Applications of Matroid Theory to Network Coding

Alex Sprintson

ECE Department

Texas A&M University

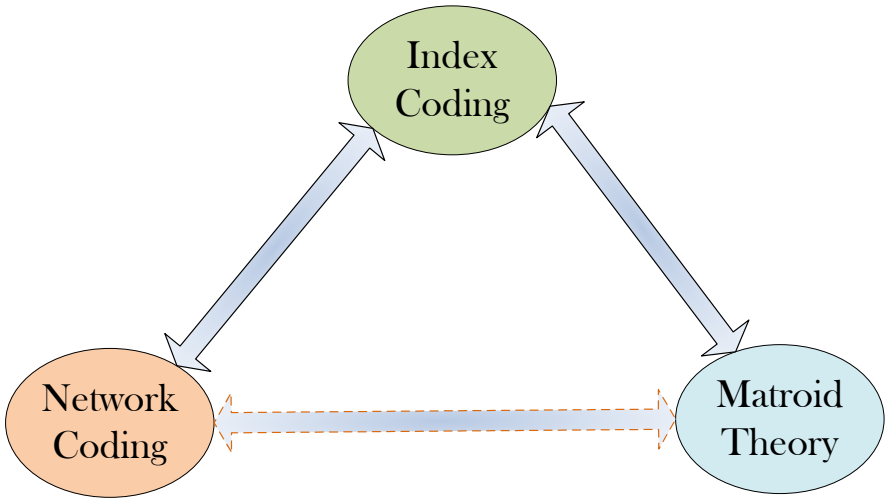
Joint work with Salim El Rouayheb & Costas Georghiades

BIRS workshop
Banff, Canada

Aug. 5, 2009

Outline

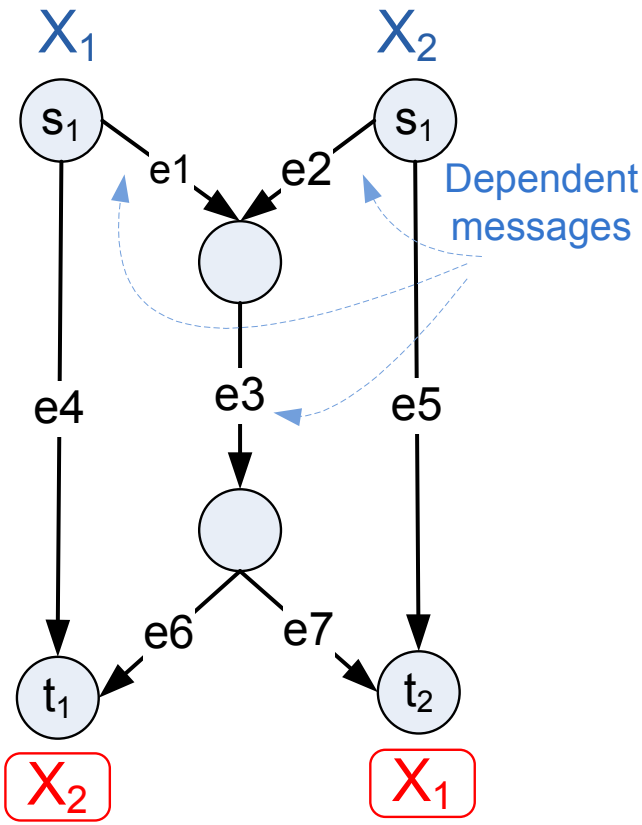
1. Outline connections between the matroid theory, network coding, and index coding.
2. Present two ways of constructing new classes of coding networks from matroids
3. Show that these constructions are instrumental for establishing several important properties of coding networks
   - E.g., Insufficiency of linear coding



Papers covered

1. R. Dougherty, C. Freiling, K. Zeger, *"Networks, Matroids, and Non-Shannon Information Inequalities,"* IEEE Trans. Inf. Th., 2007
2. Lubetzky, E. and Stav, U. 2007. *"Non-Linear Index Coding Outperforming the Linear Optimum"*. In Proceedings of the 48th FOCS 161-168.
3. S. El Rouayheb, S. and C. N. Georghiades, *"A New Construction Method for Networks from Matroids"*, ISIT, 2009

Dependency Relations in Networks

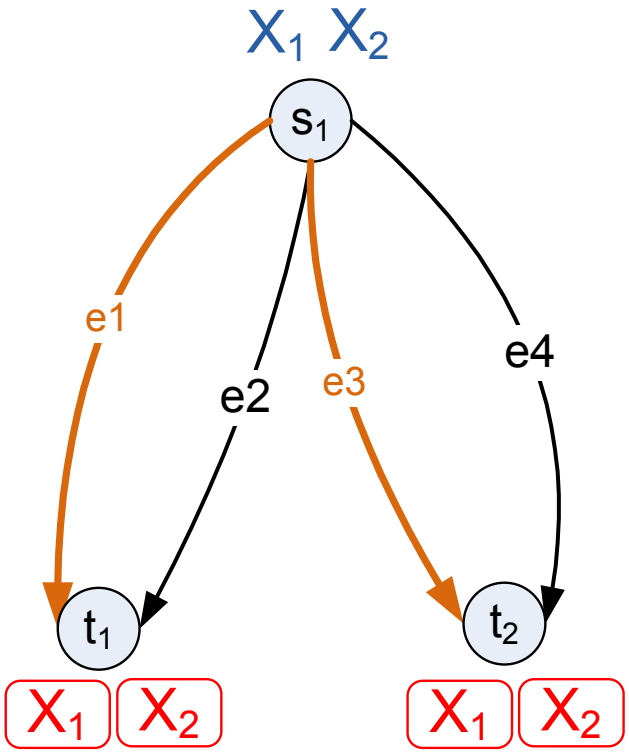


- The network dictates dependency relations among the source and edge messages
- Let Y_{e_i} the message carried by edge e_i
- For instance, for any linear network coding solution for the butterfly network, the sets $\{Y_{e1}, Y_{e2}, Y_{e3}\}$ and $\{Y_{e4}, Y_{e6}, X_2\}$ are dependent

Networks vs. Matroids

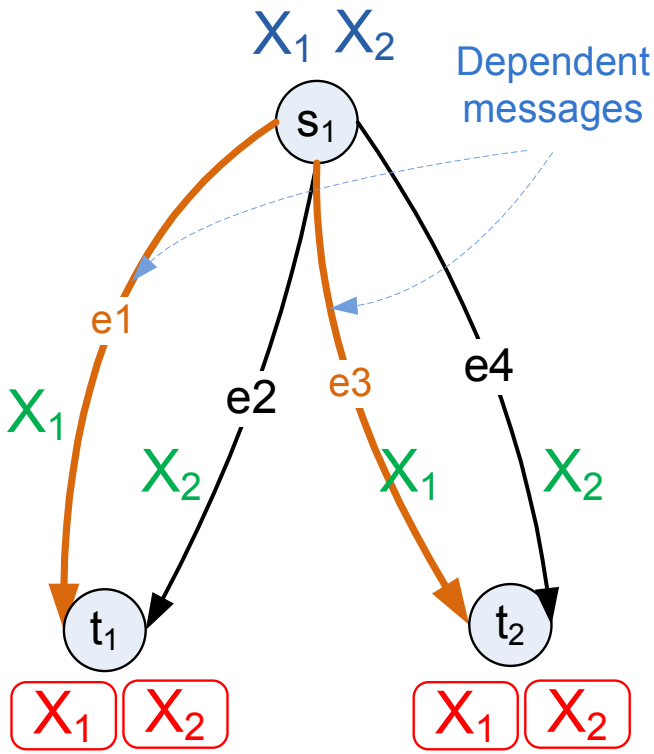
Question

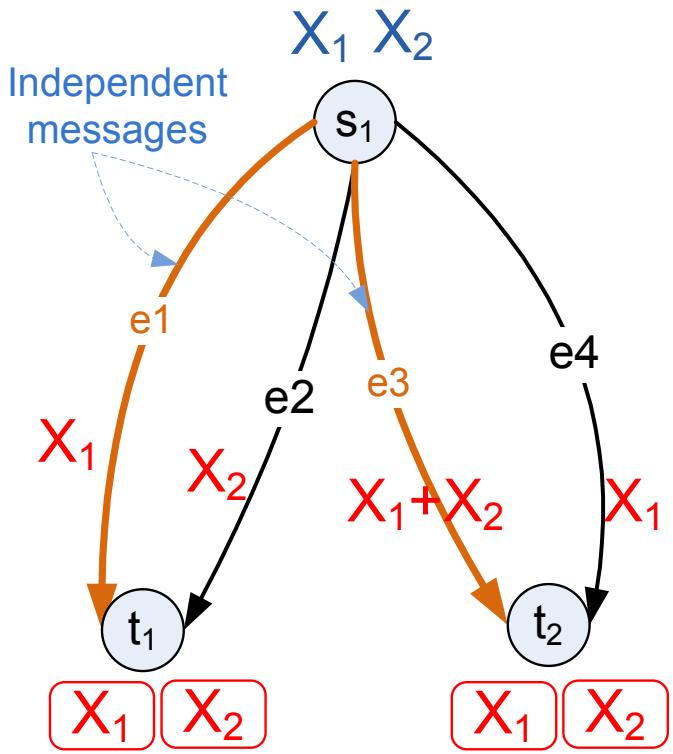
Do the dependency relations induced by a network always satisfy the three matroidal conditions?



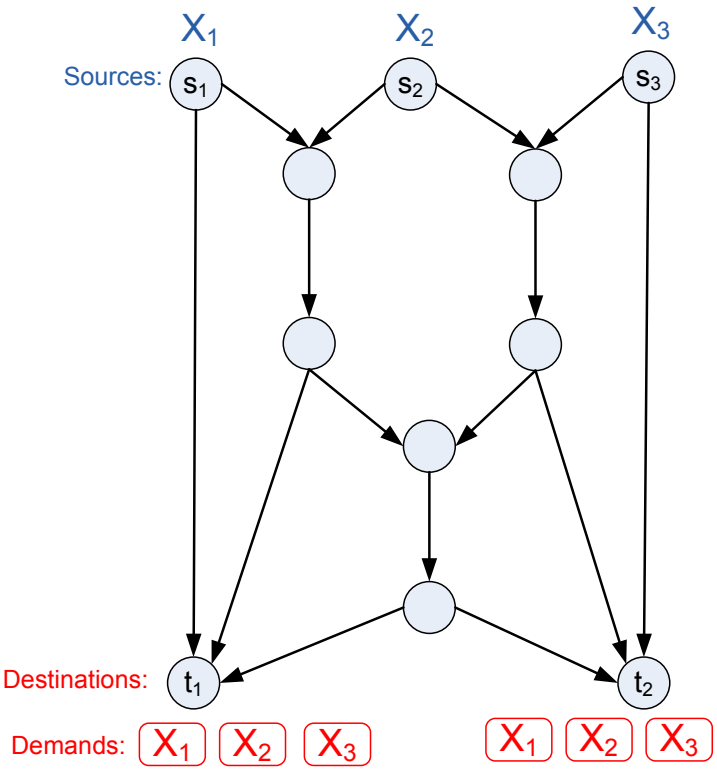
- Answer: No!
- This network does not dictate a priori the nature of the messages on edges e_1 and e_3
- $\{Y_{e_1}, Y_{e_3}\}$ can be either dependent or independent

Dependency Relations in Networks





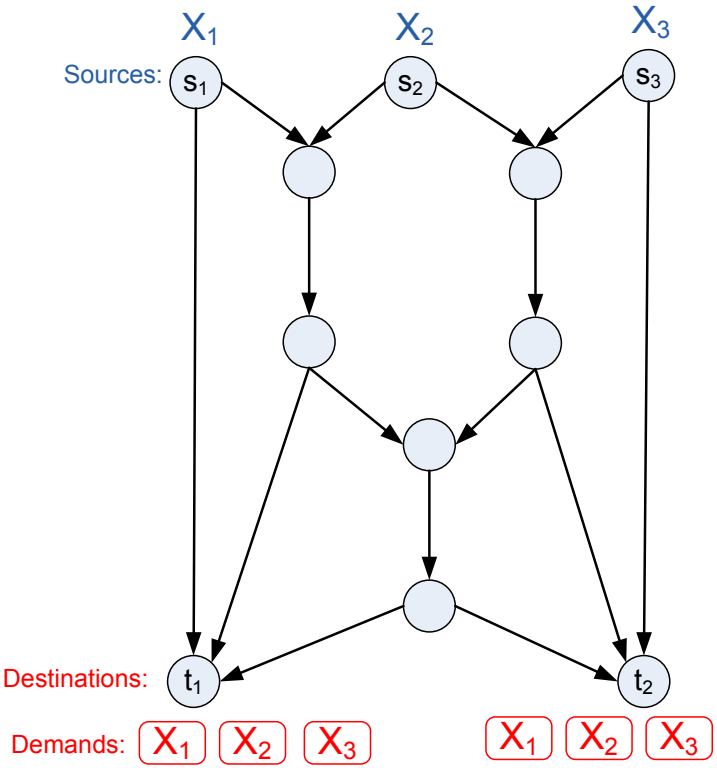
Network Model



A communication network $\mathcal{N}$ is modeled by:

- A graph $G(V, E)$
- Source nodes $s_1, s_2, \ldots$
- Messages $X = \{x\}$
  - Uniformly distributed over some finite alphabet $\mathcal{A}$
- Destination nodes $t_1, t_2, \ldots$ with demands
- Links are noise-free and interference-free

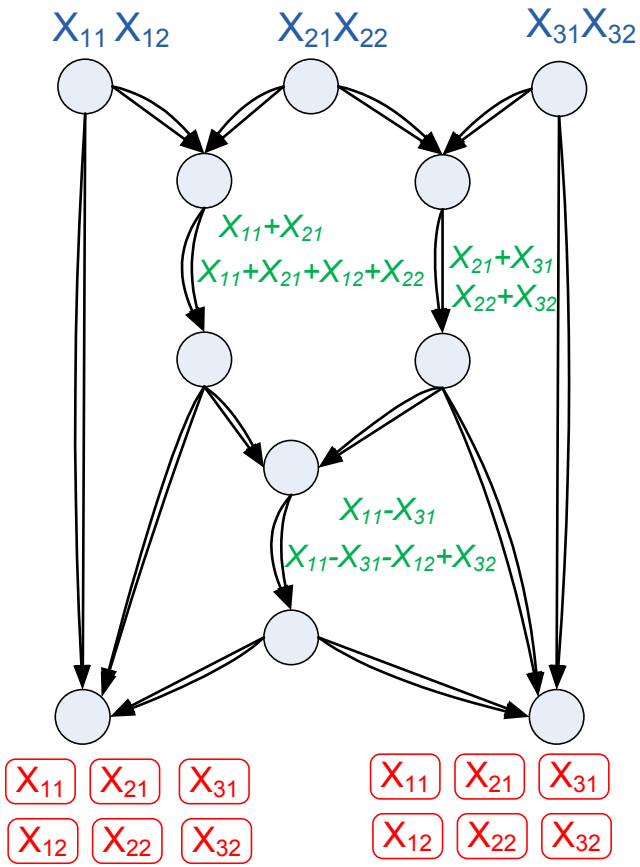
General Problem



Question

Is it possible to deliver all messages to the corresponding destinations?

Network Codes



Linear network code of dimension 2

- n - message dimensionality (each message has n symbols)
- k - source dimensionality
- A (k, n)-code - an assignment of encoding and decoding functions
- A $\frac{k}{n}$ - an achievable rate of the network (over some alphabet $\mathcal{A}$)
- Goal: maximize the achievable rate of the network

Lemma

Lemma

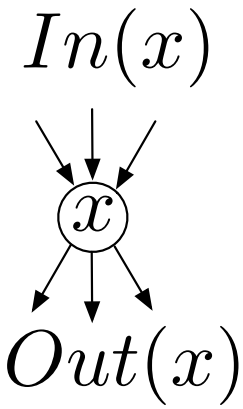
If a network has a (k, n) solution over alphabet $\mathcal{A}$ then, the following three conditions hold:

(N1) *(source rates)* $H(x) = k$[a] *for any* $x \in X$

(N2) *(edge capacities)* $H(x) \leq n$ *for any* $x \in E$

(N3) *(input/output functional dependencies) for any* $x \in V$

$$H(In(x)) = H(In(x) \cup Out(x))$$



[a] Entropies are computed using logarithms to base $|\mathcal{A}|$

- These conditions are referred to as network entropy conditions

Properties of the entropy

- For discrete random variables A, B, and C

$$H(A,C) + H(B,C) \geq H(C) + H(A,B,C)$$

- Key idea: work with a polymatroid assignment σ instead of the entropy function H

$$\sigma(A,C) + \sigma(B,C) \geq \sigma(C) + \sigma(A,B,C)$$

Lemma

Definition

Define a (k, n)-polymatroid assignment to a network $\mathcal{N}$ to be a map $\sigma : S \to \mathbb{R}$, $S = 2^{X \cup E}$ such that the following conditions hold:

(N1) (source rates) $\sigma(x) = k$ for any $x \in X$

(N2) (edge capacities) $\sigma((x) \leq n$ for any $x \in E$

(N3) (input/output functional dependencies) for any $x \in V$

$$\sigma(In(x)) = \sigma(In(x) \cup Out(x))$$

(P1) $\sigma(\emptyset) = 0$

(P2) If $A \subseteq B \subseteq S$, then $\sigma(A) \leq \sigma(B)$

(P3) If $A, B \subseteq S$, then $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$

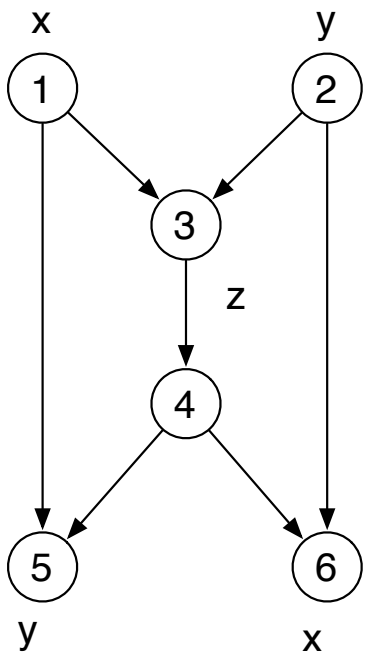
Polymatroid Assignments

- Polymatroid upper bound on the capacity of network $\mathcal{N}$

$$\sup\{\frac{k}{n} : \exists(k,n) \text{ polymatroid assignment to } \mathcal{N}\}$$

- If a network has a (k,n) coding solution over alphabet $\mathcal{A}$, then the network has a (k,n) polymatroid assignment.
- Since there may be many polymatroid assignments, polymatroid bounds might be larger than a bound obtained using entropy arguments.
- The polymatroid upper bound is the best upper bound on the network capacity obtainable using only Shannon-type informational inequalities

Example



$$2k = H(x) + H(y) =$$
$$= H(x, y) \leq H(x, y, z)$$
$$= H(x, y) \leq H(x) + H(y)$$
$$\leq k + n$$

The Rank Function of a Matroid

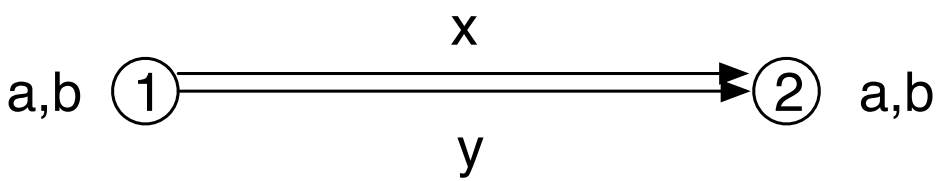
- Let (S, I) be a matroid with rank function r
  - For each $A \subseteq S$, $r(A)$ is the size of a base of $S|A$
- The rank function satisfies the following for all $A, B \subseteq S$:
  1. $0 \leq r(A) \leq |A|$
  2. If $A \subseteq B$, then $r(A) \leq r(B)$
  3. $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$

Matroidal Networks

- Let $\mathcal{N}$ be a network over graph $G(V, E)$ with message set X
- Let $M = (S, I)$ be a matroid with rank function r
- The network is referred to as matroidal associated with M if there exists a function $f : X \cup E \rightarrow$ such that
  1. f is one-to-one on X;
  2. $f(X) \subset I$
  3. $r(f(In(x))) = r(f(In(x) \cup Out(x)))$ for every $x \in V$

Example

- Consider the following network:



- Suppose we take matroid $U_{2,2}$ with ground set $\{1, 2\}$
  - We can use $f(a) = f(x) = 1$ and $f(b) = f(y) = 2$
- Suppose we take matroid $U_{2,3}$ with ground set $\{1, 2, 3\}$
  - We can use $f(a) = f(x) = 1$ and $f(b) = 2$ and $f(y) = 3$

Property of Matroidal Networks

Lemma

For any matroidal network, the polymatroid upper bound on the capacity is at least 1

Lemma

If a network is scalar-linearly solvable over some finite field, then the network is matroidal and the matroid is representable

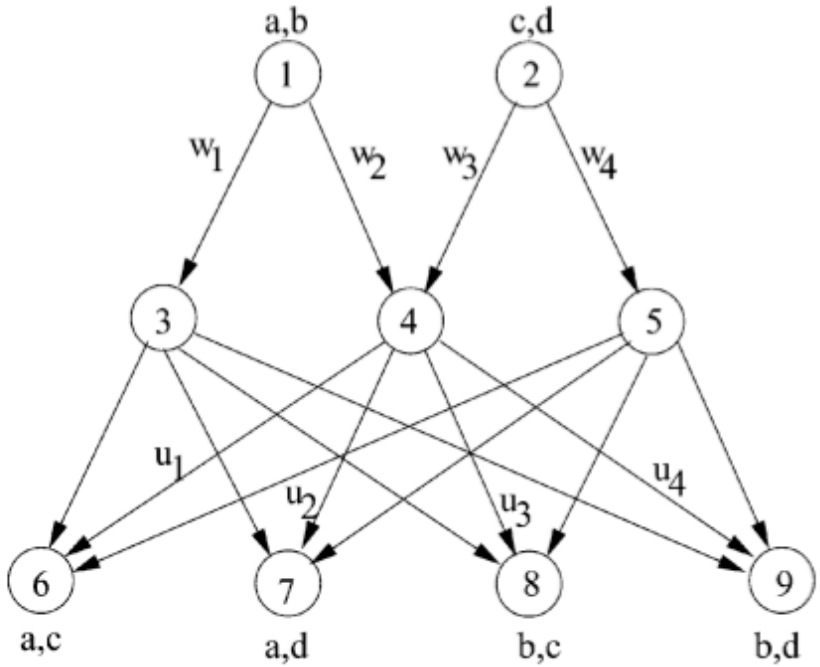
Corollary

All solvable multicast networks are matroidal.

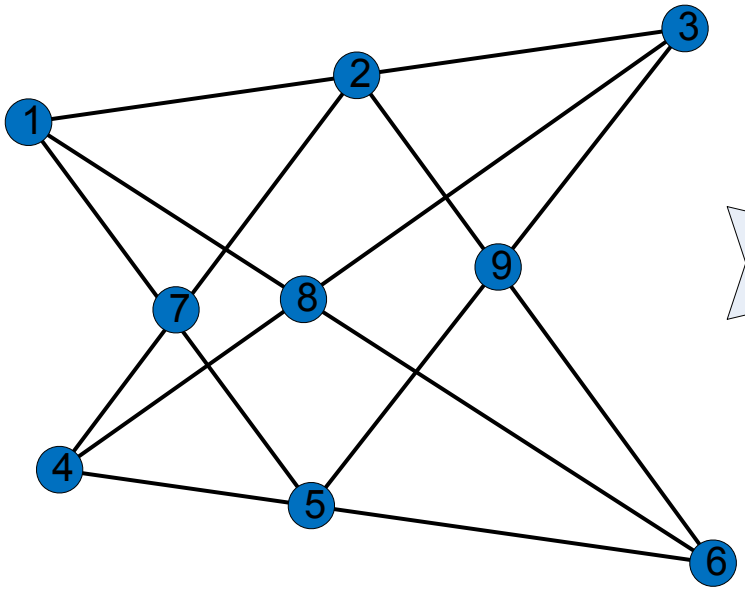
Example

Lemma

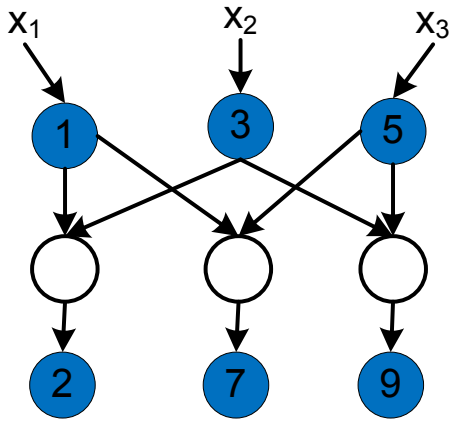
- *The M-network below is solvable, but not matroidal*
- *The network does not have any vector-linear solution of odd vector dimension*



Constructing Matroidal Networks

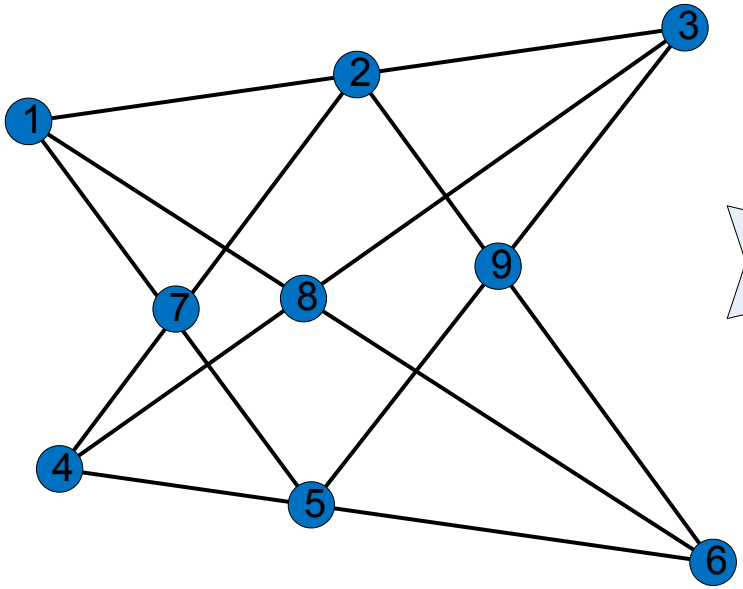


Non-Pappus Matroid

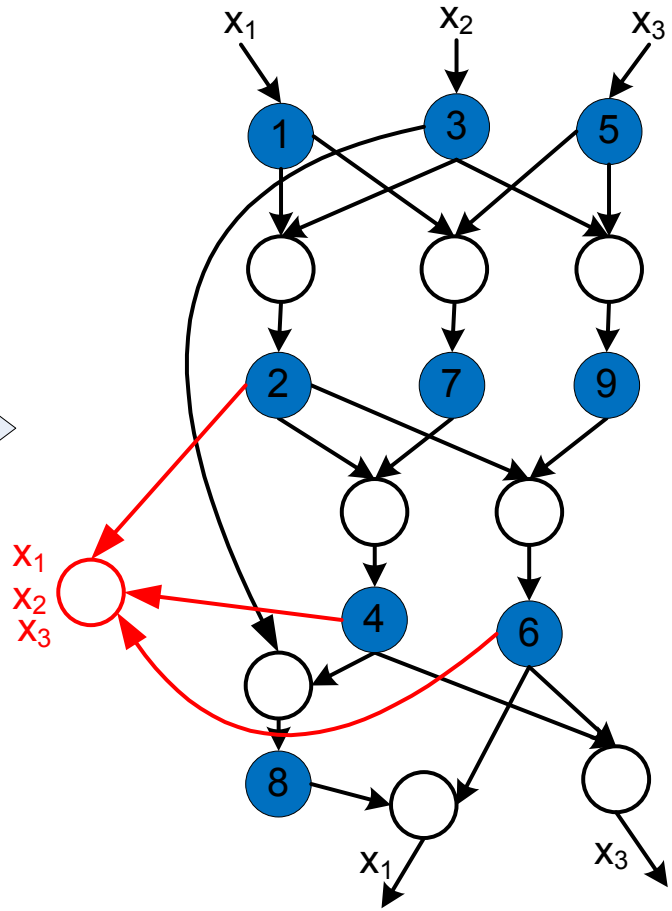


- Add intermediate nodes to mimic the dependency relations in the matroid

Constructing Matroidal Networks



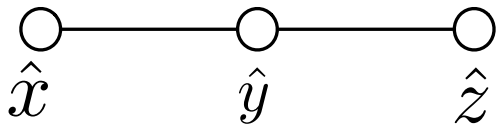
Non-Pappus Matroid



- Add intermediate nodes and destinations with specific demands chosen to reflect the dependency relations in the matroid.

Creating networks from matroids

- Start with rank-2 uniform matroid $U_{2,3}$
- Matroid has ground set $\{\hat{x}, \hat{y}, \hat{z}\}$

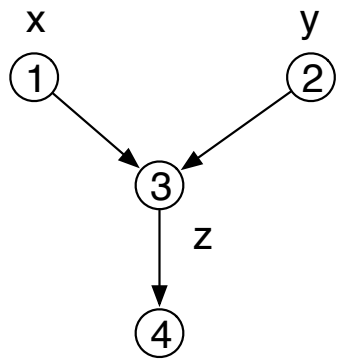


- Step 1: Choose a matroid base $B = \{\hat{x}, \hat{y}\}$ and network messages x and y and assign $f(x) = \hat{x}$ and $f(y) = \hat{y}$

x ① y ②

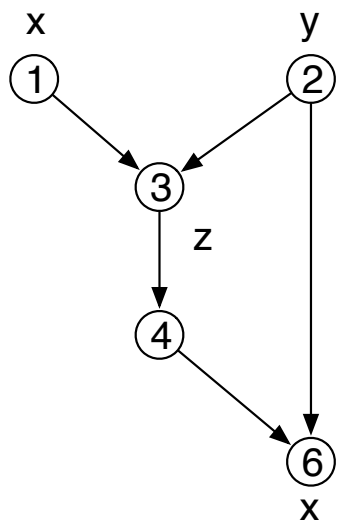
Example (cont.)

- Step 2.
  - Choose circuit is $\{\hat{x}, \hat{y}, \hat{z}\}$, with $\hat{x}, \hat{y}$ already defined,
  - add nodes n_3 and n_4
  - define $f(e_{1,3}) = \hat{x}$, $f(e_{2,3}) = \hat{y}$, $f(e_{3,4}) = \hat{z}$



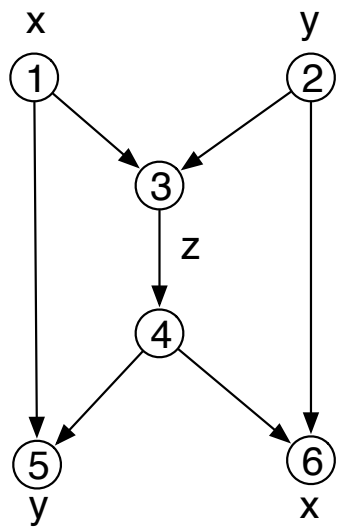
Example (cont.)

- Step 3.
  - Choose circuit is $\{\hat{x}, \hat{y}, \hat{z}\}$, with $\hat{x}$ is an image of a source node with message x.
  - Add a new receiver node n_6 which demands x



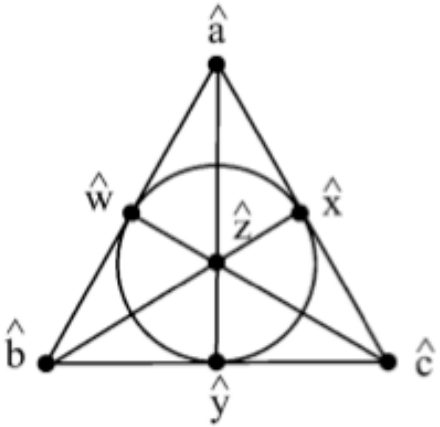
Example (cont.)

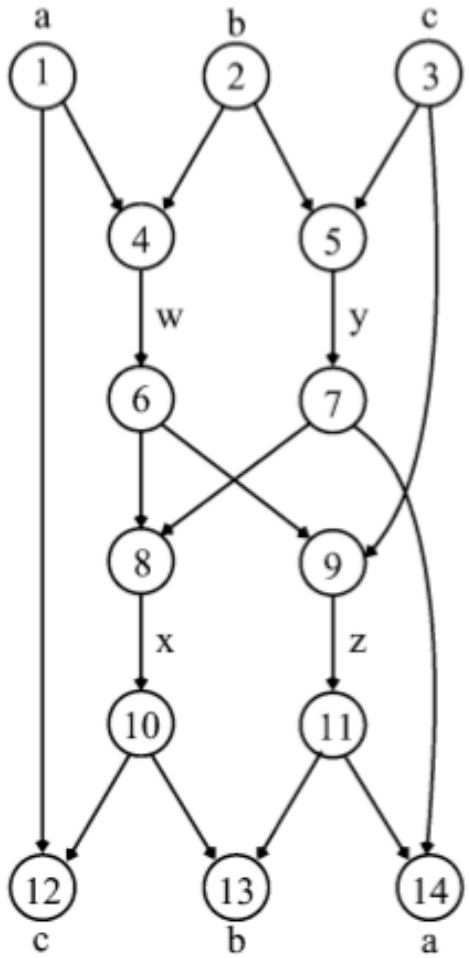
- Step 4.
  - Choose circuit is $\{\hat{x}, \hat{y}, \hat{z}\}$, with $\hat{y}$ is an image of a source node with message y.
  - Add a new receiver node n_5 which demands y



Fano network

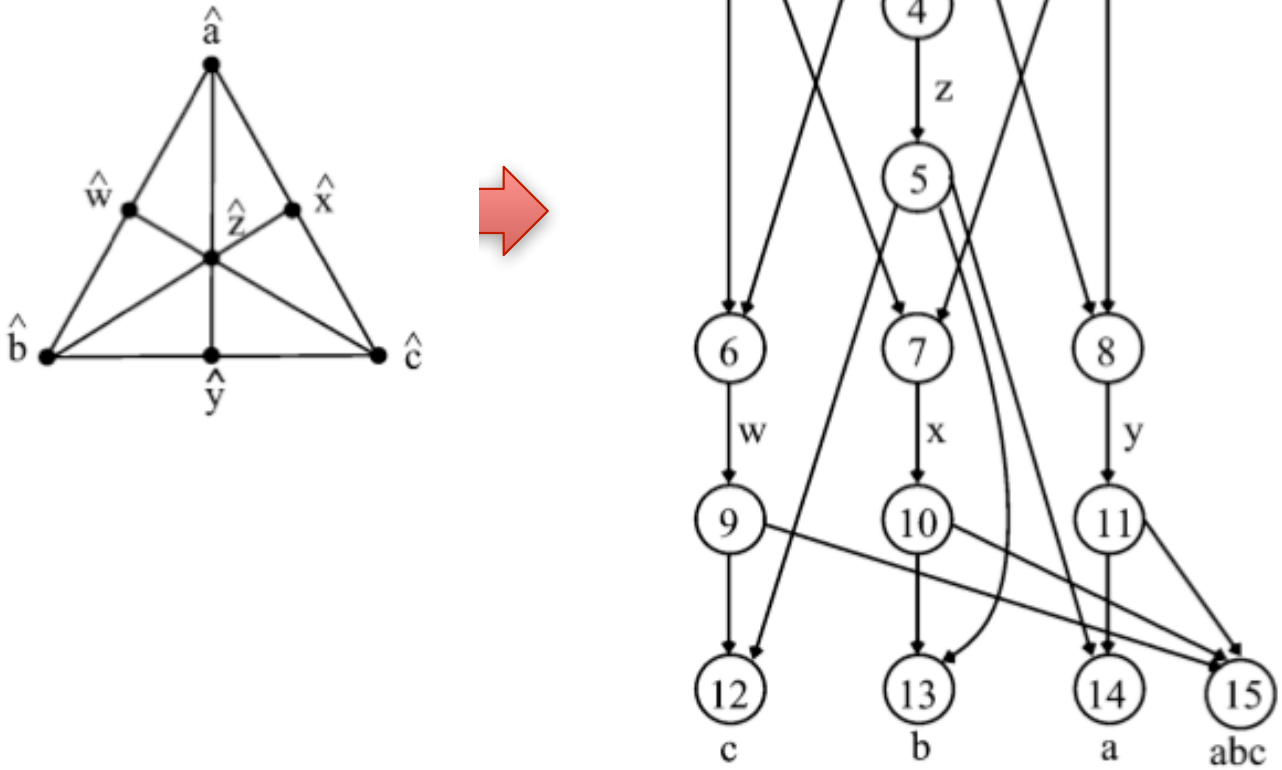
- Obtained from Fano matroid





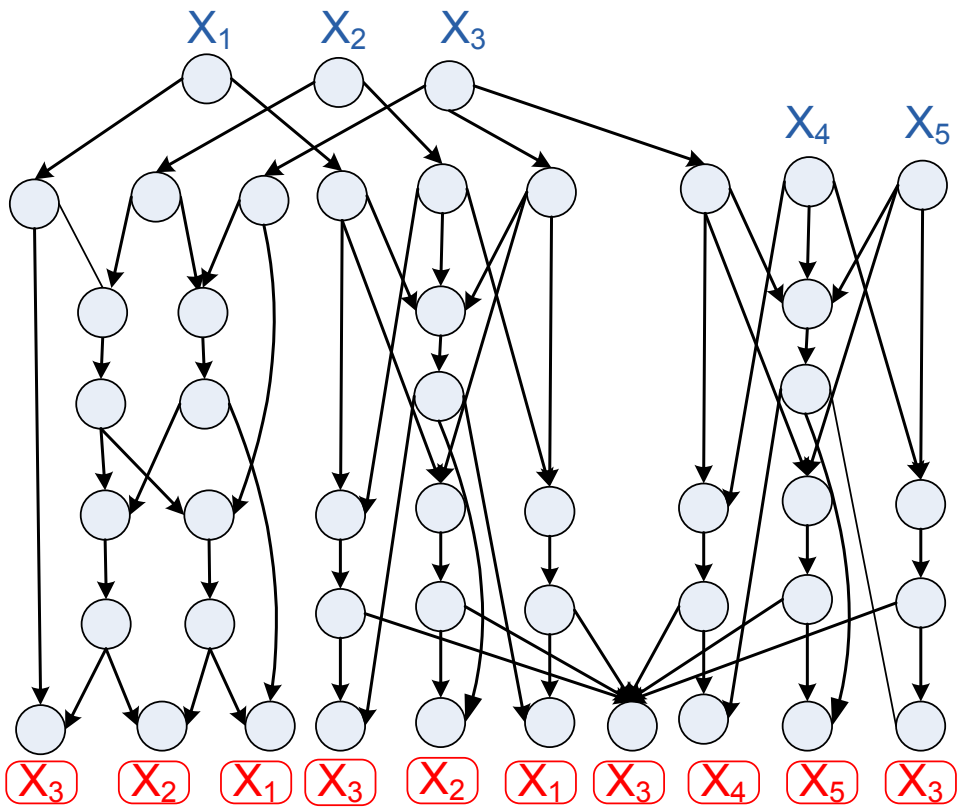
Non-Fano network

- Obtained from Non-Fano matroid



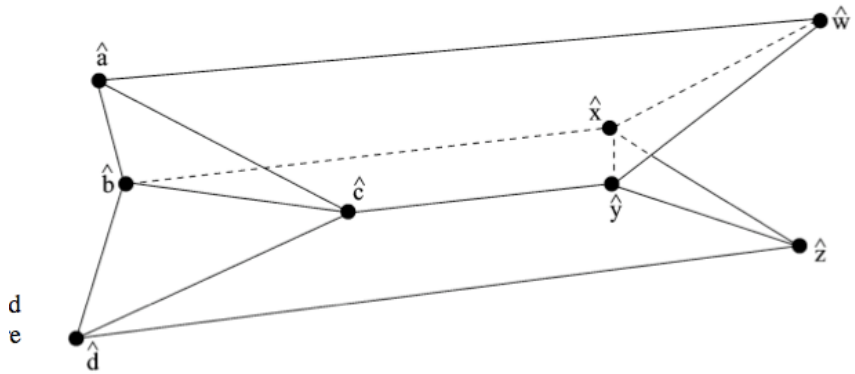
Linear vs. Non-Linear

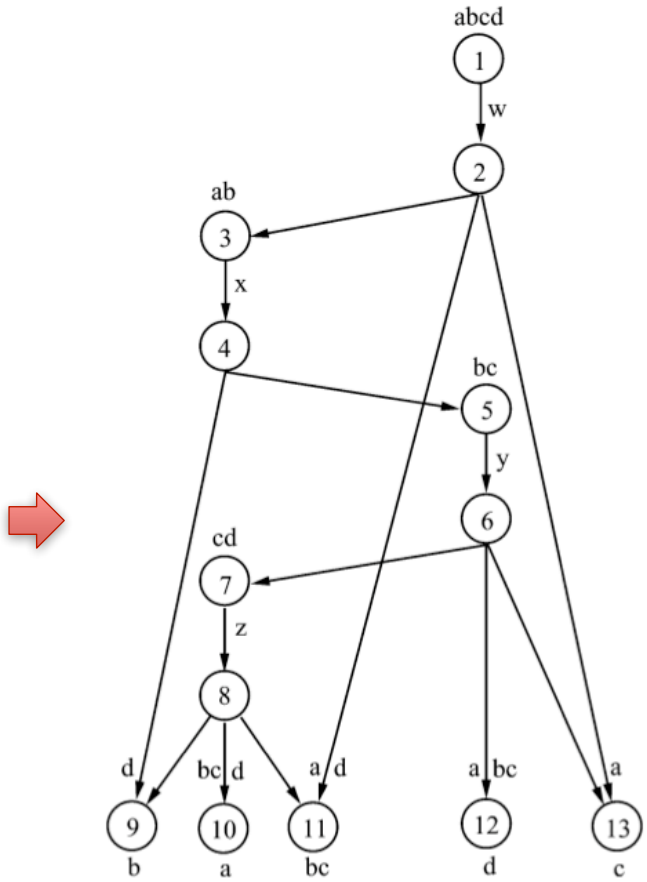
- The network on the left does not admit any scalar or vector linear code over any field
- But, it has a non-linear one over an alphabet of size 4.
- Hence, linear network codes are not sufficient



Vamos network

- Vamos network is not representable





Property of Vamos Network

Theorem

The polymatroid upper bound on the coding capacity of the Vamos network is 1

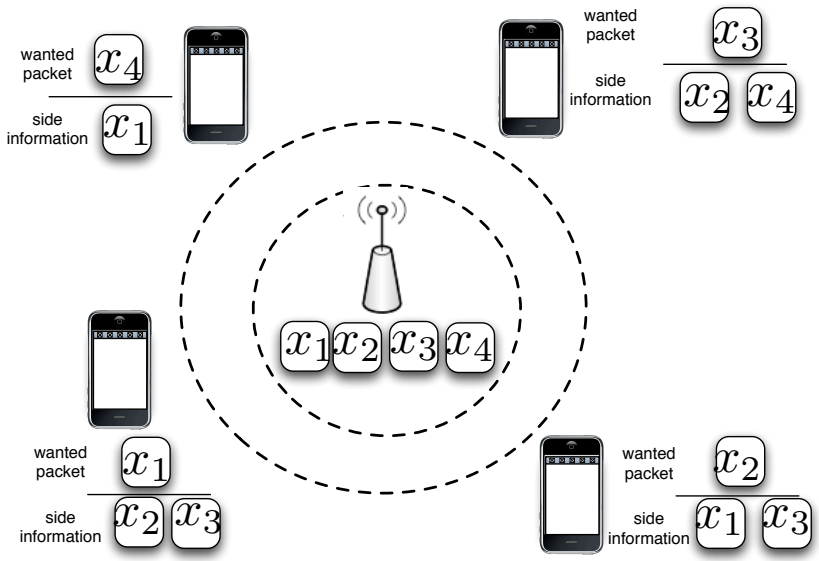
Best upper bound that can be obtained by using Shannon-type inequalities

Theorem

The coding capacity of the Vamos network is at most 10/11.

Obtained by using non-Shannon inequalities

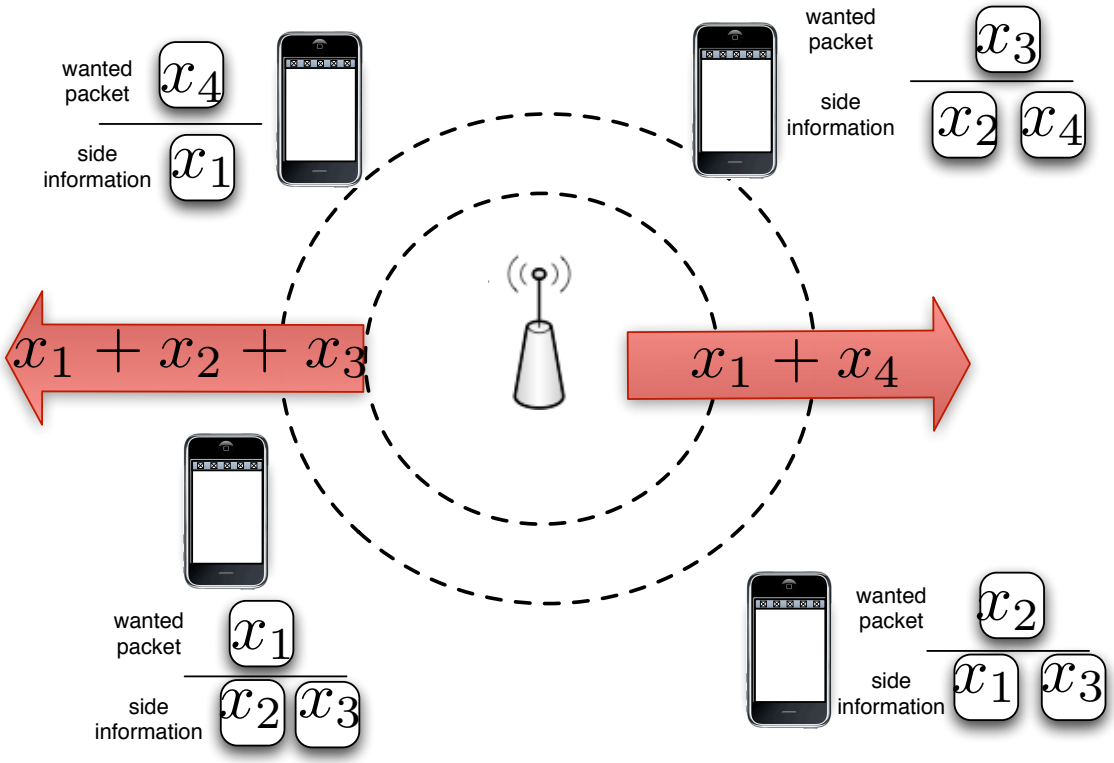
Index Coding Problem



Find a code that will satisfy the demands of all receivers with the minimum possible number of transmissions.

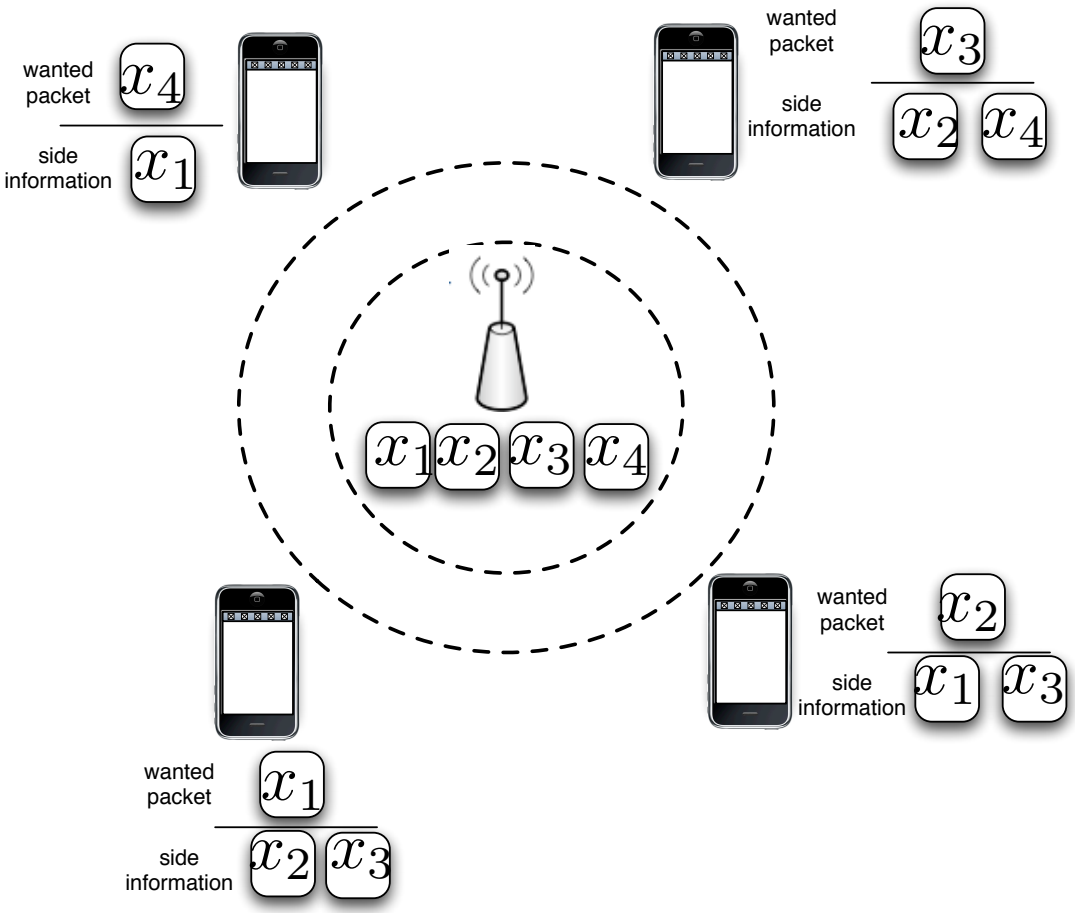
Y. Birk and T. Kol, *" Coding-on-demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients,"* INFOCOM 98.

Optimal Index Code



- $l = 2$

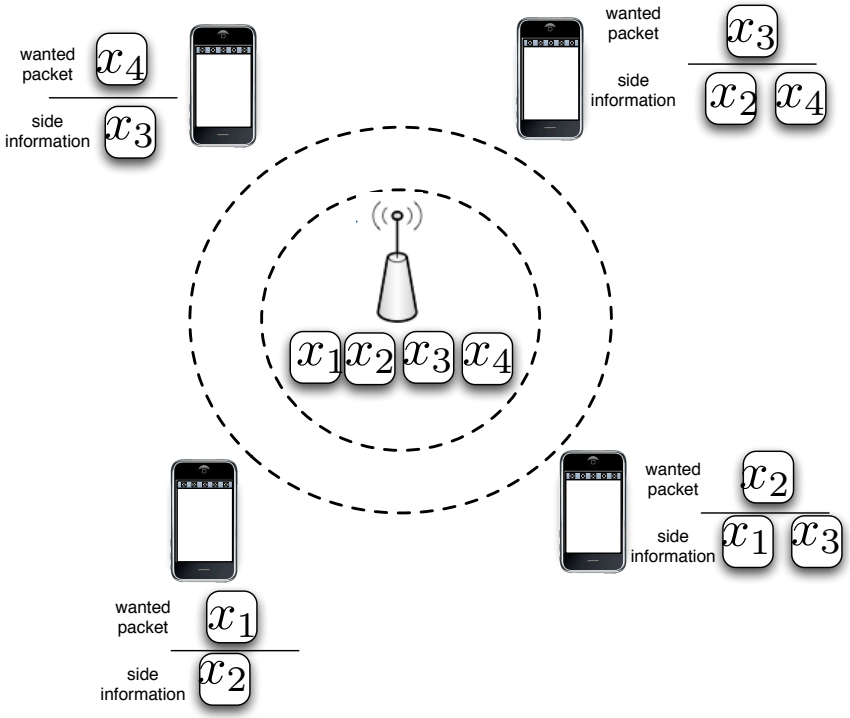
Corresponding Min-Rank Problem

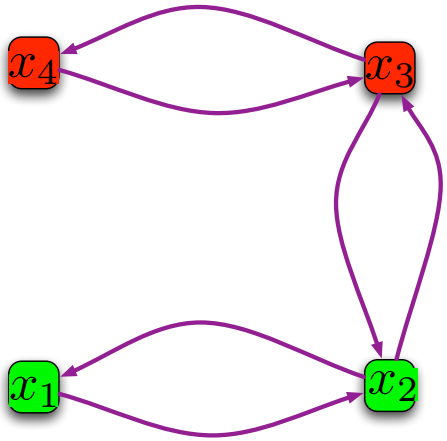


	x_1	x_2	x_3	x_4
x_1	1	X	X	0
x_2	X	1	X	0
x_3	0	X	1	X
x_4	X	0	0	1

don't care

Side-information graph G





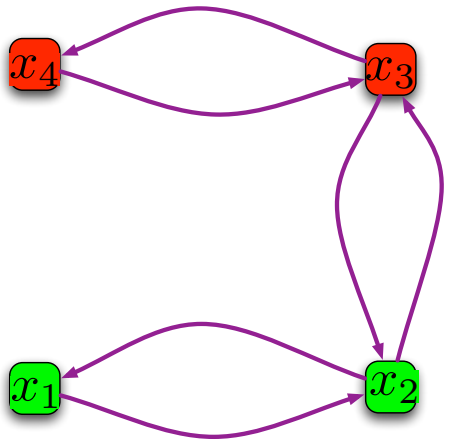
- (i, j) is an edge iff R_i knows the value of x_i

Index Code

- An index code of length l for G is
  - An encoding function $E : \{0,1\}^n \to \{0,1\}^l$
  - Decoding functions $D_1, \ldots, D_n$ so that $\forall i \in [n]$, $\forall x \in \{0,1\}^n$:

$$D_i(E(x), x|_{N_G^+(i)}) = x_i,$$

where $N_G^+(i)$ are out-neighbors of R_i in G



Scalar linear codes

	x_1	x_2	x_3	x_4
x_1	1	X	X	0
x_2	X	1	X	0
x_3	0	X	1	X
x_4	X	0	0	1

- $$OPT \leq \min_{H \subset G} rank_2(A_H + I) =: minrk_2(G)$$
- $minrk_2(G)$ - the optimal size of scalar linear code

Theorem (Lubetzky and Stav, 2007)

Theorem

- For any $\varepsilon > 0$ and sufficiently large n there exists a graph G on n vertices such that:
  - Any linear index code for G requires $n^{1-\varepsilon}$ bits
  - There exists a non-linear index code for G using n^{ε} bits
- Moreover, G is undirected and can be constructed explicitly.

- Proof techniques
  - Use the fact that codes over high-order fields may result in fewer transmissions
  - Use Ramzey graphs for the construction

1

[1] Lubetzky, E. and Stav, U. 2007. Non-Linear Index Coding Outperforming the Linear Optimum. In Proceedings of the 48th FOCS 161-168.

Proof (scketch)

- Need to find a graph such that $minrk_2(G)$ is "large" and $l(G)$ is "small"
- Idea: Use higher order fields:
  - Consider $A(a_{ij})$ representing G over $\mathbb{F}$
  - Encode Ax using $\lceil rank_{\mathbb{F}}(A) \log_2 |\mathbb{F}| \rceil$ bits
  - Decoding:

$$a_{ii}^{-1}(Ax)_i = x_i + a_{ii}^{-1} \sum_{j \in N_G^+(i)} a_{ij} x_j$$

  - $l(G) \leq \lceil minrk_{\mathbb{F}}(G) \log_2 |\mathbb{F}| \rceil$

	x_1	x_2	x_3	x_4
x_1	1	X	X	0
x_2	X	1	X	0
x_3	0	X	1	X
x_4	X	0	0	X

Proof (scketch)

- Property of minrank:

$$minrk_2(G)minrk_2(\bar{G}) \geq n$$

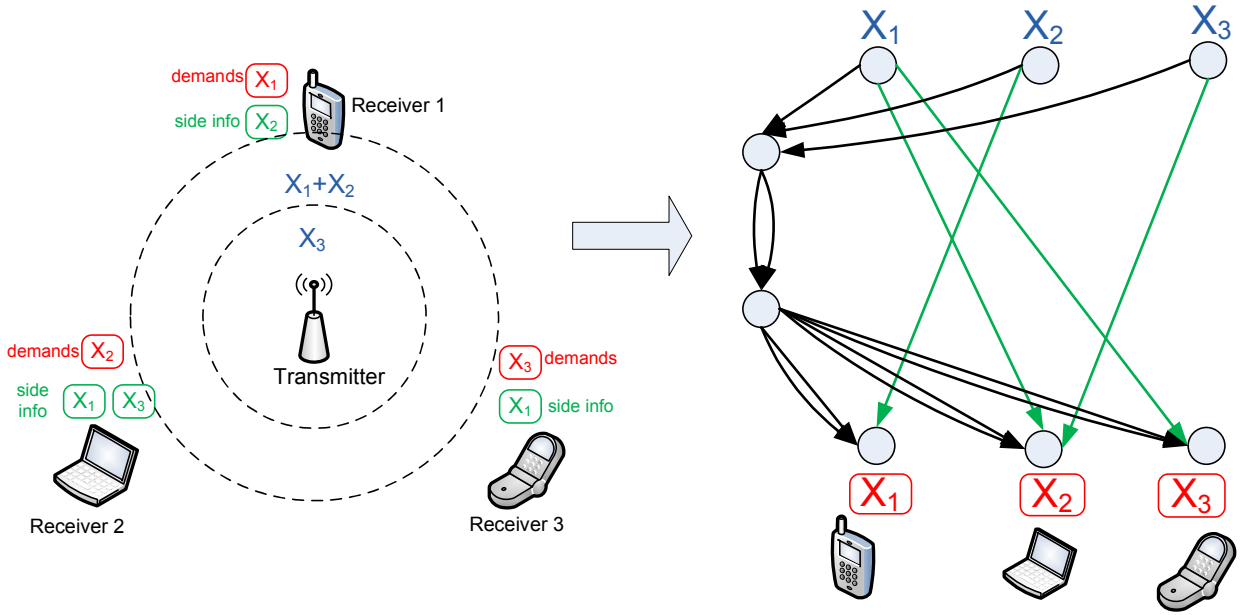
  where $\bar{G}$ is a complimentary graph
- This implies that we need to find G such that $minrk_2(\bar{G})$ is small and $minrk_{\mathbb{F}}$ is "small"
- Such G is a Ramsey graph
  - Use a construction from [Alon 98]

Theorem

Theorem

- For any $\varepsilon > 0$ and sufficiently large n there exists a graph G on n vertices such that:
  - Any linear index code for G over some field $\mathbb{F}$ requires $\sqrt{n}$ bits
  - There exists a non-linear index code for G using n^{ε} bits
- Moreover, G is undirected and can be constructed explicitly.

Equivalence to Linear Network Coding



Theorem

Given a network $\mathcal{N}$ with m edges, there exists an instance of the Index Coding problem $\mathcal{I}(\mathcal{N})$ such that $\mathcal{N}$ admits a vector linear network code of dimension n over $GF(q)$ iff $\mathcal{I}(\mathcal{N})$ has an optimal linear index code with the same properties and consisting of nm transmissions.

S. El Rouayheb, S. and C. N. Georghiades, *"On the Relation Between the Index Coding and the Network Coding Problems,"* ISIT, 2008

Back to Matroids

- R. Dougherty,C. Freiling, K. Zeger used this idea to construct networks from matroids [2]
- However the obtained network will not necessarily reflect all the dependency relations of the matroid.

Question

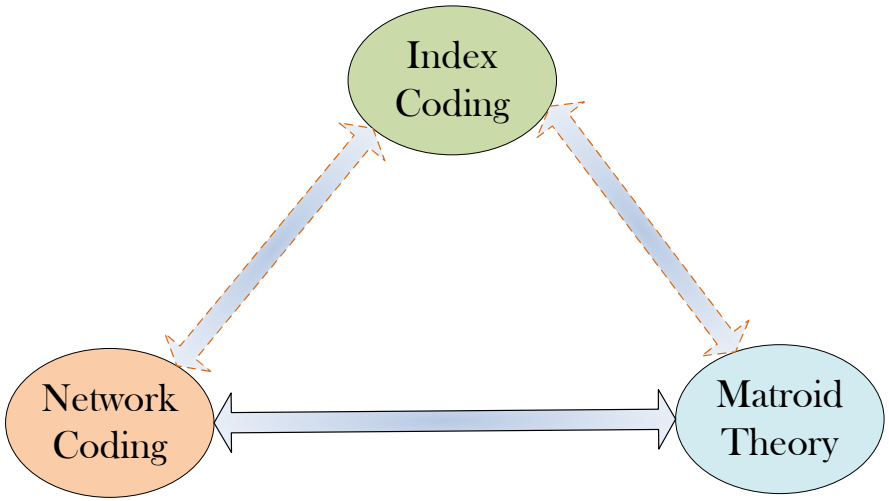
Given a matroid, can we build a network that reflects all the dependencies AND independencies in the matroid?

- If so, then a linear representation of the matroid will give a linear network code for the network, and vice versa

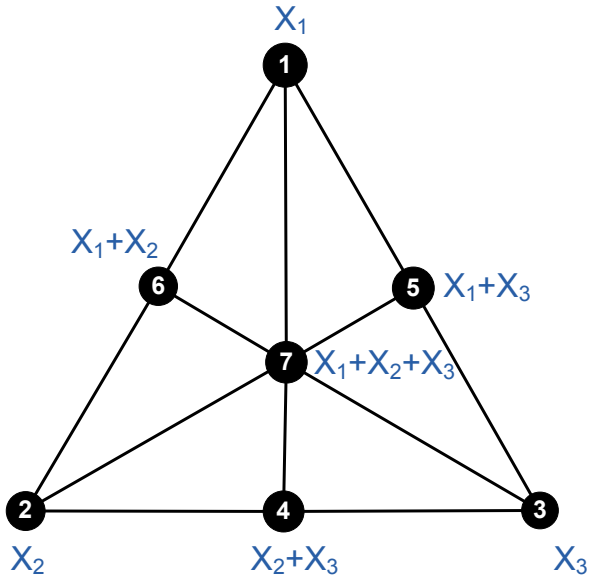
[2] R. Dougherty,C. Freiling, K. Zeger, *"Networks, Matroids, and Non-Shannon Information Inequalities,"* Trans. Inf. Th., 07

Back to Matroids

- Given a matroid, we construct a network whose dependency relations satisfy the given matroidal constraints.
- As a result, we obtain a reduction that links the existence of vector linear codes for networks to the multilinear representation properties of matroids.
- An important intermediate step in this reduction is the connection to Index Coding.



Linear Representation of Matroids



Linear Representation of the Non-Fano Matroid over $GF(3)$.

X_1, X_2, X_3 canonical basis of $GF(3)^3$

Definition

A matroid $\mathcal{M}(E, \mathcal{I})$ of rank k is linearly representable over a field $\mathbb{F}$ if

- There exists a set S of vectors in $\mathbb{F}^k$
- And a bijection $\phi : E \to S$ s.t. $\forall A \subseteq E$, $A \in \mathcal{I} \Leftrightarrow \phi(A)$ is linearly independent

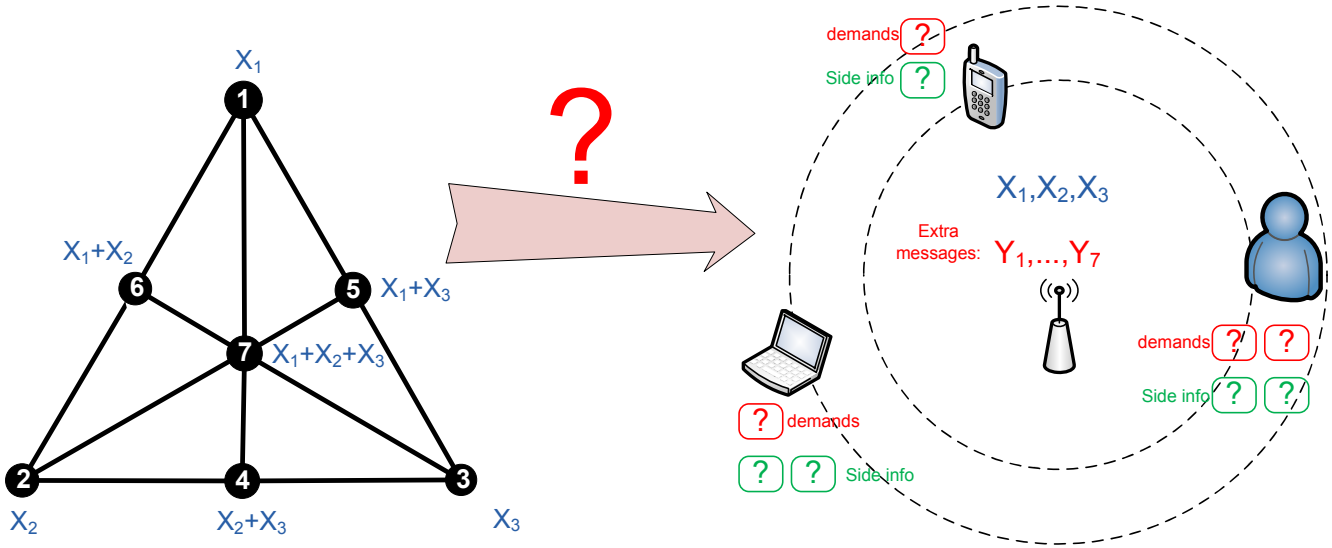
Main Theorem

- Given a matroid, we build a network that reflects ALL the matroid dependencies and independencies
- Let $\mathcal{M}(Y, \mathcal{I})$ be a matroid
- We construct an instance of the Network Coding problem $\mathcal{N}(\mathcal{M})$ s.t.

Theorem

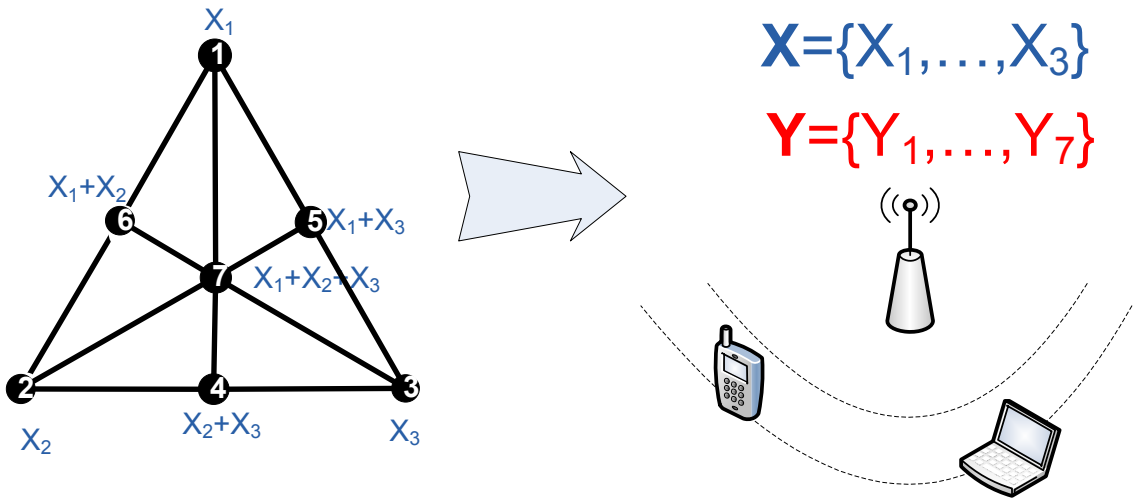
The network $\mathcal{N}(\mathcal{M})$ has a vector linear network code of dimension n over $GF(q)$ iff the matroid $\mathcal{M}$ has an n-linear representation over the same field.

Proof Idea



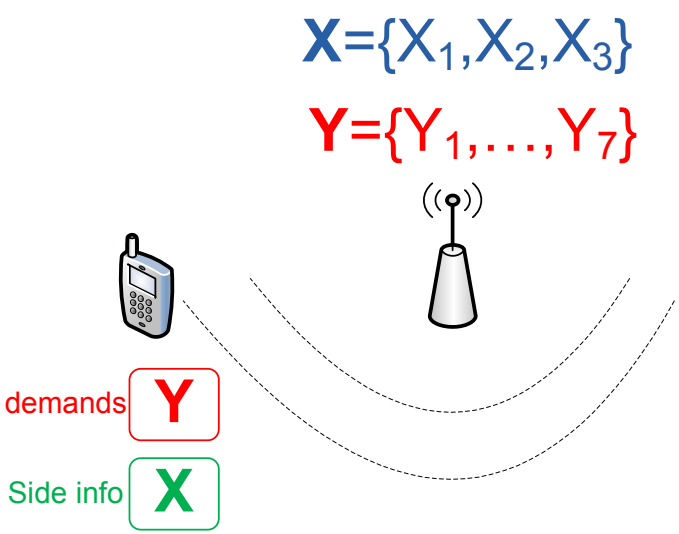
- Focus on the equivalent Index Coding formulation
- Add extra messages in the Index Coding problem to gain more degrees of freedom

Proof Outline: Transmitter



- Let $\mathcal{M}(Y, r)$ be a matroid of rank k where $Y = \{Y_1, \ldots, Y_m\}$
- In the equivalent Index Coding Problem, the transmitter has two sets of messages
  1. $X = \{X_1, \ldots, X_k\}$ corresponding to the matroid representation
  2. $Y = \{Y_1, \ldots, Y_m\}$ extra messages corresponding to the matroid ground set

Proof Outline: Diagonal Form

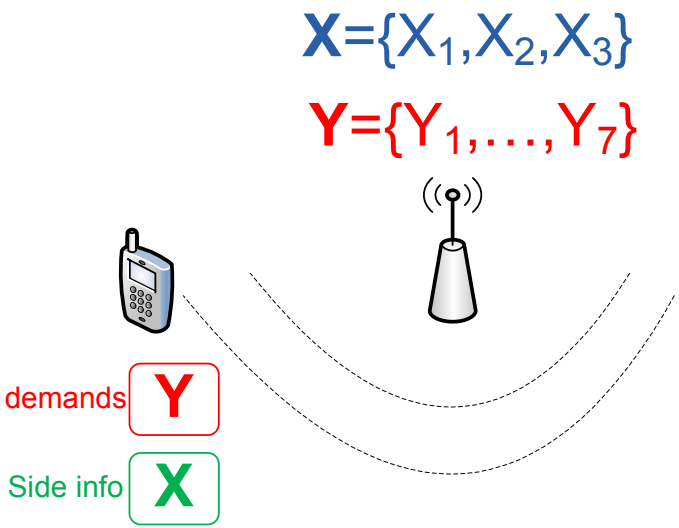


Optimal Index Code:

$$g_1(X,Y) = a_{11}X_1 + a_{12}X_2 + a_{13}X_3 + b_{11}Y_1 + \cdots + b_{17}Y_7$$
$$g_2(X,Y) = a_{21}X_1 + a_{22}X_2 + a_{23}X_3 + b_{21}Y_1 + \cdots + b_{27}Y_7$$
$$\vdots$$
$$g_7(X,Y) = a_{71}X_1 + a_{72}X_2 + a_{73}X_3 + b_{71}Y_1 + \cdots + b_{77}Y_7$$

- We add a receiver having the set X as side info and demanding the messages in Y
- A lower bound on the number of transmissions is then $|Y| = 7$
- This receiver is able to decode Y iff Matrix $[a_{ij}]$ is invertible

Proof Outline: Diagonal Form



Optimal Index Code:

$$g_1'(X,Y) = Y_1 + \underbrace{c_{11}X_1 + c_{12}X_2 + c_{13}X_3}_{f_1(X)}$$

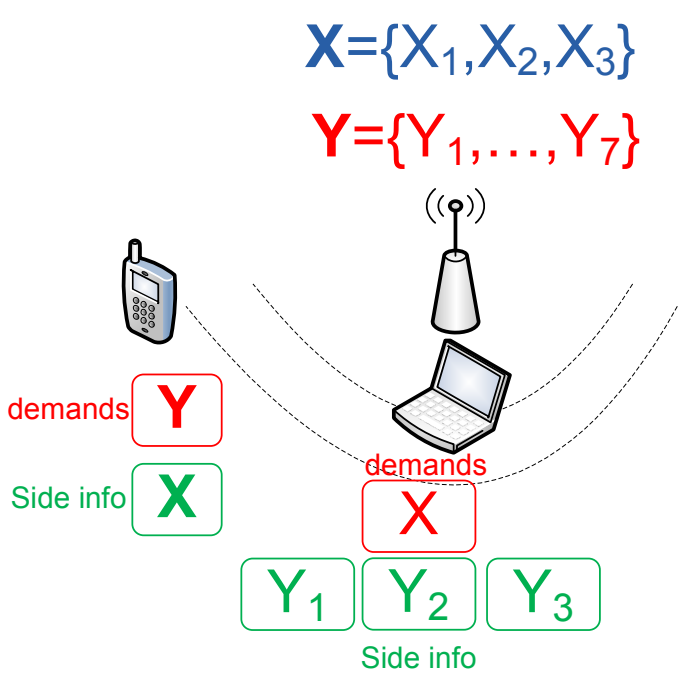
$$g_2'(X,Y) = Y_2 + \underbrace{c_{21}X_1 + c_{22}X_2 + c_{23}X_3}_{f_2(X)}$$

$$\vdots$$

$$g_7'(X,Y) = Y_7 + \underbrace{c_{71}X_1 + c_{72}X_2 + c_{73}X_3}_{f_7(X)}$$

- We want to show that the functions $f_i(X)$ give a linear representation of the matroid

Proof Outline: Independent Sets

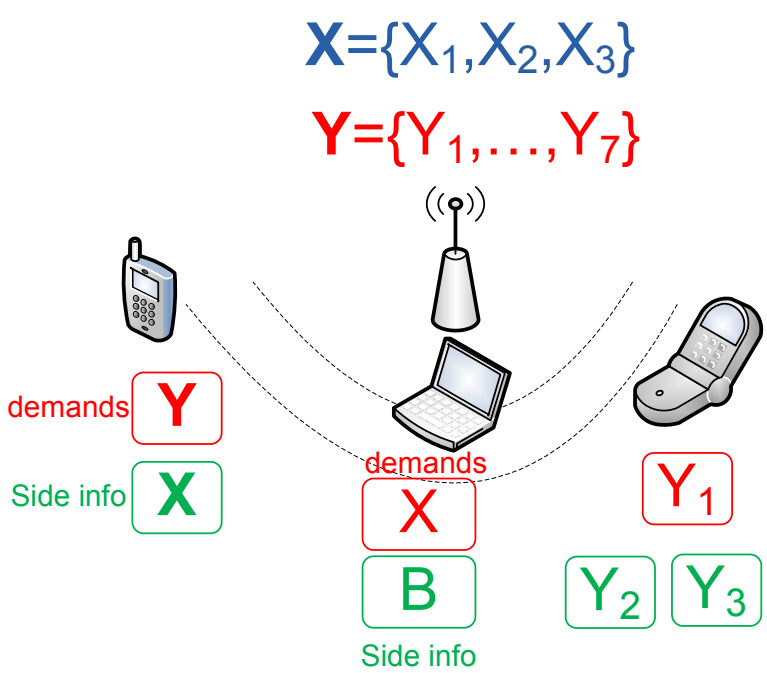


Index Code:

$X_1 + f_1(X)$
$X_2 + f_2(X)$
$X_3 + f_3(X)$
.
.
.
$Y_7 + f_7(X)$

- Let $B = \{Y_1, Y_2, Y_3\} \subseteq Y$ be a base
- The corresponding receiver can get $f_1(X), f_2(X), f_3(X)$ from the transmitted signals
- He can decode the X's iff $f_1(X), f_2(X), f_3(X)$ are linearly independent

Proof Outline: Dependent Sets

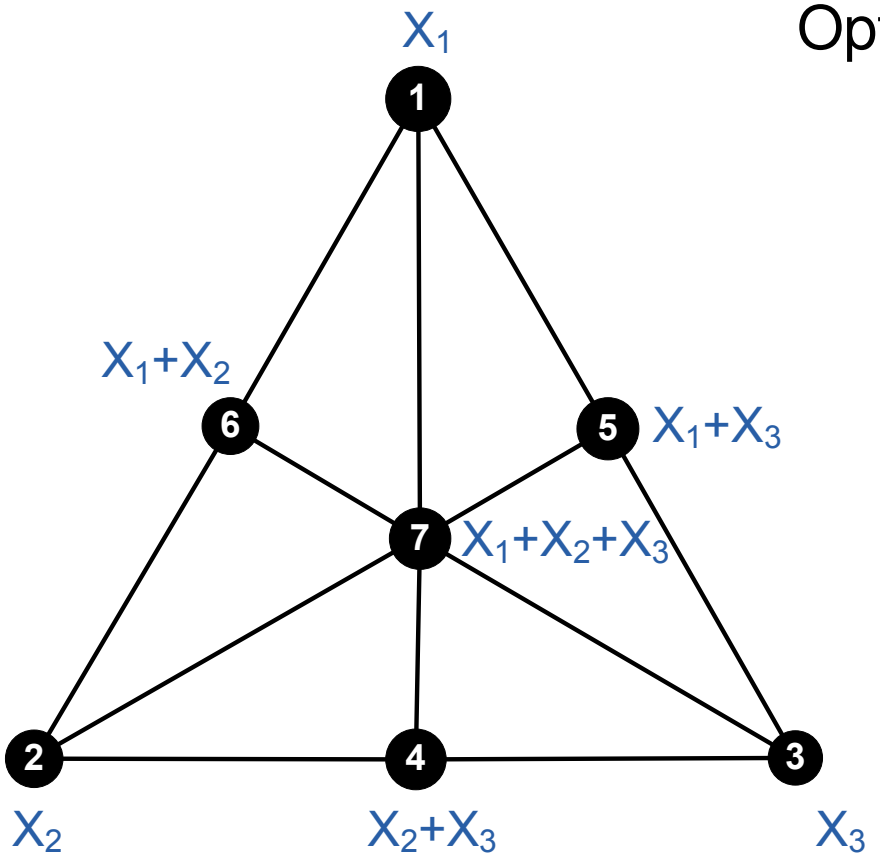


Index Code:

$Y_1 + f_1(X)$
~~Y_2~~ $+ f_2(X)$
~~Y_3~~ $+ f_3(X)$
.
.
.
$Y_7 + f_7(X)$

- $C \subseteq Y$ is a dependent set.
- For example, let $C = \{Y_1, Y_2, Y_3\}$
- The corresponding receiver can decode $f_2(X)$ and $f_3(X)$
- He can decode Y_1 only iff $f_1(X)$ is a linear combination of $f_2(X)$ and $f_3(X)$

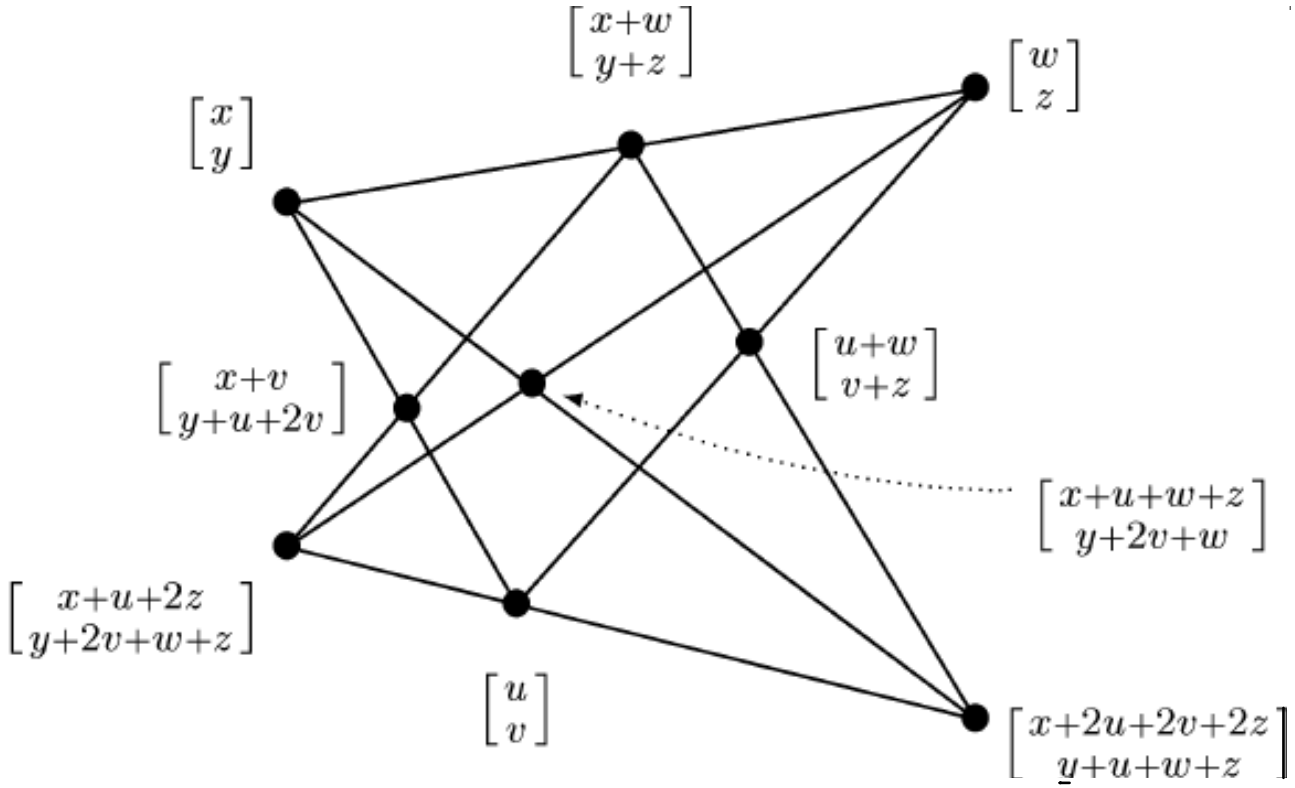
Example



Optimal Index Code:

$$Y_1 + X_1$$
$$Y_2 + X_2$$
$$Y_3 + X_3$$
$$Y_4 + X_2 + X_3$$
$$Y_5 + X_1 + X_3$$
$$Y_6 + X_1 + X_2$$
$$Y_7 + X_1 + X_2 + X_3$$

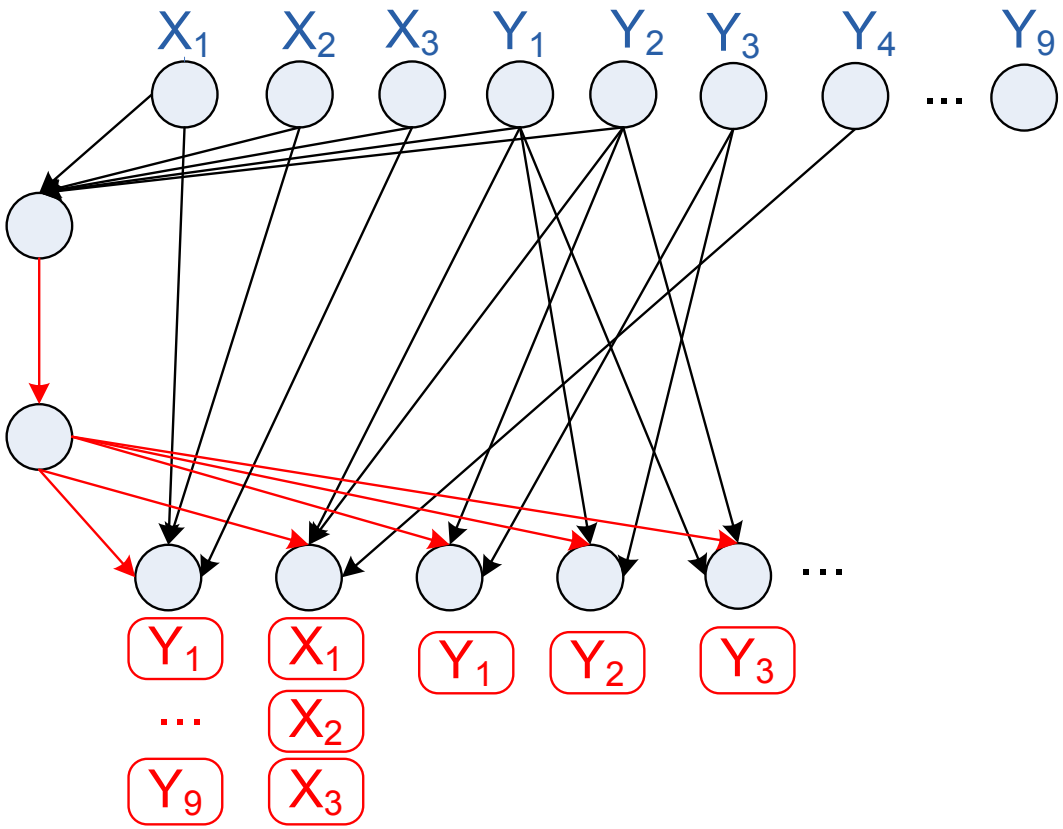
Example: The Non-Pappus Matroid



The Non-Pappus matroid is not linearly representable but has a 2-linear representation over $GF(3)$

F. Matus, *"Matroid representations by partitions"*, Discrete Mathematics, 1999

Example: The Non-Pappus Network



The Non-Pappus network does not have a scalar linear network code but a vector linear one of block length 2 over $GF(3)$.

Conclusion

- There exist connections Matroid theory, Index Coding, and Network Coding
- Open problems:
  - What is the exact capacity of the Vamos netork?
  - Is the coding capacity of the Vamos network strictly greater than its linear coding capacity.
  - Are there other structures that would be more suitable to capture the dependency/independency relations in the netoworks
    - ⋆ Such as FD-relations