Networks and Matroids

Congduan Li

Adaptive Signal Processing and Information Theory Research Group
ECE Department, Drexel University

June 1, 2012

Outline

Mappings and Definitions

Source Mapping: $S : V \to 2^{\mu}$, μ is message set.
Message Assignment: $a : \mu \to \mathcal{A}^k$, k: source dimension,
Edge assignmetn: $c : E \to \mathcal{A}^n$, n: edge capacity.
Receiver Mapping: $R : V \to 2^{\mu}$. (Demands)
Alphabet: a finite set $\mathcal{A}$ where messages are chosen from.
$In(i)$ & $Out(i)$ include message generated and demanded, resp..
Edge function: $f_e : (\mathcal{A}^k)^{\alpha} \times (\mathcal{A}^n)^{\beta} \to \mathcal{A}^n$.
Decoding function: $f_{t_l,m} : (\mathcal{A}^k)^{\alpha} \times (\mathcal{A}^n)^{\beta} \to \mathcal{A}^k$.
(k, n) solution: every demand of every receiver is satisfied.
Achievable coding rate: if (k, n) solution exists, k/n.
Solvable: $k = n = 1$ (scalar-linearly), $k = n \neq 1$ (vector-linearly).
Coding capacity: $\sup\{k/n :$
$\exists(k, n)$ coding solution in a class of network codes over $\mathcal{A}\}$.

Network Conditions

For a (k, n) solution, the following conditions hold for a network:

1. Source Rates: $H(x) = k|x|$ for any $x \subseteq \mu$
2. Edge Capacity: $H(e) \leq n$ for any $e \in E$
3. Functional Dependency:
   $H(In(t)) = H(In(t) \cup Out(t)), \forall t \in V$

Example to show coding capacity

Example

Butterfly network has two sources and two sinks with constraints of 1 on each edge.

$$\begin{aligned} 2k &= H(x) + H(y) \\ &= H(x, y) \\ &\leq H(x, y, z) \\ &= H(x, z) + H(y|x, z) \\ &= H(x, z) \\ &\leq H(x) + H(z) \\ &\leq k + n \end{aligned}$$

We get $k/n \leq 1$.

Definition

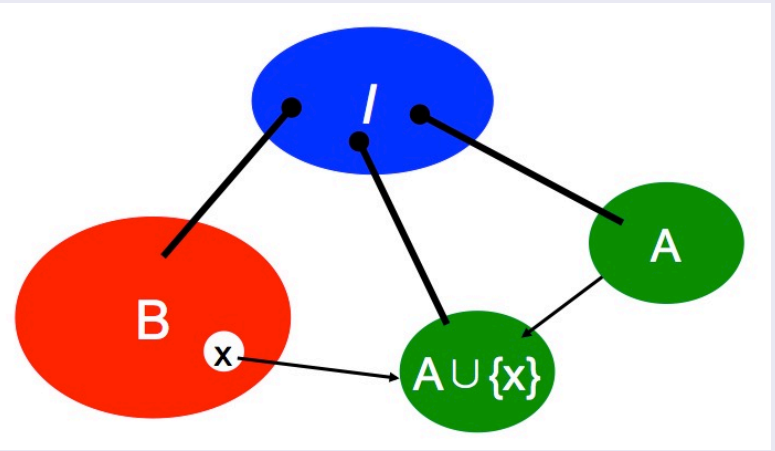
Definition

A matroid M is an ordered pair $(E, \mathcal{I})$ consisting of a finite set E and a collection $\mathcal{I}$ of subsets of E having the following three properties:

1. $\phi \in \mathcal{I}$;
2. Hereditary:
   If $I \in \mathcal{I}$ *and* $I' \subseteq I$, *then* $I' \in \mathcal{I}$;
3. Augmentation:
   If I_1 *and* I_2 *are in* $\mathcal{I}$ *and* $|I_1| < |I_2|$, *then there is an element* e *of* $I_2 - I_1$ *such that* $I_1 \cup e \in \mathcal{I}$.

Demo

Augmentation



Base/Basis

Bases $\mathcal{B}(M)$ of a matroid are the maximal independent sets.

Properties

- Same cardinality for all bases;
- The matroid is in the span of any base;

Consider

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Bases: {1,2,3}, {1,2,4}, {1,2,5}, {1,3,4}, {1,4,5}, {2,3,4}, {2,3,5}, {3,4,5}

Base

A collection of subsets $\mathcal{B} \subseteq 2^E$ of a ground set E are the bases of a matroid if and only if:

- $\mathcal{B}$ is non-empty;
- base exchange: If $B_1, B_2 \in \mathcal{B}$, for any $x \in (B_1 - B_2)$, there is an element $y \in (B_2 - B_1)$ such that $(B_1 - x) \cup y \in \mathcal{B}$.

Consider

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Bases: {1,2,3}, {1,2,4}, {1,2,5}, {1,3,4}, {1,4,5}, {2,3,4}, {2,3,5}, {3,4,5}

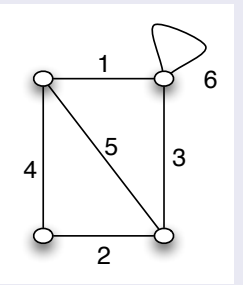
Circuit

The circuits $\mathcal{C}(M)$ of a matroid are the minimal dependent sets.

Property

- If any one element is deleted from a circuit, it will become an independent set.
- Independent sets $\mathcal{I}(M)$ does not contain any element in $\mathcal{C}(M)$.

Consider the graph



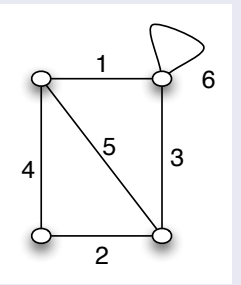
Circuits: {1,2,3,4}, {1,3,5}, {2,4,5}, {6}

Circuit

A collection of sets $\mathcal{C}$ is the collection of circuits of a matroid if and only if:

- $\phi \notin \mathcal{C}$
- if $C_1, C_2 \in \mathcal{C}$ with $C_1 \subseteq C_2$ then $C_1 = C_2$
- if $C_1, C_2 \in \mathcal{C}, C_1 \neq C_2$ and $e \in C_1 \cap C_2$ then there is some $C_3 \in C$ with $C_3 \subseteq (C_1 \cup C_2) - e$.

Consider the graph



Circuits: {1,2,3,4}, {1,3,5}, {2,4,5}, {6}

Rank Function

For any base of a matroid, $r(B) = r(M)$.
Formally, a rank function is $r : 2^E \to \mathbb{N} \cup \{0\}$, for which

- For $X \subseteq E, 0 \leq r(X) \leq |X|$
- If $X \subseteq Y \subseteq E, r(X) \leq r(Y)$
- $\forall X, Y \subseteq E, r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$

Consider

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Bases: {1,2,3}, {1,2,4}, {1,2,5}, {1,3,4}, {1,4,5}, {2,3,4}, {2,3,5}, {3,4,5};
Rank: $r(M) = r(B) = 3$

Closure

Given a rank function of a matroid, the closure operation $\mathrm{cl} : 2^{\mathrm{E}} \rightarrow 2^{\mathrm{E}}$ is defined as

$$\mathrm{cl}\ X = \{x \in E | r(X \cup x) = r(X)\}.$$

Closure is a span of a subspace.
$\mathrm{cl}\ B = E(M)$;
Independent Set:
$\mathcal{I} = \{X \subseteq E | x \notin \mathrm{cl}(X - x) \forall x \in X\}$

A subset X of $E(M)$ is said to be a flat if $\mathrm{cl}\ \mathrm{X} = \mathrm{X}$.
Consider

$$A = \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \left[\begin{array}{cccccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right] \end{array}$$

cl {1,2}={1,2,} $\rightarrow$ flat
cl {1,3}={1,3,5}

Closure

A function $\mathrm{cl} : 2^{\mathrm{E}} \to 2^{\mathrm{E}}$ is closure for a matroid $M = (E, \mathcal{I})$ iff

- If $X \subseteq E$ then $X \subseteq \mathrm{cl}X$
- If $X \subseteq Y \subseteq E$, then $\mathrm{cl}X \subseteq \mathrm{cl}Y$
- If $X \subseteq E$ then $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}X$
- If $X \subseteq E$ and $x \in E$ and $y \in \mathrm{cl}(X \cup x) - \mathrm{cl}(X)$ then $x \in \mathrm{cl}(X \cup y)$

Consider

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

cl {1,2}={1,2,} → flat

cl {1,3}={1,3,5}

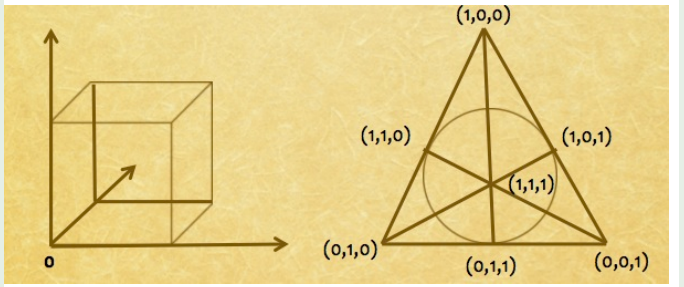
Representable Matroids

Definition

A matroid that is isomorphic (bijection between two matroids) to a vector matroid, where all elements take values from field $\mathbb{F}$, is called $\mathbb{F}$-representable.

Example

Fano matroid is only representable over field of characteristic 2 (Binary).



Binary matroids have excluded minor: $U_{2,4}$

Definition

Definition

Let $\mathcal{N}$ be a network with message set μ, node set V and edge set E. Let $\mathcal{M} = (\mathcal{S}, \mathcal{I})$ be a matroid with rank function r. The network $\mathcal{N}$ is a matroidal network associated with $\mathcal{M}$ if there exists a funciton $f : \mu \cup E \to \mathcal{S}$ such that the following conditions hold:

1. f is one-to-one on μ;
2. $f(\mu) \in \mathcal{I}$;
3. $r(f(In(x))) = r(f(In(x) \cup Out(x)))$, for every $x \in V$.

Examples

One node transmits two messages to another node. $(U_{2,2} \& U_{2,3})$

Fact

Matroid associated with a network need not to be unique.

Theorem

Theorem

If a network is scalar-linearly solvable over some finite field, then the network is matroidal. In fact, the network is associated with a representable matroid.

Proof.

On next slide. □

Proof of theorem

Proof.

Fix a scalar-linear solution to the network over finite field F, and let $a_1, \ldots a_m$ be messages. Let $x_1, \ldots$ be message and edge variables. For each i, the variable x_i can be written as a linear comnination $c_i^{(i)} a_1 + \cdots + c_m^{(i)} a_m$ of the messages, where $c_j^{(i)} \in F, \forall j$. Form a matrix with a column $C^{(i)} = \begin{pmatrix} c_1^{(i)} \\ \vdots \\ c_m^{(i)} \end{pmatrix}$ for each x_i. Let $\mathcal{M}$ be the vector matroid for this matrix and r be the rank function of $\mathcal{M}$. $f(x_i) = i$. f is one-to-one, giving condition 1. If x_i is message a_j, $C^{(i)}$ has all components zero except the j-th component. If $x_i \in Out(y)$, then x_i is a linear combination of $In(y)$, so $r(f(\{x_i\} \cup In(y))) = r(f(In(y)))$. □

Corollary

Corollary

All solvable multicast networks are matroidal.

Proof.

In "Linear Network Coding" by Li, Yeung and Cai 2003, it is showed that all solvable multicast networks are scalar-linearly solvable over some finite field. Combined with previous theorem, we obtain this corollary. □

Fact

Fact

Unsolvable network is not matroidal.

Example

One node has two messages (a,b) but only have one output edge (x) and another node is requiring both messages. If matroidal,

$$\begin{aligned} 2 &= r(f(a), f(b)) \\ &\leq r(f(a), f(b), f(x)) \\ &= r(f(x)) \\ &\leq 1 \end{aligned}$$

Fact

Not all solvable networks are matroidal.

Example

M-network: vector routing solvable but not matroidal. Solution showed on board and can be found in [1].

Proof.

Use the Shannon-type information ineqyality:

$$I(C;D) \leq I(A;B) + H(C|A) + H(D|B)$$

Construction Steps

- Matroid $\mathcal{M} = (\mathcal{S}, \mathcal{I})$ with rank function r, network $\mathcal{N}$ with V, E, μ
- Function $f : \mu \cup E \to \mathcal{S}$ and $g : \mathcal{S} \to V$

1. Choose base $B = \{b_1, \ldots b_{r(\mathcal{S})}\}$ and let $f(m_i) = b_i$ and $g(b_i) = n_i$.
2. (to be repeated until it is no longer possible) Find circuit $\{x_0, \ldots x_j\}$ that only $g(x_0)$ has not been defined, we do:
   1. add a new node y and edges $(e_1, \ldots e_j)$ connecting $g(x_i)$ to y and define $f(e_i) = x_i$;
   2. add another new node n_0 with a single in-edge e_0 connecting y to n_0 and let $f(e_0) = x_0$ and $g(x_0) = n_0$.

Construction Steps Cont.

1. (to be repeated as many times as desired) If $\{x_0, \ldots x_j\}$ is a circuit and $g(x_0)$ is a source node with message m_0, then add to the network a new receiver node y which demands the message m_0 and which has in-edges $e_1, \ldots e_j$ where e_i connects $g(x_i)$ to y and where $f(e_i) = n_0$.
4. (to be repeated as many times as desired) Choose a base $B = \{b_1, \ldots b_{r(\mathcal{S})}\}$ and create a receiver node y that demands all of the network messages, and such that y has in-edges $e_1, \ldots e_{r(\mathcal{S})}$ where e_i connects $g(x_i)$ to y. Let $f(e_i) = x_i$.

Examples

Example

Show on board: Butterfly network ($U_{2,3}$), Vamos Network.

Vamos Network: Routing Capacity

Obtained from Vamos matroid (V_8), the non-representable matroid with minimum number of elements.

Theorem

The routing capacity of the Vamos network is 2/5.

Proof.

Consider demands at node n_{10} and n_{12}. These two require edges $e_{3,4}$ and $e_{5,6}$ to carry all k components of a and d. Then consider the demand of node n_9 for b. For possible largest coding rate, $e_{3,4}$ and $e_{5,6}$ must carry at least $k/2$ components of b. Thus $2k + k/2 \leq n$ and $k/n \leq 2/5$.
A code achieving this capacity: $e_{1,2} = b_1, c, d$, $e_{3,4} = b_1, a, d$, $e_{5,6} = b_2, a, d$, $e_{7,8} = b_2, a$. □

Q&A

Thank you!

- "Information Theory and Network Coding", Raymond Yeung, Chap 17,18&19
- "Networks,Matroids, and Non-Shannon Information Inequalities", R. Dougherty, C. Freiling and K. Zeger, Trans. Information Theory, Vol. 53, No. 6 June 2007
- "On coding for non-multicast networks", M. Medard, M. Effros, T. Ho and D. Karger, in proc. 41st Allerton, 2003