{S} \cup \mathcal{T})$$

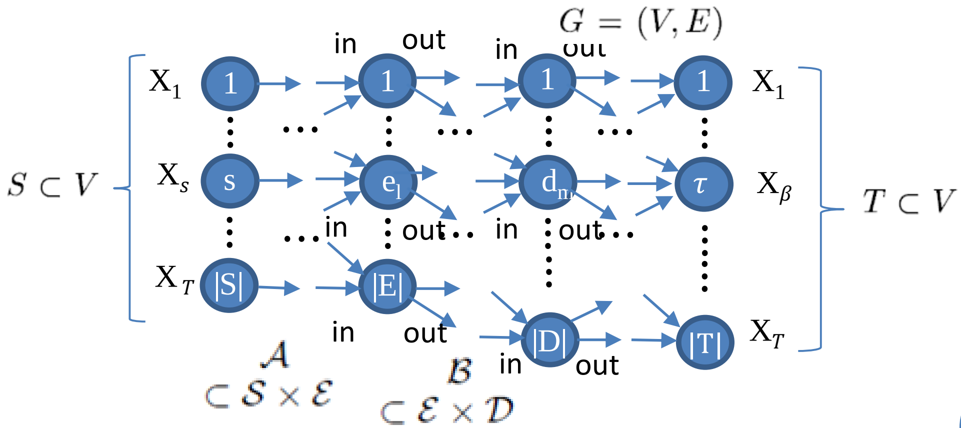
$$\mathcal{R} = \{ \text{ R: R is admissible, where R } = \{R_e, e \in \mathcal{R}\}\}$$

Admissible Rate Region

Admissible Rate Vectors

Information Theory & Network Coding , Chapter 2, Raymond Yeung., Springer 2008, 2002. ISBN 978-0-387-79233-0

2. Rate Region Implicit Characterization by Yan, Yeung & Zhang.



$(n, (\eta_e : e \in \mathcal{E}, (\tau_s : s \in \mathcal{S}))$ block code of length n is:

Sources Encoding function

$s \in \mathcal{S}, e \in Out(s)$

$$k_e\colon\ \mathcal{X}_s = \{1, 2, \ldots, 2^{n\tau_s}\} \to \{0, 1, \ldots, \eta_e - 1\}$$

Nodes Encoding function

$e \in Out(i),\ i \in V \backslash (\mathcal{S} \cup \mathcal{T})$

$$k_e\colon\ \prod_{d \in In(i)} \{0, 1, \ldots, \eta_d - 1\} \to \{0, 1, \ldots, \eta_e - 1\}$$

Decoding function

$t \in \mathcal{T}$

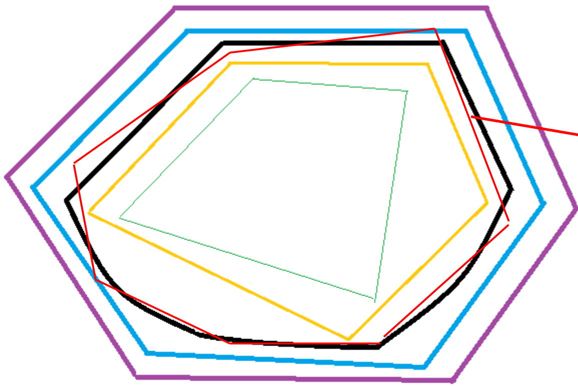
$$g_t\colon\ \prod_{d \in In(i)} \{0, 1, \ldots, \eta_d - 1\} \to \mathcal{X}_{\beta(t)}$$

X_s information r.v. $s \in \mathcal{S}$
taking values in $\mathcal{X}_s = \{1, 2, ..., [2^{n\tau_s}]\}$
τ_s inf. s.r.
η_e inf. n.r.
At $t \in \mathcal{T}$
$X_\beta(t), \beta(t) \subset \mathcal{S}$

Yan X., Yeung R.W., Zhang Z. An implicit Characterization of the Achievable rate region for acyclic multisource multisink network conding, IEEE transactions on Information Theory, Vol 58, No. 9 2012

Why not other Outer and inner bounds instead ?

$$\text{Ingletons Inequality },\ \lrcorner\ M(E,I,\rho) \text{ be matroid },\ \rho \text{ rank function}$$
$$\forall X_1, X_2, X_3, X_4 \subseteq E,$$
$$\rho(X1) + \rho(X_2) + \rho(X_1 \cup X_2 \cup X_3) + \rho(X_1 \cup X_2 \cup X_4) + \rho(X_3 \cup X_4)$$
$$\leq \rho(X_1 \cup X_2) + \rho(X_1 \cup X_3) + \rho(X_1 \cup X_4) + \rho(X_2 \cup X_3) + \rho(X_2 \cup X_4)$$



Aubrey William Ingleton, 1969

(Ingleton + Shannon inequalities) K=4 , best tied inner bound, for N>4 can overlap Entropic Region

$N \geqslant 4$

Entropic Region

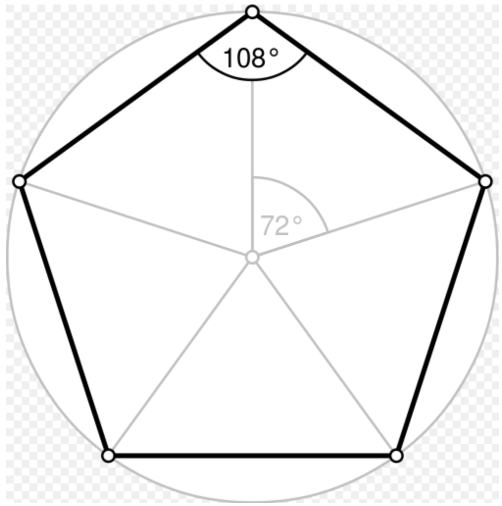
- Inner bound (Ingleton inequalities)
- Better Inner (Binary linear codes)
- Better Outer bound (Non Shannon inequalities)
- Outer bound (Shannon inequalities)

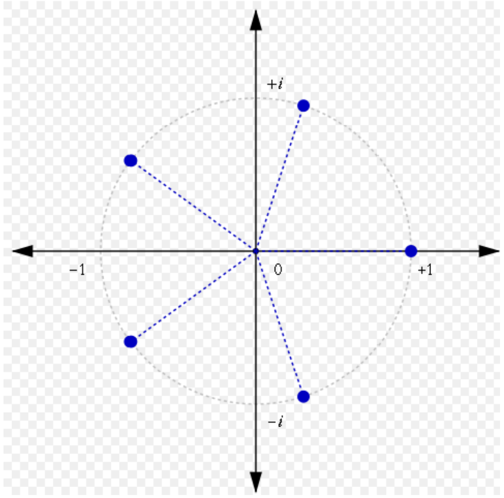
$$\text{First discovered Non-Shannon-Type Information Inequality:}$$
$$2I(X_3;X_4) \leq I(X_1;X_2) + I(X_1;X_3,X_4) + 3I(X_3;X_4|X_1) + I(X_3;X_4|X_2)$$

Z. Zhang & R. Yeung 1997

A non Shannon type Conditional Inequality of information Quantities, Zhen Zhang, Raymond Yeung. IEEE transactions of Information Theory Vol 43 No 6, November 1997

Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes (Isomorphic Objects in symmetries)





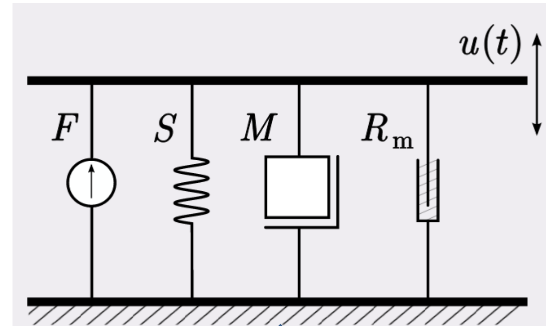
The group of fifth roots of unity under multiplication is isomorphic to the group of rotations of the regular pentagon under composition.

So, in listing codes, w.r.t. performance for testing them in a network, we must avoid double counting the ones that produce exactly the same effect. We need to test non-isomorphic codes.

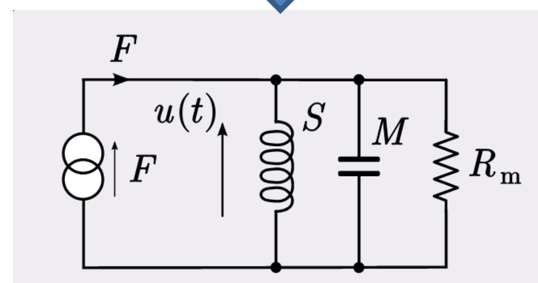
Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes (Isomorphic classes)

In classifying systems we need to avoid to double count the ones that are system analog models.

mechanical simple resonator

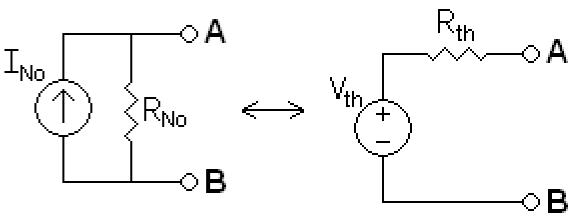


Isomophic systems



electrical analogy

$R_{th} = R_{no}$; $V_{th} = I_{no} R_{no}$; $\frac{V_{th}}{R_{th}} = I_{no}$



Norton's theorem and Thévenin's theorem offers an *isomorphism class* of electrical circuits..

Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes

- ✓ **binary linear codes- Abstract Algebra Perspective – Dr. Marcel Wild research.**

1st step: From **counting of orbits** to **averaging fix points.**

- ✓ Groups
- ✓ Cauchy-Frobenius Counting Lemma
- ✓ Set Transversal under a group action
- ✓ group Action set permutation representation.
- ✓ Orbits Equivalence classes
- ✓ Group action orbit space
- ✓ Group action Partitions of finite sets.
- ✓ Orbits enumeration – fix points Average.
- ✓ Groups for binary linear matroid isomorphic classes enumeration.

$$b(n, \leq r) = \frac{\sum\limits_{(A,\pi)\in GL_r^2 \times S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Group conceptualization

Group

Set — Binary Operation

$$(G, .)$$

Closure $\forall a,\text{b}\in G,\ a.b \in G$

Associativity $\forall a,\text{b},\text{c}\in G,\ (a.b).c = a.(b.c)$

Identity element $\exists e \in G, \text{ s.t. } \forall a \in G, e.a = a.e = a$

Inverse element $\forall a \in G,\ \exists b \in G \text{ s.t. } a.b = b.a = e, e \in G$

Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Transversal of orbits and the partition determined by a group action of a finite set.

Transversal

⌟ C be collection of sets, transversal $F \subset C$, F contains exactly one $x \in c \subset C$.
if $\forall i$,j $c_i \cap c_j \neq \emptyset$, $c_i, c_j \in C$, each $f \in F$ corresponds to exactly one $c \in C$

Transversals and Partitions

As $x \sim {}_G x' \leftrightarrow \exists g \in G$ s,t. $x' = gx$,
$\therefore$ F yields a set partition of X, dissected into pairwise disjoint and nonempty subsets $G(t), t \in F$

$$X = \bigcup_{t \in F} G(t)$$

$$\therefore G \backslash\backslash X := \{G(t) | t \in F\}$$

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes

Given an element $x \in X$

Orbit of an element: $Gx := \{ g.x | g \in G\}$

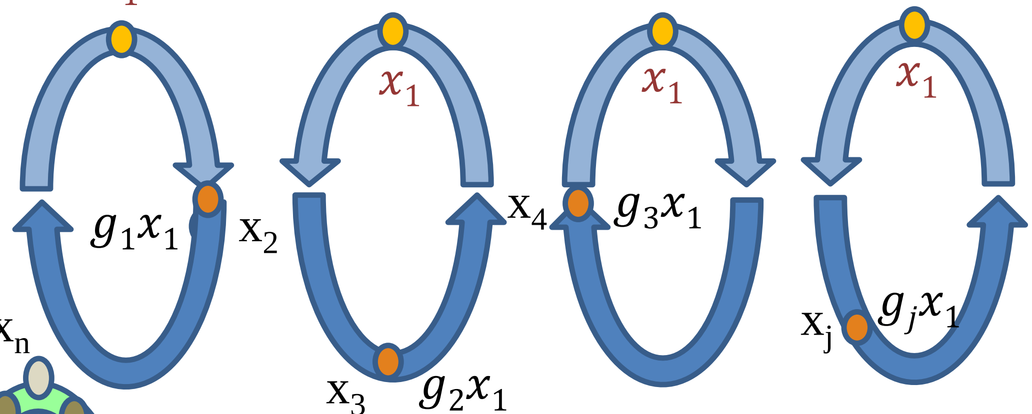
Orbit Space: $G\backslash\backslash X := \{Gx \mid x \in X\}$

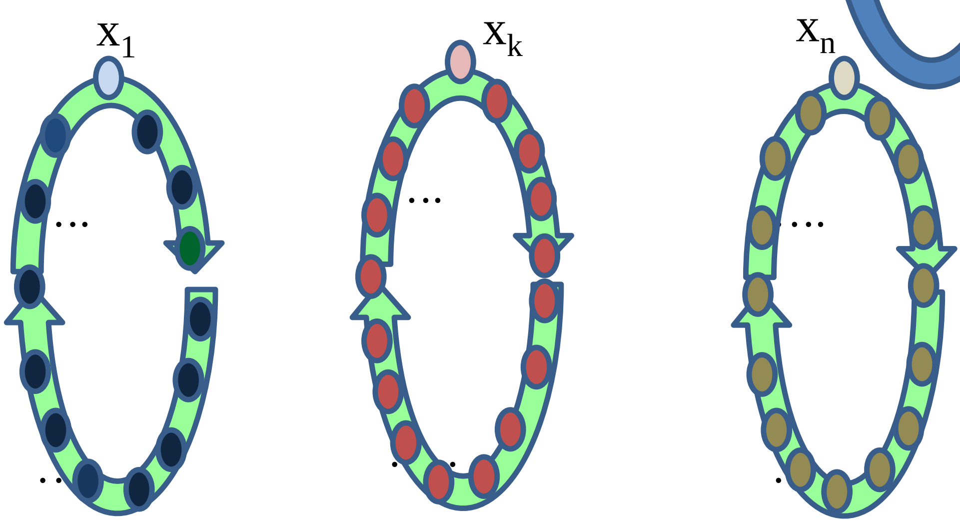
Orbits in X under the Action of group G

Orbits $\Leftrightarrow$ Permutations

$Gx = \{g_k x_i = xj \mid x_i, x_j \in X, g \in G\}$

$g_1 x \; U \; g_2 x \; U \; \ldots U \; g_n x = Gx$





$Gx_1 \; U \ldots \quad Gx_k \; U \ldots \quad U \; Gx_n = G\backslash\backslash X$

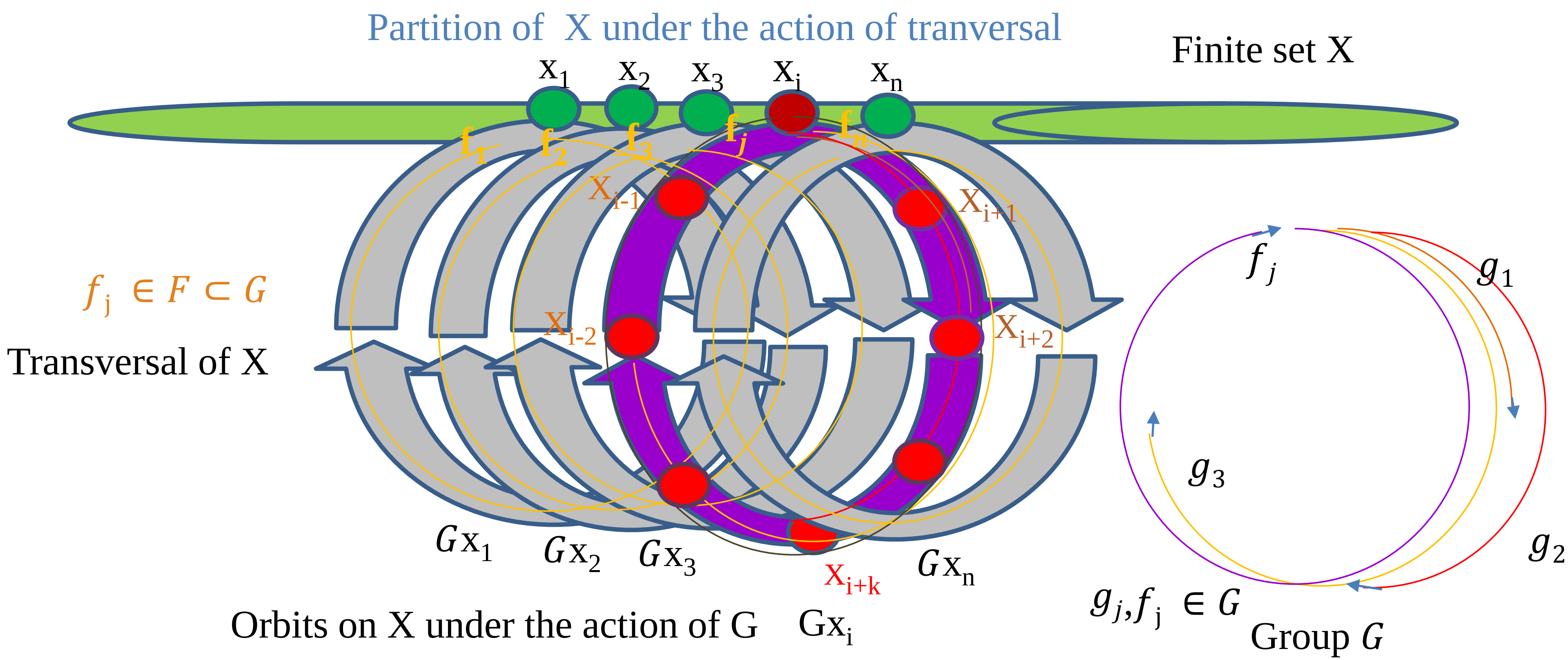
Orbit Space of a Group Action

The orbit space or quotient of the action of a group over a finite set

Appendix. Entropic vectors enumeration: Analytical enumeration of binary linear codes

A group acting on a finite set determines a partition on it.

The set of orbits of points x ∈ X, under action of G, form a partition of X



Group Actions and Partitions

Each set partition of $X \to$ action of a certain group on X.

$\lrcorner X_i$,where $i \in I$, an index set,

A partition of pairwise disjoint, nonempty sets of X.

$\exists \ {}_{S_x}X$ and has orbits X_i,

$$\bigoplus_i S_{x_i} := \{\pi \in S_x | \forall i \in I : \pi X_i = X_i\}$$

Lemma: ${}_G x \equiv$ a permutation representation of G on X and

$\to$ a set partition of X into orbits.

$\Leftarrow$, each set partition of X $\leftrightarrow$ to an action of certain subgroup of of S_x which has blocks of the partition as its orbits.

An Action of a group in a finite set equivalent to a permutation representation of the set.

Conjugacy Classes of a Group

Conjugacy

group may be partitioned into conjugacy classes;

Suppose G a group. $a, b \in G$ are called conjugate if $\exists g \in G$ with $gag^{-1} = b$, $\Leftrightarrow a \sim b$

, it partitions G into equivalence classes.

$\Rightarrow$ every $g \in G$ belongs to precisely one conjugacy class, classes $Cl(a) = Cl(b)$ iff $a = g^{-1}bg$, and disjoint otherwise.

Conjugacyclassof S_n group

The conjugacy class containing $a \in G$ is

$$Cl(a) = \{gag^{-1} : g \in G\}$$

Conjugacy classes of the symmetric group of permutations.

Conjugacy Classes of The Product of Two Groups

Theorem

⌟ G, H be groups, with sets of conjugacy classes C_G and C_H

respectively. $\therefore$, if $C_{G\times H} = \{A \times B : A \in C_G, B \in C_H\}$

In our problem the total number of conjugacy classes is

$|C_\lambda||D_\mu|$

Main Program Run_Testing_Code

Section 1: Import Data from Binary linear Codes Enumeration Construction.

Import JSON file containing non-isomorphic binary linear codes using **JsonLab *Matlab*** package

Section 2: Browsing File of Imported Codes

Code_types structure to be tested is loaded to be iterated using a For-loop.
A code from the structure to be tested is uploaded in the **variable Code_names**
Code_names is declared as to be binary array.

Main Program Run_Testing_Code

Section 3: Generating possible choices for Variables

Run **Create_combinations function** to return all possible variable candidates

Section 4: Testing Code to Achieve Rate Region

Run **Testing_code** function to test the code against constraints
If **Code** achieves rate region **Testing_code** returns successful permutation
If **Code** does not achieve rate region **Testing_code** returns 0.

Section 5 Archiving Codes that achieve Network Rate Region

Successful permutations are archived in the ***Matlab*** structure **all_types.**
Code_types(code_type).Code_names(code_name).code archives codes that achieve Network rate region.
Code_types(code_type).Code_names(code_name).partition archives successful permutation partition.

Function Create_combinations

Arguments

✓15 Columns binary linear **Code**

Value Returned

✓Combinations of 2 columns out of 6 in Array C,
✓Combinations of 4 columns out of 6 in Array D,
✓Combinations of 3 columns out of 9 in Array E.

General Algorithm

✓ Use **choosenk** ***Matlab*** function to compute combinations in C, D, E.
✓ Index columns of **Code** from combinations of C, D, E by vectorization.
✓ Compute entropy of **Code** columns for each combination in C, D, E.

Appendix .Algorithm to Evaluate Codes that Achieve Rate region of a Given Network

Function Testingcode

Arguments

- ✓ Combination Array of 3 out of 15,
- ✓ Combination Array of 4 out of 15,
- ✓ Combination Array of 2 out of 15,
- ✓ Binary linear code to be tested.

Value Returned

- ✓ A permutation of column vectors that match all the constraints.
- ✓ Control is sent back to main program, **Run_Testing_Code**.

General Architecture

- ✓ **5 Nested for-loops**, one for each of the 2 source variables & 3 auxiliary ones
- ✓ **Succession of If-statements** nested in the loops to evaluate the constraints.

Function Testingcode

Variable candidates

- ✓ Fix source variables from the identity matrix, to assure linear independence.
- ✓ 3 Auxiliary variables from remaining bits of the original binary linear code.

Selecting candidates

- ✓ Variable candidates are checked against **Permute** to prevent redundancy
- ✓ Add selected variables to **Permute**
- ✓ **Permute** stores current permutation tree branch

Constrained permutation tree pruning

- ✓ Entropy constraints are checked before a branch is added to **Permute**
- ✓ **Permute** indexes **Code** by vectorization to compute ranks.
- ✓ When a branch fails, **Permute** is reset.

Appendix: Implicit Characterization of rate region from Entropic Vectors.

Network Rate Region from Entropic Region

- ✓ Compute Entropic Region , then its Closure
- ✓ Entropic region Closure intersected Network Topology equalities
- ✓ Projected onto a series of Capacities Variables

It solves fundamental limits, boundaries of the set.

1. Its unknown if they actually can be computed.
2. We want to substitute something that is outside of the set for something that is inside of it.
3. After intersection and projection we get 2 things which match.
4. The answer is in the sandwich in between the two.

$$\Upsilon(A) = \{\boldsymbol{r} \in \mathbb{R}^{|\mathcal{E}|} : \quad \boldsymbol{r} \geq \boldsymbol{r}' \text{ for some } \boldsymbol{r}' \in A\}$$

$$\mathcal{R}_{\text{in}} \subset \mathcal{R} \subset \mathcal{R}_{\text{out}}$$

$$\mathcal{R}_{\text{in}} = \overline{\Upsilon(\text{proj}_{(h_{Z_l}, l \in \mathcal{E})}(\Gamma_N^* \cap C_1 \cap C_2 \cap C_3 \cap C_4))}.$$

$$\mathcal{R}_{\text{out}} = \Upsilon(\text{proj}_{(h_{Z_l}, l \in \mathcal{E})}(\overline{\Gamma}_N^* \cap C_1 \cap C_2 \cap C_3 \cap \overline{C_4}))$$

Raymond W. Yeung, Information Theory and Network Coding. Springer, 2008.

2. Yan, Yeung & Zhang Implicit Characterizing of Rate Region.

$$\Upsilon(A) = \{\boldsymbol{r} \in \mathbb{R}^{|\mathcal{E}|}: \quad \boldsymbol{r} \geq \boldsymbol{r}' \text{ for some } \boldsymbol{r}' \in A\}$$

$$\mathcal{R}_{\text{in}} = \overline{\Upsilon(\text{proj}_{(h_{Z_l},\, l \in \mathcal{E})}(\Gamma_N^* \cap C_1 \cap C_2 \cap C_3 \cap C_4))}.$$

$$\mathcal{R}_{\text{out}} = \Upsilon(\text{proj}_{(h_{Z_l},\, l \in \mathcal{E})}(\overline{\Gamma}_N^* \cap C_1 \cap C_2 \cap C_3 \cap \overline{C_4}))$$

$$\mathcal{R}_{\text{in}} \subset \mathcal{R} \subset \mathcal{R}_{\text{out}}$$

Yan X., Yeung R.W., Zhang Z. An implicit Characterization of the Achievable rate region for acyclic multisource multisink network conding, IEEE transactions on Information Theory, Vol 58, No. 9 2012

Appendix: Rate Region Implicit Characterization by Yan, Yeung & Zhang.

implicit Rate Region expressions

$\Upsilon(A) = \{\boldsymbol{r} \in \mathbb{R}^{|\mathcal{E}|}: \ \boldsymbol{r} \geq \boldsymbol{r}' \text{ for some } \boldsymbol{r}' \in A\}$ ⟷ $\Lambda(\mathcal{B}) = \{\mathbf{h} \in \mathcal{H}_{\mathcal{N}} : 0 \leq \mathbf{h} \leq \mathbf{h}'\} \quad \mathbf{h}' \in \mathcal{B}$

$\mathcal{R}_{\text{out}} = \Upsilon(\text{proj}_{(h_{Z_l}, l \in \mathcal{E})}(\overline{\Gamma}^*_N \cap C_1 \cap C_2 \cap C_3 \cap \overline{C_4}))$ ⟷ $\mathcal{R}_{out} = \Lambda\left(\text{proj}_{Y_S}\left(\overline{\Gamma}^*_N \cap \mathcal{L}_{123} \cap \mathcal{L}_4 \cap \mathcal{L}_5\right)\right)$

$\mathcal{R}_{\text{in}} = \overline{\Upsilon(\text{proj}_{(h_{Z_l}, l \in \mathcal{E})}(\Gamma^*_N \cap C_1 \cap C_2 \cap C_3 \cap C_4))}.$ ⟷ $\mathcal{R}' = \Lambda\left(\text{proj}_{Y_S}\left(\overline{\text{con}(\Gamma^*_{\mathcal{N}} \cap \mathcal{L}_{123})} \cap \mathcal{L}_4 \cap \mathcal{L}_5\right)\right)$

$\mathcal{R}_{in} = \overline{\text{con}}(\mathcal{R}')$

$\mathcal{R}' \subset \mathcal{R}_{out}$

$\mathcal{R}_{\text{in}} \subset \mathcal{R} \subset \mathcal{R}_{\text{out}}$

$\boldsymbol{R} = (R_l, l \in \mathcal{E})$

Appendix: Implicit Characterization of rate region from Entropic Vectors.

Fundamental limits in terms of Entropic Region .

Finding Network codes capacities

Unknown set - Entropic region ,

Use outer bound, and inner bound,

tie them

∃ known ways to calculate outer bound.

Vectors on Shannon outer bounds are rank functions of matroids.

We want the ones for which there is some associated matrix

$$\boldsymbol{r} \in \Gamma_N \cap \mathbb{Z}^{2^N-1},\ r(\mathcal{A}) \leq |\mathcal{A}|$$

$$\boldsymbol{r} \in \Gamma_N \cap \mathbb{Z}^{2^N-1} \text{ s.t. } \exists \mathbf{A} \in GF(q)^{M \times N} \Rightarrow r(\mathcal{A}) = \text{rank}(\mathbf{A}_{:,\mathcal{A}})$$

All of them are entropic, so they are an inner bound. .

Enumerating representable linear binary matroids gives an inner bound

Raymond W. Yeung, Information Theory and Network Coding. Springer, 2008.

Appendix. Shannon Entropy, Joint Entropies and Shannon Inequalities

Basic Shannon Inequalities

Def. $I(X_1;X_2|X_3) = \sum_{X_1X_2X_3} p_{X_1X_2X_3}(X_1,X_2,X_3)\log\frac{p_{X_1,X_2|X_3}(X_1,X_2|X_3)}{p_{X_1|X_3}(X_1|X_3)p_{X_2|X_3}(X_2|X_3)}$

Basic Inequalities: $\forall\alpha,\beta,\gamma\subset N_n=\{1,\ldots,n\}, I(X_\alpha;X_\beta|X_\gamma)\geq 0$

Information Theory & Network Coding , Chapter 2 pg 17,26 , Raymond Yeung., Springer 2008, 2002.
ISBN 978-0-387-79233-0

Information Inequalities

Inf. Expr.:
$\forall X, Y, Z$ r.v. is $\sum_{X,Y,Z} C_i H(X,Y) + D_j H(X|Z) + E_k H(Y|Z)$

$\lrcorner f$ be an inf. expr.

Given c a constant, $f \geq c$ is an inf. ineq.

$f = c$ is an inf. id.

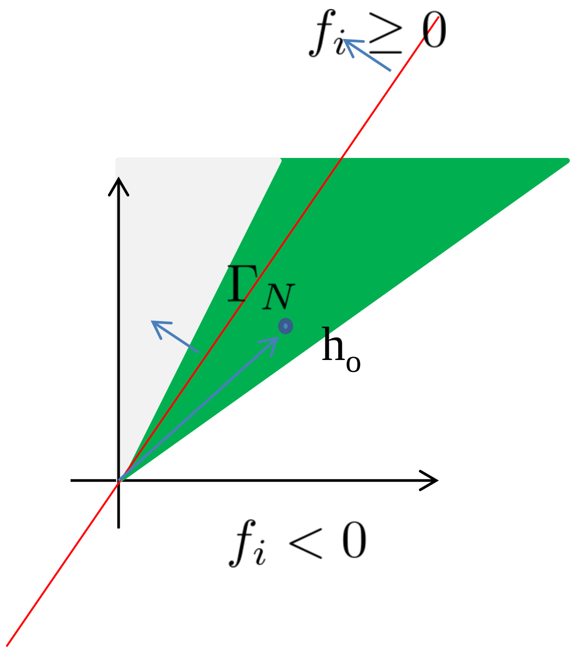
Information inequalities govern impossibilities in inf. Th.

Non-Shannon Inequalities:
Inf.Inequalites that aren't implied by Basic Ineq.

Shannon Inequalies:
Inf. Inequalies that are implied by Basic Ineq.

Appendix. Shannon Entropy, Joint Entropies and Shannon Inequalities

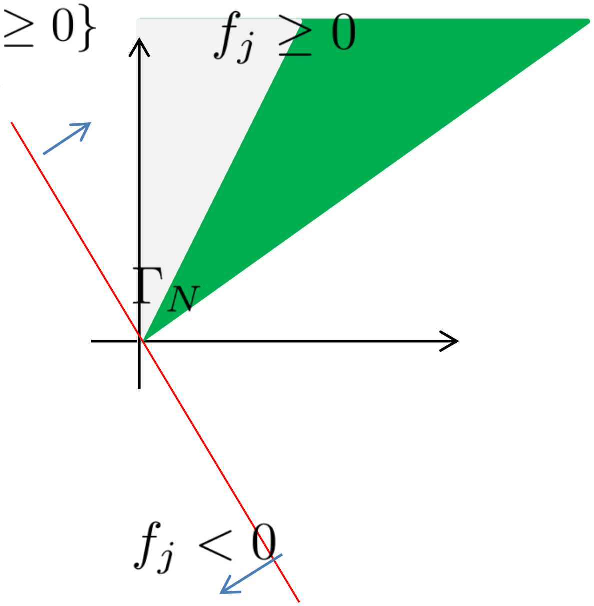
Information Inequalities



Consider
$\mathcal{H}_\mathcal{N} = \mathbb{R}^{2N-1}$

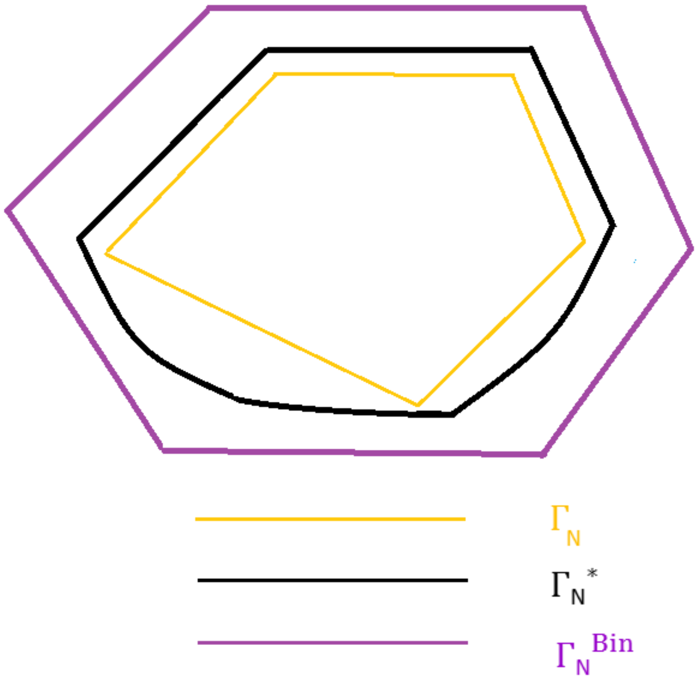
$\Gamma^*_N = \{h \in \mathcal{H}_\mathcal{N} : \text{h is entropic}\}$
$\lrcorner \overline{\Gamma^*_N}$ its convex cone.

$f_i \geq 0$ iff $\overline{\Gamma^*_N} \subseteq \{h \in \mathcal{H}_\mathcal{N} : f(h) \geq 0\}$
$\therefore$ iff $\Gamma^*_N \subseteq \{h \in \mathcal{H}_\mathcal{N} : f(h) \geq 0\}$
$\because \Gamma^*_N \subset \overline{\Gamma^*_N}$



Information Theory & Network Coding , Chapter 13, pg 320 , Raymond Yeung., Springer 2008, 2002. ISBN 978-0-387-79233-0
Networks, Matroids and Non Shannon Information Inequalities , R. Dougherty, Chris Freiling, Kenneth Zeger, IEE E Transactions on Information theory Vol. 53 NO6. June 2007.

Appendix: Inner and outer bounds for the entropic region.



Γ_N Shannon Outer bound (loose)

basic inequalities

$I(X;Y) = H(X) + H(Y) - H(XY) \geq 0$

$I(X_A; X_B | X_C) \geq 0, \forall A, B, C \subseteq X$

Half-space contraints

Γ_N^* Entropic Vectors Region

$\overline{\Gamma}_N^*$ Binary matroid Inner bound

for $N < 4$

A non Shannon type Conditional Inequality of information Quantities, Zhen Zhang, Raymond Yeung.
IEEE transactions of Information Theory Vol 43 No 6, November 1997

Appendix: Groups and Group Actions,

- ✓ **Characterization of the General Linear Group**
- ✓ **Characterization of the Symmetric group**
- ✓ **Fixed points, stabilizer groups , orbits**
- ✓ **Left and Right group actions over a finite set**
- Natural bijection between Orbits and Cosets of Stabilizers
- Standard Quotient Theorem:
- Lagrange Theorem
- Orbit-Stabilizer Theorem
- Proof Cauchy Frobenius Lemma

Appendix: Groups and Group Actions,

The general linear group of degree n through elementary matrices – the set

Set : n×n invertible matrices,

Operation: Ordinary matrix multiplication.

It is a group since:

•Product of two invertible matrices is again invertible,
•Inverse of an invertible matrix is invertible.
•Neutral element is the identity matrix.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 \quad b_1 c_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}^{-1} = \frac{1}{a_1 d_1 - b_1 c_1}\begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix} \qquad \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}^{-1} = \frac{1}{a_2 d_2 - b_2 c_2}\begin{bmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{bmatrix}$$

$$\begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 \quad b_1 c_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}^{-1}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}^{-1}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \qquad \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The general linear group of degree n through elementary matrices – the binary operation

The elementary matrices generate the general linear group of invertible matrices.

Row switching

$$R_i \leftrightarrow R_j \qquad T_{i,j} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Row multiplication

$$kR_i \rightarrow R_i, \qquad k \neq 0 \qquad T_i(m) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & m & 0 & m & m \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Row addition

$$R_i + kR_j \rightarrow R_i,\ i \neq j \qquad T_{i,j}(m) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ m & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & m & 1 & m \end{bmatrix}$$

Left multiplication (pre-multiplication) by an elementary matrix represents elementary row operations, Right multiplication (post-multiplication) represents elementary column operations.

Permutations notations and fixed points

Permutations:

Rearranging members of a set into a particular sequence or order

Example,

Set {1,2,3}: (1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), and (3,2,1).

The number of permutations of n distinct objects is n!

Cauchy's two-line notation:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix};\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix};\ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};\ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};$$

Cycle notation: permutation as a product of cycles corresponding to the orbits of the permutation

$$\sigma_1 = (1)(2)(3)\ ;\ \sigma_2 = (1)(2\ \ 3)\ ;\ \sigma_3 = (1\ \ 2)(3)\ ;\ \sigma_4 = (1\ \ 2\ \ 3)\ ;\ \sigma_5 = (1\ \ 3)(2)$$

An orbit of size 1 is called a fixed point of the permutation.

The subgroup of all permutations for a given set

symmetric group of S, Sym(S)

Set: all permutations of any given set S ,

Operation : Composition of maps (product)

Neutral element: Identity function .

Example,

(1,2,3), (1,2,3), (1,2,3), (1,2,3), (1,2,3), (1,2,3),

↓ ↓ ↓ ↓ ↓ ↓

(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1).

(1,2,3)

↓

(1,3,2)

↓

(3,2,1)

(1,2,3)

↓

(3,2,1)

Appendix: Groups and Group Actions,

Left group action over a finite set

Left Group Action of Group G on Set X

Definition: a group G with binary operation$(\cdot)$

function $G \times X \to X \quad s.t.$

$\forall g \in G$ and $x \in X$,

mapping $(g, x) \to g.x$ operation

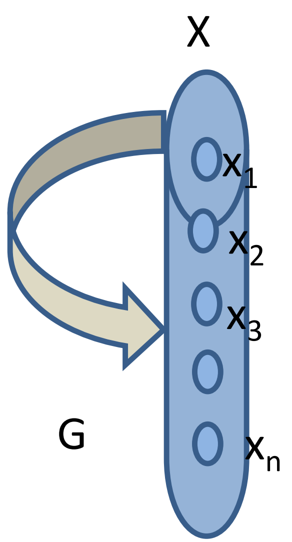
satisfies properties:

(i) compatibility $\quad (g \cdot h).x = g.(h.x) \quad \forall g, h \in G \; and \; \forall x \in X.$

(ii) identity $\quad \exists \; e, \; s.t. \; \; e.x = x \quad \forall x \in X,$

e neutral element of G.

X is left $G-set$.



Appendix: Groups and Group Actions,

Right group action over a finite set

Right Group Action of Group G on Set X

Definition: a group G with binary operation(•)

function $X \times G \to X \quad s.t.$

$\forall g \in G$ and $x \in X$,

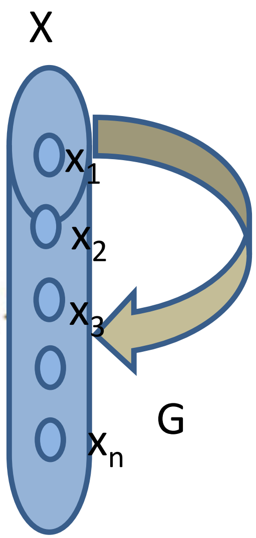
mapping $(x, g) \to x.g$, operation

satisfying axioms:

(i) compatiblity: $x.(g.h) = (x.g).h = (x).g \cdot h \quad \forall g, h \in G$ and $\forall x \in$

(ii) identity: $x.e = x \quad \forall x \in X$

X is right $G-set$.



Equivalence in between Left group action and Right group action on a finite set

left group action ⟺ right group action

$$(g \cdot h)^{-1} = h^{-1} g^{-1}$$

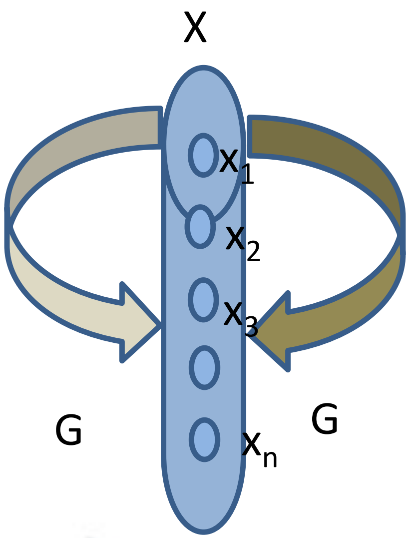
$$\forall g, h \in G \text{ and } \forall x \in X.$$

left group action $(g \cdot h).x =$

$$(g \cdot h)^{-1}(g \cdot h).x.(g \cdot h)$$

$$(h^{-1} g^{-1} g \cdot h).x.(g \cdot h) =$$

$= x.(g \cdot h)$ right group action



Appendix: Groups and Group Actions,

- Characterization of the General Linear Group
- Characterization of the Symmetric group
- Fixed points, stabilizer groups , orbits
- Left and Right group actions over a finite set
- ✓ **Natural bijection between Orbits and Cosets of Stabilizers**
- ✓ **Standard Quotient Theorem:**
- ✓ **Lagrange Theorem**
- ✓ **Orbit-Stabilizer Theorem**
- ✓ **Proof Cauchy Frobenius Lemma**

Frobenius-Cauchy- Burnside Lemma

Stabilizers and Fixed points

orbits

$G(x) \subset X$

X_g fix points

stabilizers.

$G_x \leq G$

Stabilizer of $x \in X$ is $G_x := \{g|gx = x\}$

$x \in X$ is fixed under Fixed point g in G iff $gx = x$.

The set of all fixed points of G is $X_g := \{x|gx = x\}$

The set of all fixed points of a subset S in G is $X_S := \{g \in S|gx = x\}$
If $S = G$ we call it Set of invariants.

we say x is a fixed point of g and g fixes x.

stabilizer subgroup of x (also called the isotropy) is the set of all elements in G that fix x:

Appendix: Cauchy-Frobenious-Burnside Counting Theorem

Natural bijection between Orbits and Cosets of Stabilizers

For a fixed x in X, consider map G to X

$$g \to g.x \text{ for all } g \in G.$$

image of this map is the orbit of x

the coimage is the set of all left cosets of G_x.

The standard quotient theorem of set theory

gives a natural bijection between G/G_x and Gx

given by $hG_x \to h.x$.

orbit-stabilizer theorem.

If G and X are finite then the orbit-stabilizer theorem, together with Lagrange's theorem, gives $|Gx| = [G : G_x] = |G|/|G_x|$.

This result can be employed for counting arguments.

Appendix: Cauchy-Frobenious-Burnside Counting Theorem

Standard Quotient Theorem:

The mapping $G(x) \to G/Gx : gx \to gG_x$ is a bijection ,

$$gx = g'x \Leftrightarrow g^{-1}gx = g^{-1}g'x \Leftrightarrow x = g^{-1}g'x$$

$$\Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow G_x = g^{-1}g'G_x \Leftrightarrow g'G_x = gG_x$$

$$\Downarrow$$

Corollary: If G is a finite group acting on set X , then $x \in X$

$$|G(x)| = |G|/|G_x|$$

The standard quotient bijection in between orbits and cosets of the Stabilizer

Lagrange Theorem:

Lagrange's Theorem *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. number of distinct left cosets of H in G is $\frac{|G|}{|H|}$.*

⇩

$|G| = r|H|$. ⇩

$|a_iH| = |H|$ for each i,

⇩

$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|$.

⇩ cosets are disjoint,

$G = a_iH \cup \cdots \cup a_rH$.

⇩

a in G, $aH = a_iH$ for some i $a \in aH$.

⇩

$a_1H, a_2H, \ldots, a_rH$

distinct left cosets of H in G.

Appendix: Cauchy-Frobenious-Burnside Counting Theorem

Orbit-Stabilizer Theorem

Corollary:

If G is a finite group acting on the set X , then for each $x \in X$

we have $|G(x)| = |G|/|G_x|$

⇧

$G(x)$ has the same number of elements as G / G_x

$|G(x)| = [G : G_x]$

⇧

$g * x \mapsto g G_x$

⇧

there is a well-defined bijection:

$G(x) \to G / G_x$

⇧

Standard Quotient Theorem

(Frobenius-Cauchy- Polya) from standard quotient theorem to Orbit Stabilizer theorem Burnside Lemma

Appendix: Cauchy-Frobenious-Burnside Counting Theorem

Lemma (Cauchy-Frobenius):

The number of orbits of a finite group G acting on a finite set X is equal to the average number of fixed points:

$$|G \backslash\backslash X| = 1/|G| \sum_{ginG} |X_g|$$

$|G| \sum_{t \in F}(1) = |G|.|$

number of orbits of finite group G acting on a finite set X

$\sum_{x \in G(t)} |G(x)|^{-1} = |G(x)||G(x)|^{-1} = 1$

$GX := \{G(t) | t \in F\}$

F is transversal

$\sum_x |G||G(x)|^{-1} = |G| \sum_x |G(x)|^{-1} = |G| \sum_{t \in F} \sum_{x \in G(t)} |G(x)|^{-1}$

Orbit-Stabilizer Theorem

Enumerating elements in the Stabilizer

$\sum_x \sum_{g \in G_x} 1 = \sum_x |G_x| =$

Enumerating fixed points in G x X

$\sum_{g \in G} |X_g| = |\{(g, x) \in G \times X | g.x = x\}| = \sum_{g \in G} \sum_{x \in X_g} 1$

Proof Cauchy Frobenius Lemma

Appendix: Networks , Matroids, Non Shannon Inequalities

$if\ S(x) \neq \emptyset, \ \rightarrow \ |x| = k$ source dim

$if\ e_i \in \epsilon \ \rightarrow \ |e_i| = n$ edge cap

$\forall\, e(x,y)\,, \exists\, f_e: (A^k)^\alpha \times (A^n)^\beta \rightarrow A^n \quad \alpha = |\mu_1, \mu_2, \cdots \mu_n|, \ \beta = |e_{i1}, e_{i2}, \ldots e_{im}|$ Edge function

$\forall\, x \in v, m \in R(x)\,, \exists\, f_{x,m}: (A^k)^\alpha \times (A^n)^\beta \rightarrow A^k \quad \alpha = |\mu_1, \mu_2, \cdots \mu_n|, \ \beta = |ei_1, e_{i2}, \ldots e_{im}|$ Decoding function

$$\forall A,\ (k,n)code: \begin{cases} f_e \rightarrow e \in \epsilon \\ f_{x,m} \rightarrow x \in R(x) \end{cases}$$

$a{:}\, \mu \rightarrow A^k$ *message assigment*
$c{:}\ \epsilon \rightarrow A^n$ *symbol vector*

$$c(e) = f_e(a(x_1), \cdots, a(x_\alpha), c(x_{\alpha+1}), \cdots, c(x_{\alpha+\beta}))$$

$$\forall\, a,\ \ f x_{,m}(a(x_1), \cdots, a(x_\alpha), c(x_{\alpha+1}), \cdots, c(x_{\alpha+\beta})) = a(m)$$

x demand is satisfied,

(k,n) code is a (k,n) solution if every x demand is satisfied

Networks, Matroids and Non Shannon Information Inequalities , R. Dougherty, Chris Freiling, Kenneth Zeger, IEE E Transactions on Information theory Vol. 53 NO6. June 2007.

Appendix: Networks , Matroids, Non Shannon Inequalities

(k,n) solution : over some alphabet, if every demand is satisfied → k/n is achievable coding rate .

Solution of Networks

Solvable: if it has a (k,n) solution k=n=1.

Scalar linearly Solvable: if it has a linear (k,n) solution k=n=1.

Vector linearly Solvable: if it has a linear (k,n) solution k=n.

Coding capacity: sup $\{ \frac{\mathrm{k}}{\mathrm{n}}: \exists\, (k,n)\ coding\ solution\ in\ C\ over\ A\}$

Linear

Routing

} $C\ class\ of\ codes$

A alphabet

If $\exists\, (k,n)\ solution \mid \frac{k}{n} = Capacity,$ → Achievable coding capacity

Networks, Matroids and Non Shannon Information Inequalities , R. Dougherty, Chris Freiling, Kenneth Zeger, IEE E Transactions on Information theory Vol. 53 NO6. June 2007.

Appendix: Networks , Matroids, Non Shannon Inequalities

Codes of interest:

- Linear: linear edge and decoding functions
- Routing: simple copy - edge and decoding functions

Networks of interest:

- Multicast: One source node, receiver catching all source messages
- Multiple unicast: each message generated and demanded by just one source respectively

Network coding goal:

Achievable coding rate as large as possible

sup { $\frac{k}{n}$: $\exists\ (k, n)$ $coding\ solution\ in\ C\ over\ A$}

Network $\mathcal{N}(\mu, v, \epsilon)$

$\epsilon = \epsilon_{in} \cup \epsilon_{out}$

S: $v \rightarrow 2^{\mu}$

$x \rightarrow S(x)$

R: $v \rightarrow 2^{\mu}$

$x \rightarrow R(x)$

$In(x) = S(x) \cup \epsilon_{in}$

$Out(x) = R(x) \cup \epsilon_{out}$

Input (x)=$[\mu_1, \mu_2, \cdots \mu_n; e_{i1}, e_{i2}, \ldots e_{im}]$

Networks, Matroids and Non Shannon Information Inequalities , R. Dougherty, Chris Freiling, Kenneth Zeger, IEE E Transactions on Information theory Vol. 53 NO6. June 2007.

Appendix : Characterization of entropy functions

Proposition 1: $\forall$ subsets $\alpha, \beta, \gamma \subset N_n=\{1,\dots,n\}$, let $\Omega = \{X_i, i = 1, \dots, n\}$ be jointly distributed discrete random variables set, $\rightarrow$ $I(\alpha, \beta|\gamma\} \geq 0$ (**Basic Inequalities**)

⇩

Joint entropies are maps $H_\Omega: 2^{N_n} \rightarrow [0, \infty)$

F_n is set of All maps $2^{N_n} \rightarrow [0, \infty)$

Def. $\boldsymbol{\Gamma_n} = \{\boldsymbol{F} \epsilon F_n: F(\emptyset) = 0 : \alpha \subset \beta \rightarrow F(\alpha) \leq F(\beta); \forall \alpha, \beta \epsilon 2^{Nn}\ F(\alpha)+F(\beta) \geq F(\alpha \cup \beta)+F(\alpha \cap \beta)\}$

Def. A function $\boldsymbol{F} \epsilon F_n$ is called constructible iff $\exists\ \Omega$, s.t. $H_\Omega = \boldsymbol{F}$

Def. $\boldsymbol{\Gamma_n}* = \{\boldsymbol{F} \epsilon F_n: \boldsymbol{F}$ is constructible$\}$

Def. A function $\boldsymbol{F} \epsilon F_n$ is called asymptotically constructible iff $\exists$ *sequence of sets* Ω^k, $k=1,\dots,$ $\exists\ H_{\Omega^k}$ s.t $\lim_{k\rightarrow\infty} H_{\Omega^k} = \boldsymbol{F}$

$\boldsymbol{F}$ is asymptotically constructible iff $\boldsymbol{F} \epsilon \overline{\boldsymbol{\Gamma_n} *}$

On Characterization of Entropy function via Information Inequalities. Zhen Zhang, Raymond Yeung, IEEE transactions on Information Theory, Vol. 44 No. 4, July 1998,

Appendix : Shannon Information inequalities

Information Identities

$h(\alpha|\beta)=h(\alpha,\beta)-h(\beta)$

$I(\alpha;\beta)=h(\alpha)-h(\alpha|\beta)$

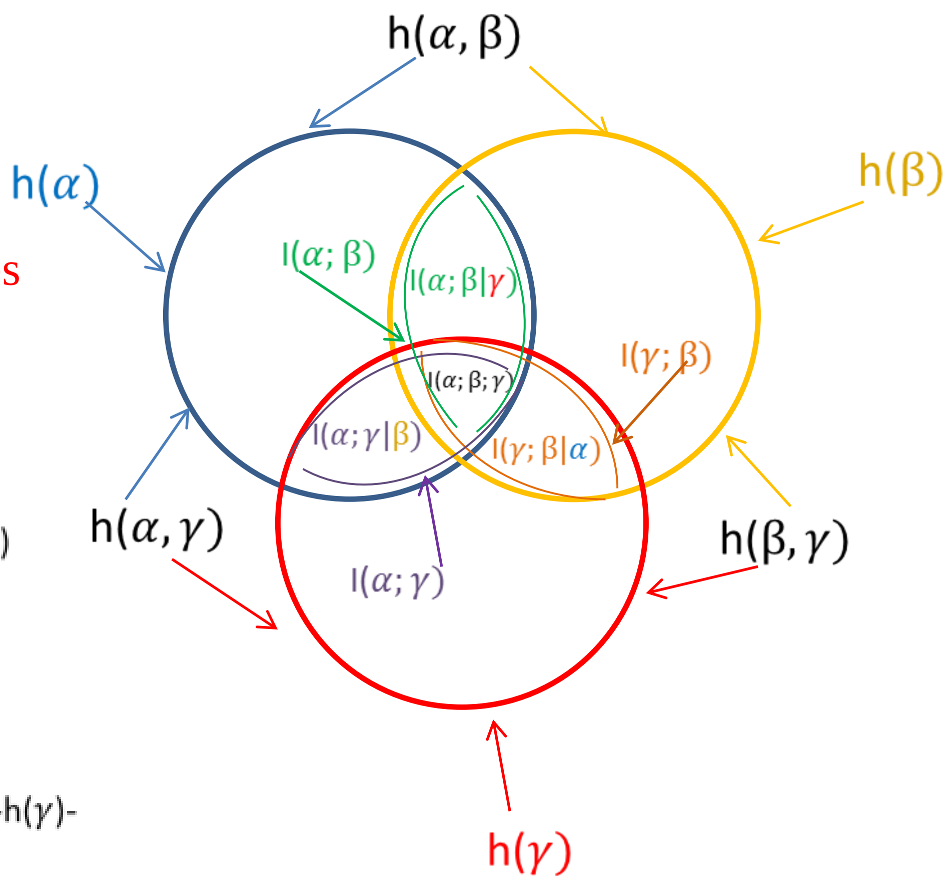
$I(\alpha;\beta|\gamma)=h(\alpha|\beta)-h(\alpha|\beta,\gamma)$

$h(\emptyset)=0$

$I(\alpha;\beta)=h(\alpha)+h(\alpha)-h(\alpha,\beta)$

$I(\alpha;\beta|\gamma)=h(\alpha,\gamma)+h(\beta,\gamma)-h(\gamma)-h(\alpha,\beta,\gamma)$

$I(\alpha;\beta,\gamma) = I(\beta;\alpha|\gamma) + I(\alpha;\gamma)$



$h(\alpha)=h(\alpha|\emptyset)>0$

$h(\alpha|\beta)>0$

$I(\alpha|\beta)>0$

$h(\alpha,\beta|\gamma)\leq h(\alpha|\gamma)-h(\beta|\gamma)$

$h(\alpha|\beta,\gamma)\leq h(\alpha|\gamma)\leq h(\alpha,\gamma|\beta)$

Shannon Inequalities

Recent Progresses in Characterising Information Inequalities, Therence Chan, Entropy 2011, 13, 379-401 doi:10.3390/e13020379

Networks, Matroids and Non Shannon Information Inequalities , R. Dougherty, Chris Freiling, Kenneth Zeger, IEE E Transactions on Information theory Vol. 53 NO6. June 2007.

- ✓ **Analytical approach for binary linear codes- Abstract Algebra – from Dr. Marcel Wild research.**

2nd step:
Averaging
Sym group fix points from points fixed by a canonical representative of Conjugacy classes Times size of the class.

- ✓ The Sym group Conjugacy classes Cardinality.
- ✓ Type of Permutation
- ✓ Partitions associated with cycle type
- ✓ Polya Cycle Index

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu, i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Appendix: Entropic vectors - analytic enumeration of binary linear codes

Burnside lemma expression readapted for conjugacy classes of matrices and permutations.

$$b(n, \leq r) = \frac{\sum_{(A,\pi) in GL_r^2 x S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

$$|H \wr_x G \backslash\backslash Y^x| = \frac{\sum_{(\psi,g)\in H \wr_x G} \prod_{v=1}^{c(g)} |Y_{h_v(\psi,g)}|}{|H^x||G|}$$

$$b(n, \leq r) = \frac{\sum_{(A,\pi) in GL_r^2 x S_n} \prod_{i=1}^{n} |Y_{A^i}|^{a_i(\pi)}}{|GL^2||S_n|}$$

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu,i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

Construction Enumeration Analytical method :

- ✓ **Group Theory approach for binary linear codes- Abstract Algebra – from Dr. Marcel Wild research.**

4th step:

General Linear & Sym group Acting Together on the set of binary linear codes.

- ✓ Polya Index and Vector index analogy
- ✓ Permutation & Automorphism number analogy.
- ✓ Symmetric Permutations and Linear transformations Analogy.

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu, i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Type of Permutation characterize all possible Partitions induced By the sym Group over the Finite set.

$\pi\tau \in S_n$ are conjugate iff $a_i(\pi) = a_i(\tau)$ for all $1 \leq i \leq n$. A conjugation preserves cycle type,

specifying a cycle type,

$\Updownarrow$

specifying a partition of n,

$\Updownarrow$

specify a conjugacy class in S_n.

Conjugacy classes of $S_n \leftrightarrow$ number of partitions of n,

The sequences $\lambda = (\lambda_1, \ldots, \lambda_t)$,$\lambda_i \in \mathbb{N}$ s.t.

$\lambda_1 + \cdots + \lambda_t = n$ and $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_t$.

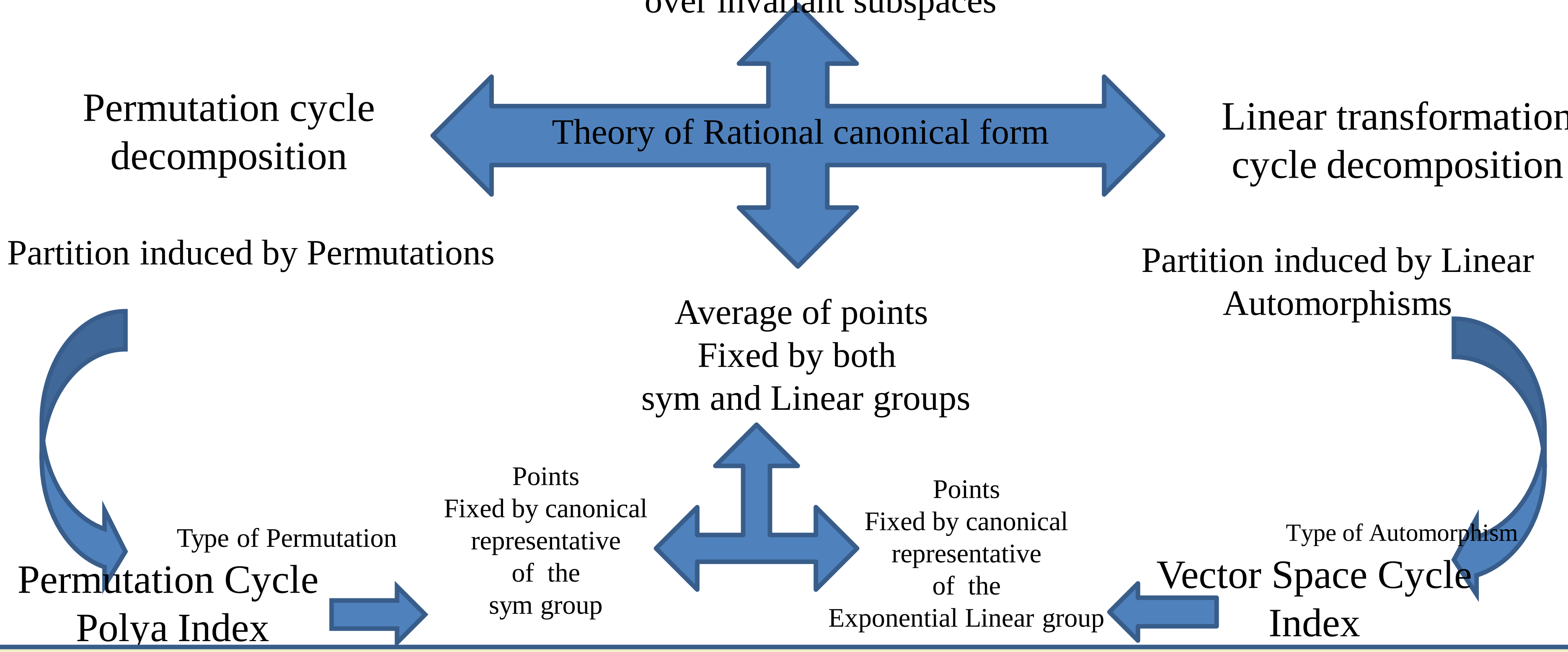
If λ is a partition of n, $\therefore \lambda \vdash n$

Appendix: Entropic vectors - analytic enumeration of binary linear codes

Analogy (Joseph Kung)

Permutation Cycle decomposition & **Automorphisms decomposition**

- ✓ Decomposition of Linear transformations into direct sum of Cyclic linear transformations
- ✓ Decomposition of Vector Space automorphisms into direct sum of Cyclic automorphisms over invariant subspaces



Construction Enumeration Analytical method Outline :

- ✓ **Analytical approach for binary linear codes- Abstract Algebra – from Dr. Marcel Wild research.**

2nd step:
Averaging
Sym group fix points from points fixed by a canonical representative of Conjugacy classes Times size of the class.

- ✓ The Sym group Conjugacy classes Cardinality.
- ✓ Type of Permutation
- ✓ Partitions associated with cycle type
- ✓ Polya Cycle Index

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu, i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

The Size of a conjugacy class in the symmetric group

arrange 1 to 7 in any of 7!

$(a_1a_2)(a_3a_4)(a_5a_6a_7)$

Notice $(a_1,a_2)= (a_2,a_1)$

$(a_5a_6a_7)=(a_7a_5a_6)=(a_6a_5a_7)$

each k-cycle over counted by a factor of k.

Notice $(a_1a_4)(a_3,a_4)=(a_3a_4)(a_1a_2)$

over counted ways to arrange 2-cycles

we have

$$\frac{7!}{3 \cdot 2 \cdot 2 \cdot 2} = 210$$

cycle type permutations in S_7.

cycle type c_1 1-cycles, c_2 2-cycles, . . . c_k k- cycles,

$$1c_1 + 2c_2 + \cdots + kc_k = n.$$

in our example $c_1 = 0$, $c_2 = 2$, and $c_3 = 1$

The Size of a conjugacy class in the symmetric group

n! possible ways to permute
but we need to **correct over counting.**
Therefore:

- ✓ Each of the $\mathbf{c_j}$ j-cycles can be rotated around j ways and be the same cycle,
  - ✓ so **divide by** $\mathbf{j^{c_j}}$
    $j = 1, 2, \ldots, k.$
- ✓ There are $\mathbf{c_j}$ j-cycles which *can be permuted around in* $\boldsymbol{c_j}$*!* ways,
  - ✓ so **divide by** $\mathbf{c_j!}$
    $j = 1, 2, \ldots, k.$

The Size of a conjugacy class in the symmetric group

Number of permutations in the conjugacy class described by the c_i 's is

$$|C_\lambda| = n! \left(\prod_{i=1}^{k} i^{c_i} \prod_{i=1}^{k} c_i! \right)^{-1}$$

The denominator is often called z_λ (for partitions of cycle type λ)

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

Construction Enumeration Analytical method Outline :

- ✓ **Analytical approach for binary linear codes- Abstract Algebra – from Dr. Marcel Wild research.**

2nd step:
Averaging
Sym group fix points from points fixed by a canonical representative of Conjugacy classes Times size of the class.

- ✓ The Sym group Conjugacy classes Cardinality.
- ✓ Type of Permutation
- ✓ Partitions associated with cycle type
- ✓ Polya Cycle Index

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n)\, 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu, i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Decomposition of a Permutation to the direct sum of cyclic Permutations

(Type of a permutation)

let π be a permutation of finite set S

$$|S| = d$$

$$\pi = \sigma_1 . \sigma_2 \cdots \sigma_n , \quad \sigma_i \cap \sigma_j = \emptyset ,$$

$$S = S_1 \cup S_2 \cup S_n , \quad S_i \subset S , \quad \pi S_i = S_i$$

S_i is the minimal subset of S invariant under π.

type of the permutation $a(\pi) = (a_1(\pi), \ldots, a_i(\pi) \ldots, a_d(\pi))$

$a_i(\pi)$ is the number of cyles of length i in the cycle decomposition.

The Type of permutation and the cyclic decomposition of permutations.

Appendix: Entropic vectors - analytic enumeration of binary linear codes

Points Fixed by a representative of Permutations group Conjugacy Classes

$\pi\tau \in S_n$ are conjugate iff $a_i(\pi) = a_i(\tau)$ for all $1 \leq i \leq n$.

The conjugacy classes of S_n ⟺ partitions of n,

sequences $\lambda = (\lambda_1, \ldots, \lambda_t)$ of natural numbers

satisfying

$\lambda_1 + \ldots + \lambda_t = n$ $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_t.$

λ is a partition of n $\lambda \vdash n$

set of all partitions of n is: $Part(n) := \lambda | \lambda \vdash n$

$\lambda_j = i$ is denoted as $a_i(\lambda)$

λ parametrize the conjugacy classes C_λ of the group S_n.

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).
Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

he cycle Index for permutations.

Introducing the Polya cycle Index

Expressing Permutations of a Group as a Polynomial

let G is a permutation group on S,

the permutation cycle index,

also called Polya cycle index,

$$Z(G;x) = \frac{\sum_{\alpha \in G} \prod_{i,b} x_{i,b}^{a_{i,b(\alpha)}}}{|G|}$$

$Z(G;x)$ is the generating function of permutations in G,

Construction Enumeration Analytical method Outline :

- ✓ **Analytical approach for binary linear codes- Abstract Algebra – from Dr. Marcel Wild research.**

3th step:
General Linear group fix points
From points fixed by a
canonical representative
of Conjugacy classes
Times
Size of the class.

- ✓ Conjugacy classes of the $GL_n(r)$
- ✓ Conjugacy classes Cardinality of General Linear Group
- ✓ Type of Automorphisms.
- ✓ The vector space cycle index

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu,i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

elements of H^X group partitioned in conjugacy classes;

$$H^x = \{ \psi: (h_1, h_2, h_3, \ldots\ldots\ldots h_x) \mid h_i \in H \}$$

ψ and ψ' of H are conjugate if

ψ_i in H^X with $\psi_i \psi' \psi_i^{-1} = \psi$

conjugacy is equivalence relation

partitions H^X into equivalence classes.

every ψ in H^X belongs to one conjugacy class

$Cl(\psi') = Cl(\psi) \Leftrightarrow \psi', \psi$ are conjugate,

$$Cl(\psi) = \psi_i \psi \psi_i^{-1} : \psi_i \in H^x$$

Conjugacy classes of the products of elementary matrices from the linear group of permutations

Appendix: Entropic vectors - analytic enumeration of binary linear codes

The Polya cycle index Enumeration objects classes under permutation group action.

The vector space cycle index counting objects classes under linear group action **.**

LEMMA 2. (Joseph Kung 1981)
Let p be a monic irreducible polynomial in R of degree m,
and $b=(b_1, b_2, \dots)$ a partition of j.
Define *the numbers* d_i *by*
$d_i = b_1 1 + b_2 2 + .*. + b_i\, i + b_{i+1}\, i + \dots b_j\, i.$
Then $c_p(b)$*, the number of invertible matrices commuting with the block diagonal matrix D(p, b), is given by*

$$c_p(b) = \prod_i \prod_{k=1}^{b_i} \left(q^{md_i} - q^{m(d_i - k)}\right).$$

In particular, $c_p(b)$ *depends only on the degree of p.*

$$h(u, \epsilon) := \prod_{i=1}^{e} \prod_{k=1}^{\beta_i} \left(2^{m\delta_i} - 2^{m(\delta_i - k)}\right)$$

$$|D\mu| = |D(p; \epsilon_1, \dots, \epsilon_s)| = \frac{|GL_r^2|}{h(p_1, \epsilon_1) \cdots h(p_s, \epsilon_s)}$$

Enumeration of Binary and Ternary matroids and other applications of the Brylawski-Lucas-Theorem , Marcel Wild , preprint, No. 1693, Technische Hochschule Darmstadt(1994).

Consequences of the Brilawsky- Lucas Theorem for Binary Matroids , Marcel Wild, Europ, J.Combinatorics 17, 309-316, 1996

Appendix: Entropic vectors - analytic enumeration of binary linear codes

Type of Automorphism

Automorphism α

α ⟺ array $a(\alpha)$ its Type,

Entries indexed by (i, b),

i → positive integer,

b → sequence of nonnegative integers

finitely many nonzero terms.

$a_{i,b}(\alpha)$ → number of subspaces U

in the primary decomposition of α of order $p(z)^i$,

$p(z)^i$ is irreducible

α restricted to U having species b.

$a(\alpha)$ has finitely

many nonzero entries.

$$a(\alpha) = \begin{pmatrix} a_{i_1,b_1}(\alpha) \cdots & a_{i_1,b_j}(\alpha) & a_{i_1,b_n}(\alpha) \\ \vdots \quad \cdots & \vdots & \vdots \\ \quad \cdots & & \\ a_{i_m,b_1}(\alpha) \cdots & a_{i_m,b_j}(\alpha) & a_{i_m,b_n}(\alpha) \end{pmatrix}$$

The type of automorphism needed to complete the expression for number of points fixed by a canonical automorphism using the vector space cycle index.

Appendix: Entropic vectors - analytic enumeration of binary linear codes

Decomposition of an Automorphism in to the direct sum of cyclic automorphisms

Definition: (Vector space cycle index)

Let H be a finite linear group acting on the vector space V:

a finite subgroup of GL(V) of all automorphims of V.

$x_{i,b}$, i → positive integer

b → a sequence of nonnegative integers with finitely many nonzero terms.

The Vector space cycle index is :

$$Z(\mathrm{H}; x) = \frac{\sum_{\alpha in G} \prod_{i,b} |x_{i,bi}|^{a_{i,b}(\alpha)}}{|H|}.$$

, where $\prod_{i,b} |x_{i,bi}|^{a_{i,b}(\alpha)}$ is weight of the automorphism.

The vector space cycle index and the weight of automorphisms used to count the points fixed by the canonical automorphism of linear vector space.