Network Codes and Groups

Babak Hassibi

Joint work with Sormeh Shadbakht, Wei Mao and Matthew Thill

Department of Electrical Engineering
California Institute of Technology, Pasadena, CA 91125

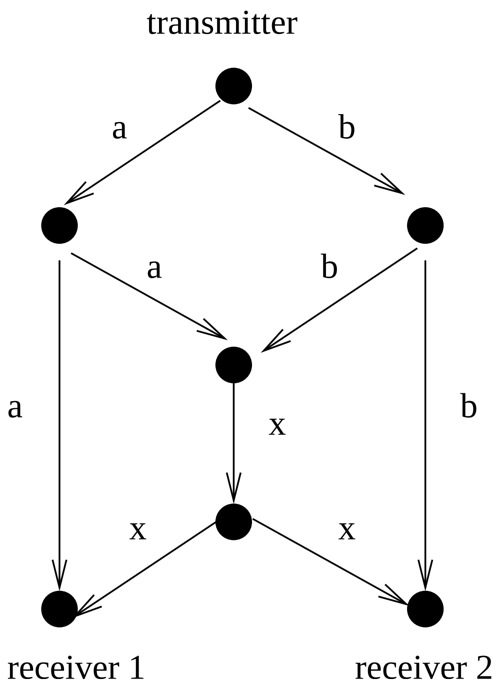
Workshop on Algebraic Structure in Network Information Theory

Banff International Research Station, August 18, 2011

Outline

- **Insufficiency of Linear Network Codes**
- **Entropy Vectors**
- **Group Network Codes**
  - Ingleton-violating groups
  - partitions and Monte Carlo Markov chain methods

Network Coding

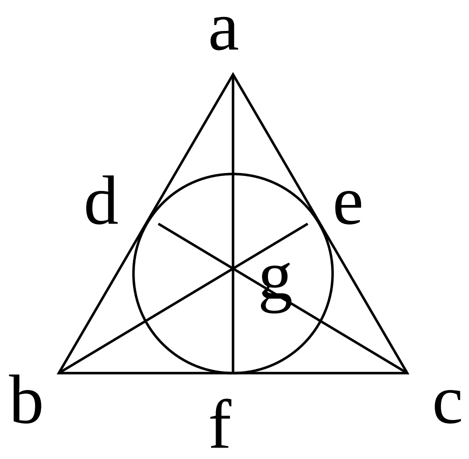


- combine symbols to improve on the routing capacity
- combining a and b via modulo-2 addition, $x = a + b$, increases the capacity to 2 bits (over the 1.5 bits achieved by routing)
- *linear network coding:* the symbols belong to a finite field and nodes perform linear operations (**Is this sufficient?**)

Matroids

- A matroid $\mathcal{M}$ consists of a ground set $\mathcal{G}$ and a rank function $r(\cdot)$: $2^{\mathcal{M}} \to \mathcal{N} \cup \{0\}$, such that
  1. $r(A) \leq |A|$
  2. if $A \subseteq B$ then $r(A) \leq r(B)$
  3. $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (submodularity)
- this generalizes the notion of rank for vector spaces
- if the ground set can be considered as a set of vectors over a finite field, with the usual rank function, the matrix is called *representable*
- not all matroids are representable
- the connection to linear network codes comes from the fact that the entropy of any collection of random variables is simply the rank of the matrix relating the variables to the (independent) sources

The Fano Matroid

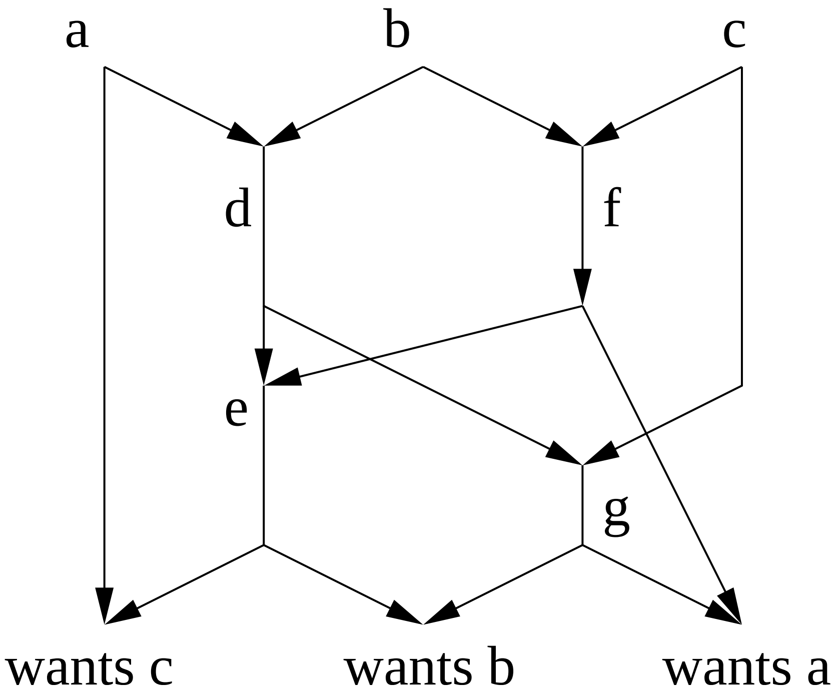


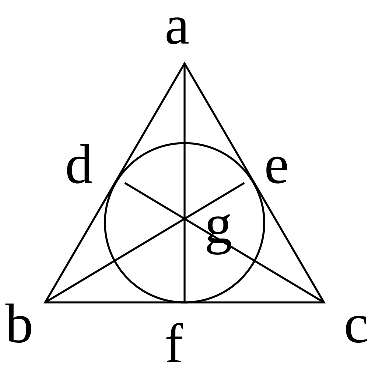
The Fano matroid has a representation only over $GF(2)$

$$A_7 = \begin{array}{c} \\ \\ \\ \end{array}\begin{array}{ccccccc} a & b & c & d & e & f & g \\ \end{array}$$

$$A_7 = \left[\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

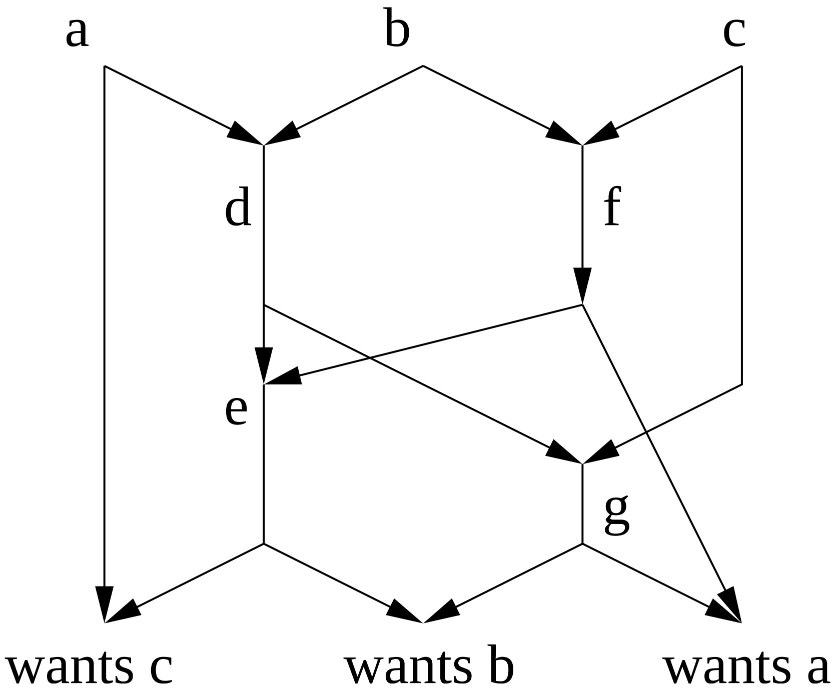
The Fano Network

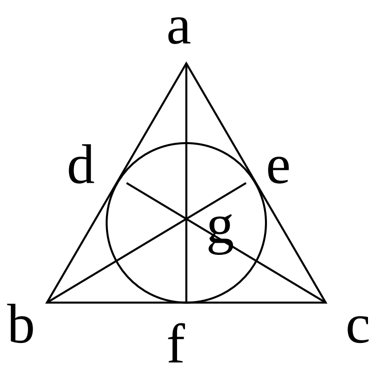




- The sources are a, b, c and the sinks require c, b, a, respectively
- Links are unit capacity
- What is the maximum rate?

The Fano Network Solution

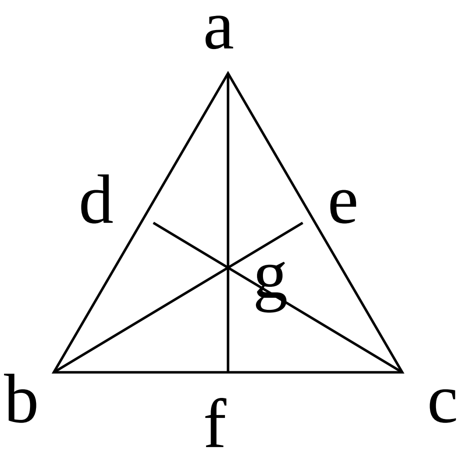




$$d = a + b \ \ , \ \ f = b + c \ \ , \ \ e = d + f = a + c \ \ , \ \ g = d + c = a + b + c$$

- Therefore the capacity is 3
- The network only has a solution on $GF(2)$

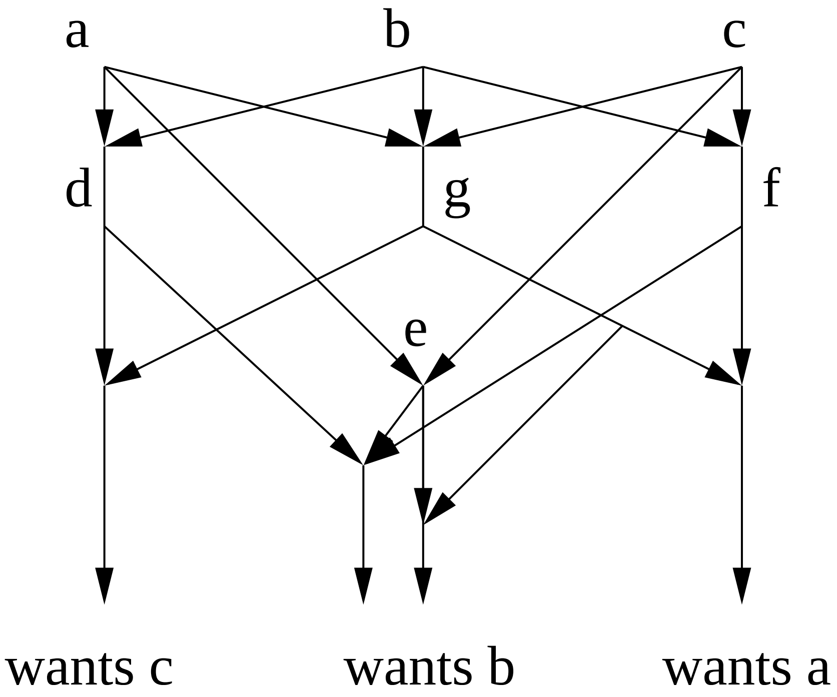
The Non-Fano Matroid

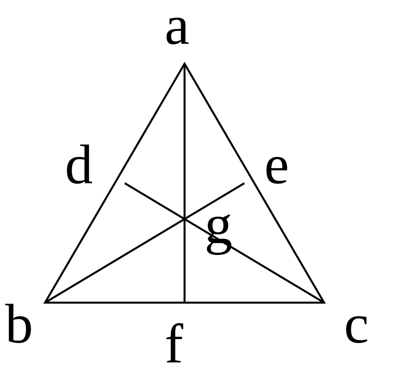


The Non-Fano matroid has a representation over every field except $GF(2)$

$$B_7 = \begin{array}{c} \\ \\ \\ \end{array}\begin{array}{ccccccc} a & b & c & d & e & f & g \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}$$

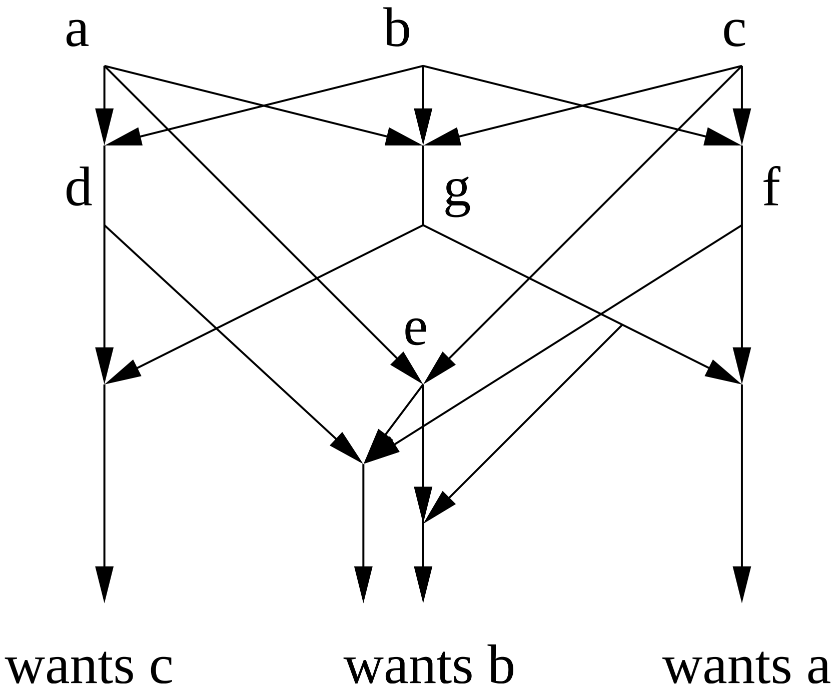
The Non-Fano Network

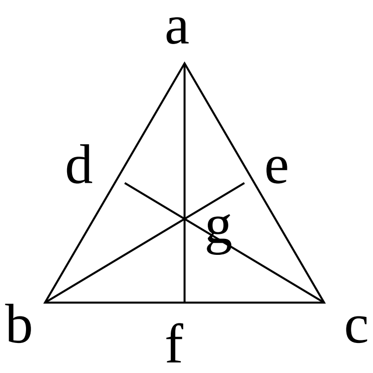




- The sources are a, b, c and the sinks require c, b, a, respectively
- Links are unit capacity
- What is the maximum rate?

The Non-Fano Network Solution

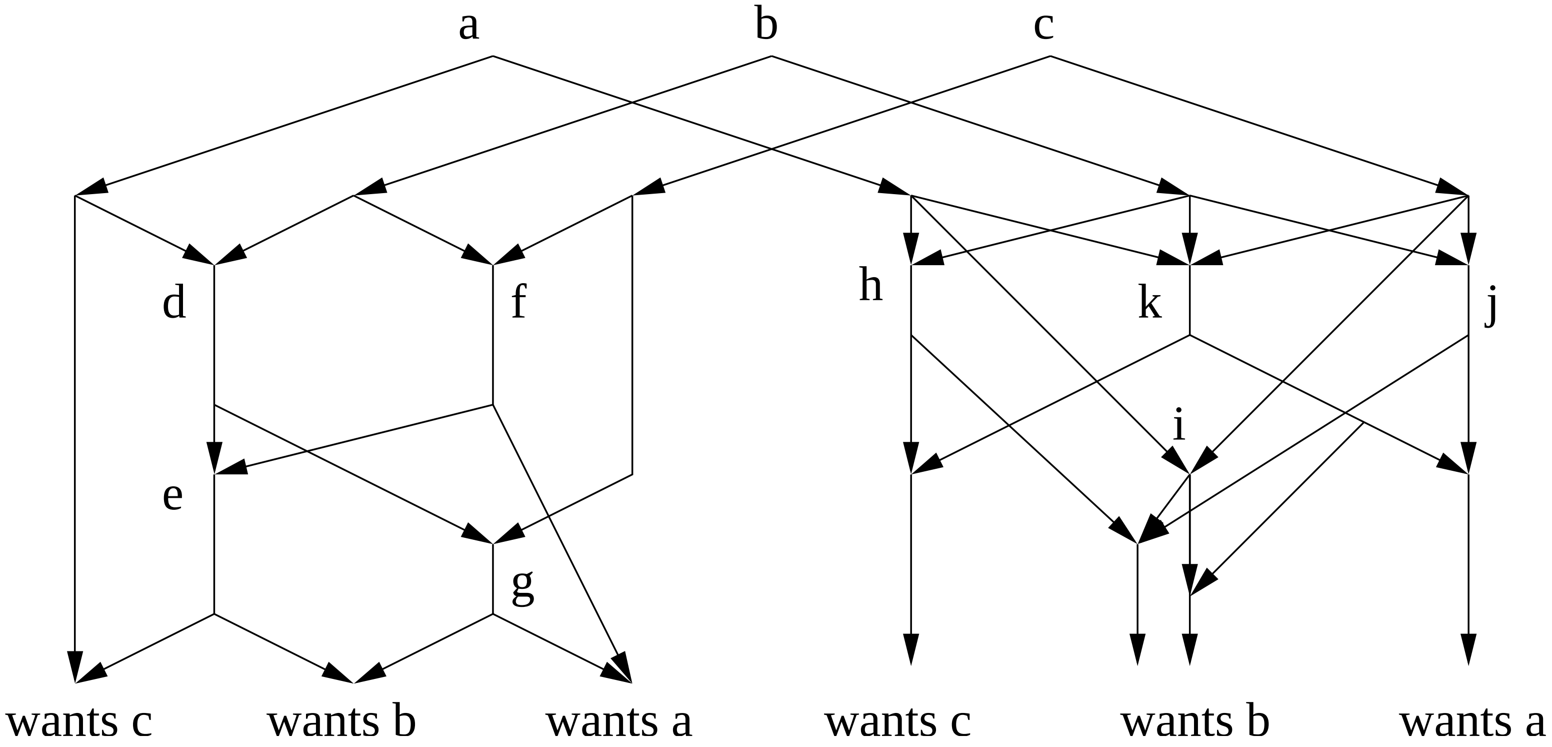




$$d = a + b \ \ , \ \ e = a + c \ \ , \ \ f = b + c \ \ , \ \ g = a + b + c$$

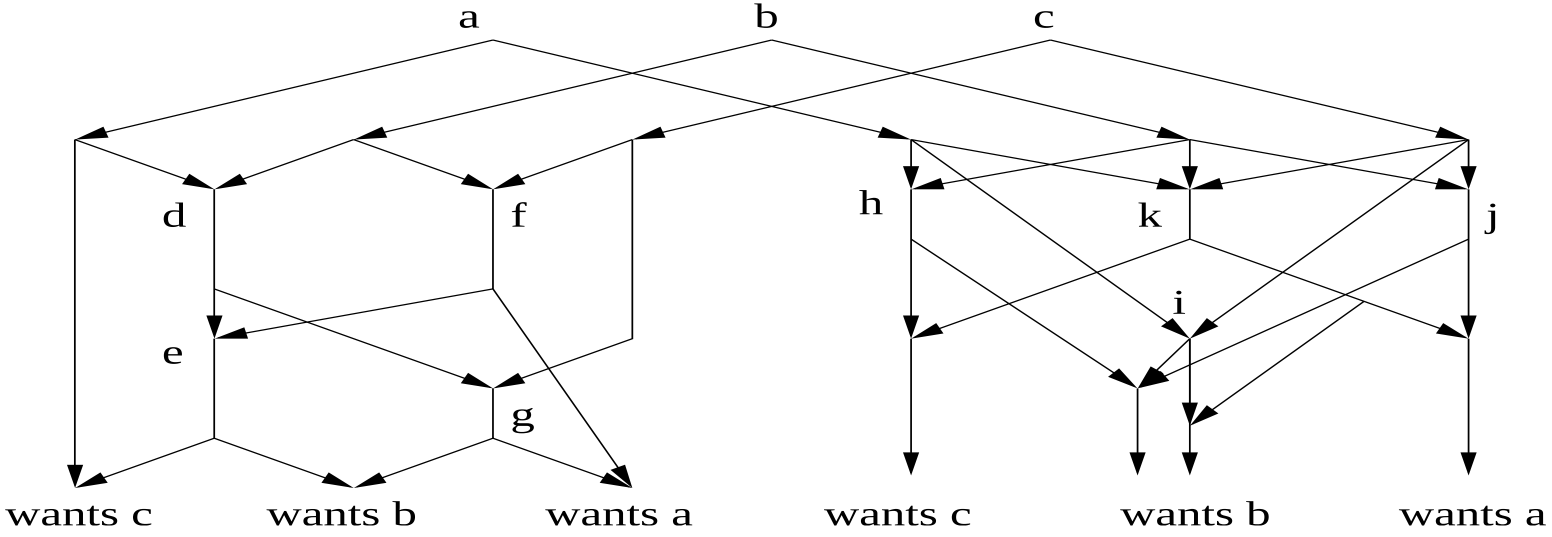
- Therefore the capacity is 4
- The network only has a solution except on $GF(2)$

A Network with No Linear Solution



- This network has no linear coding solution with capacity 7
- The linear network coding capacity can be shown to be $\frac{70}{11} < 7$

Capacity is 7



- View a, b, c, d, e, f, g on the LHS as elements of $GF(2)^n$ and a, b, c, h, i, j, k on the RHS as elements of $GF(2^n + 1)$, such that

$$d = a \oplus b \;\;,\;\; f = b \oplus c \;\;,\;\; e = d \oplus f = a \oplus c \;\;,\;\; g = d \oplus c = a \oplus b \oplus c$$

$$h = a + b \;\;,\;\; i = a + c \;\;,\;\; j = b + c \;\;,\;\; k = a + b + c$$

- The resulting capacity is $7\frac{n}{\log(2^n+1)} \approx 7(1 - \frac{1}{n}2^{-n})$

Insufficiency of Linear Network Codes

- The above example (inspired by Dougherty, Freiling and Zeger) shows that linear network codes cannot achieve the capacity region of general wired networks
- This means we need nonlinear network codes
- *Question:* Is there a certain class of codes, or a certain structure, that we can consider, or do we need to consider all nonlinear codes?

Matroid Representations

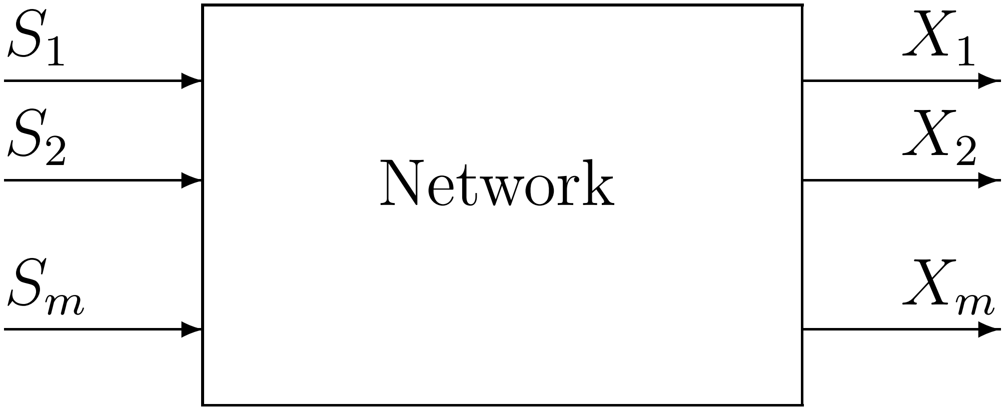
- Unfortunately, determining whether a general matroid is representable is a classical open problem in matroid theory
- However, the question of whether a matroid is *binary representable* has a relatively simple answer
  - the matroid must have no 4-element minor such that all pairs are independent and all triples dependent—see matrix below

$$\begin{bmatrix} 1 & 0 & 1 & ? \\ 0 & 1 & 1 & ? \end{bmatrix}$$

- Similar, albeit more complicated, conditions exist for ternary and quaternary matroids.
- One can use these results to develop a linear programming approach to the design of optimal linear network codes over $GF(2)$, $GF(3)$ and $GF(4)$ (the topic of another talk....)

A Generic Network Problem

Consider the following acyclic discrete memory-less network and assume that each source needs to transmit to its corresponding destination at rate R_i, $i = 1, 2, \ldots, m$:



It is not terribly hard to show that (cf. Ahlswede) the *rate region* for reliable communication is

$$\mathcal{R} = \mathrm{cl}\left\{ R_i, i = 1, \ldots, m \ \mid \ R_i < \frac{1}{T}\left(H(X_i^T) - H(X_i^T | S_i^T) \right) \right\} \quad \text{as } T \to \infty$$

Equivalently, if we are interested in optimizing a certain linear combination of the rates, we must solve

$$\lim_{T\to\infty} \sup_{p(S_i^T) \text{ and network operations}} \sum_{i=1}^{m} \alpha_i \frac{1}{T}\Big(H(X_i^T) - H(X_i^T|S_i^T)\Big)$$

This problem is notoriously difficult, since

- it is infinite-dimensional (what is called an *infinite-letter characterization*)
- for any T, the problem is highly non-convex in the $p(S_i^T)$ and the "network operations"

Ergo: No one does it this way!

Entropy Vectors

Consider n discrete random variables with alphabet-size N. For any set $\mathcal{S} \subseteq \{1, \ldots, n\}$, we have the normalized entropy $h_{\mathcal{S}} = \frac{1}{\log N} H(X_i, i \in \mathcal{S})$. *The $2^n - 1$ dimensional vector obtained from these entropies, is called an* entropy vector.

Conversely, any $2^n - 1$ dimensional vector which can be regarded as the entropy vector of some collection of n random variables, for some value of N, is called *entropic*.

The space of entropic vectors is denoted by Γ_n^*.

Theorem 1 *The closure of the space of entropic vectors, $\bar{\Gamma}_n^*$ is compact and convex.*

Networks and Entropy

But what does all this say about our network problem?

Well, networks put two types of constraints on entropy vectors:

1. topological constraints
2. channel constraints

Convex Formulation of the Network Problem

Theorem 2 *The problem of determining the capacity of an acyclic, memoryless wired network can be reduced to the optimization problem*

$$\max \sum_{i=1}^{m} \alpha_i \left(h(X_i) + h(S_i) - h(X_i, S_i) \right),$$

subject to $h \in \bar{\Gamma}_n^*$ *and*

- $h(S_1, \ldots, S_m) = \sum_{i=1}^{m} h(S_i)$, *for sources*
- $h(X_{out}, X_{In}) - h(X_{In}) = 0$, *for topological constraints*
- $h(X_i) \leq C_i$, *for channel constraints*

Thus, by going to the space of entropy vectors, we have circumvented both the *infinite-letter characterization* problem, as well as the *non-convexity.*

- Network information theory for wired networks is essentially the problem of characterizing $\bar{\Gamma}_n^*$.

Unfortunately, a characterization of $\bar{\Gamma}_n^*$ for $n \geq 4$ is open.

Entropy and Matroids

- A (poly)matroid is a set of objects along with a rank function that satisfies submodularity
- Entropy satisfies submodularity and therefore defines a polymatroid

$$H(A \cup B) + H(A \cap B) \leq H(A) + H(B)$$

- However, not all matroids are entropic
- A matroid is called *representable* if it can be represented by a collection of vectors over some (finite) field
- All representable matroids are entropic, but not all entropic matroids are representable
- When a matroid is representable, the corresponding network problem has an optimal solution which is a linear network code (over the field which represents the matroid)

Entropy and Groups

Given a finite group G, and $G_1, \ldots, G_n$ of its subgroups, the $2^n - 1$-dimensional vector whose components are

$$v_{\mathcal{S}} = \log \frac{|G|}{|\cap_{\alpha \in \mathcal{S}} G_\alpha|}.$$

for all $\mathcal{S} \subseteq \{1, \ldots, n\}$, is *entropic.*

Theorem 3 (Chan and Yeung) *Conversely, any entropic vector for some collection of n random variables, can be approached to desired accuracy, by some finite group and n of its subgroups*

Abelian Groups and the Ingleton Inequality

One may ask what types of groups are needed to characterize $\bar{\Gamma}_n^*$? Here is an important result.

Theorem 4 (Chan) *If G is an Abelian group, then the resulting entropy vectors satisfy the Ingleton bound*

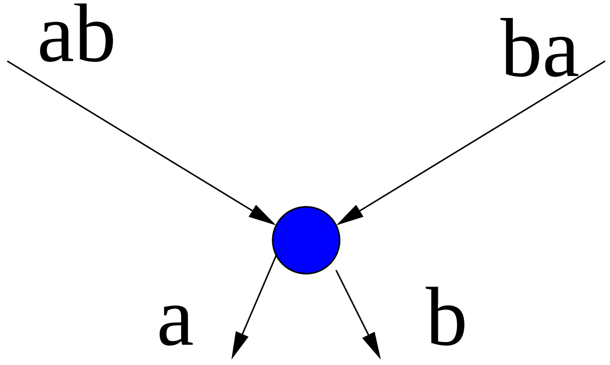
$$h_{ij} + h_{ik} + h_{il} + h_{jk} + h_{jl} \geq h_{ijk} + h_{ijl} + h_{kl} + h_i + h_j.$$

The Ingleton bound was first discovered in the context of representable matroids.

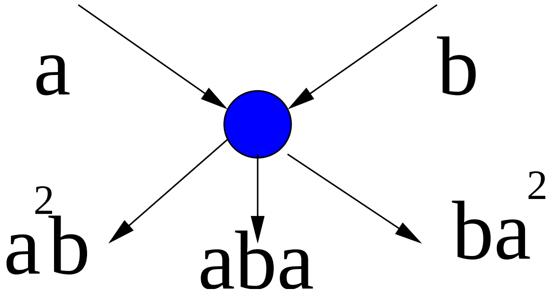
It is known that entropy can violate the Ingleton bound and so Abelian groups are not sufficient.

Linear network codes form an Abelian group, which is again why they are insufficient.

Codes from Non-Abelian Groups



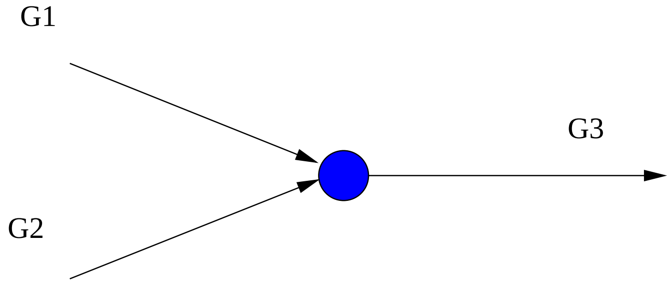
If a and b are chosen from a non-Abelian group, one may be able to infer more about them from ab and ba.



There is also a larger set of signals that one may transmit.

Group Network Codes

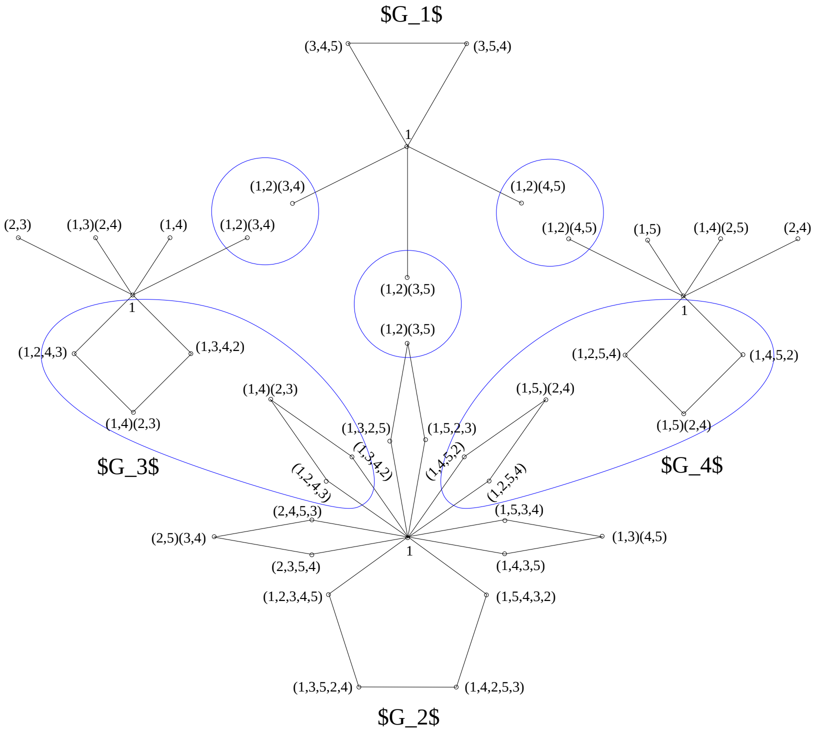
- choose a finite group G
- each edge in the network corresponds to a subgroup G_i of G
- the symbols transmitted on this edge are the *cosets* induced by G_i
  - we therefore require
$$\log \frac{|G|}{|G_i|} \leq C_i$$
- if G_1 and G_2 are input to a node whose output is G_3, we require that $G_3 \supseteq G_1 \cap G_2$
  - this determines the input-output mapping at this node, since any two cosets of $G1$ and G_2 will uniquely identify a coset in G_3



But what Kind of Groups to Use?

- We know we need non-Abelian groups
- But not all non-Abelian groups are stronger than linear network codes
- Let us search for non-Abelian groups that violate the Ingleton bound

The Group $PGL(2, p)$



- We have found the smallest Ingleton-violating group to be the projective linear group $PGL(2, 5)$ with 120 elements
- Its generalizations, $PGL(2, p)$, for $p \geq 5$, all violate Ingleton, as does the general linear group $GL(2, p)$.

- Good news: in some sense, these are the simplest non-Abelian groups. Bad news: subgroups are hard to characterize
- Have also looked at solvable groups. These are stronger than linear network codes, though we have not found ones that violate Ingleton. Their subgroups are easier to characterize.

While this may be somewhat encouraging, we are still a ways from constructing good group codes. Is there anything else we can do?

Where is This All Coming From?

Ans: Stat Mech and Typical Sequences

- Suppose we have T particles that can be in one of N states with probability p_i, $i = 1, 2, \ldots, N$.
- Then the *typical* micro-states will be those for which

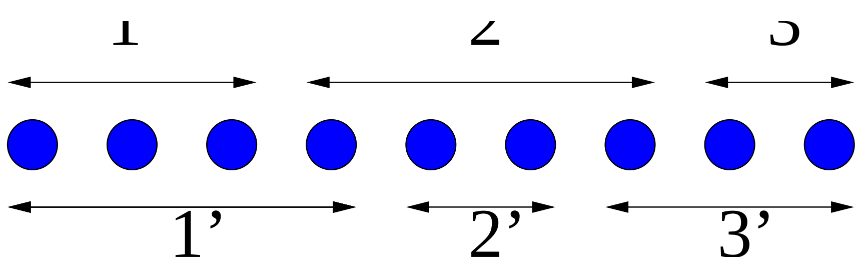
$$T_i = Tp_i.$$

- The entropy is simply the log of the number of microstates

$$\log \frac{T!}{T_1! T_2! \ldots T_N!}, \quad T_i = Tp_i, \quad \sum_{i=1}^{N} T_i = T.$$

One can think of the numerator as the size of the symmetric group S_T of T elements and the denominator as the size of a certain subgroup of S_T.

Entropy and Partitions



$$\begin{cases} T_1 = 3 \quad , \quad T_2 = 4 \quad , \quad T_3 = 2 \\ h_1 = \log \frac{9!}{3!4!2!} = \log 1260 = 10.3 \text{bits} \end{cases}$$

$$\begin{cases} T_{1'} = 4 \quad , \quad T_{2'} = 2 \quad , \quad T_{3'} = 3 \\ h_2 = \log \frac{9!}{4!2!3!} = \log 1260 = 10.3 \text{bits} \end{cases}$$

$$\begin{cases} T_{11'} = 3 \quad , \quad T_{21'} = 1 \quad , \quad T_{22'} = 2 \quad , \quad T_{23'} = 1 \quad , \quad T_{33'} = 2 \\ h_{12} = \log \frac{9!}{3!1!2!1!2!} = \log 15120 = 13.9 \text{bits} \end{cases}$$

Staking Out the Entropy Region

- Take a set of size T and for each random variable partition it into N sets
- The entropies and joint entropies can be computed from the partitions and their various intersections
- By making *local* changes to the partitions, we can move from one entropy vector to the next
- As T and N grow, one can stake out the entire entropic region to desired accuracy
- This idea can be used to perform random walks on entropy vectors and thereby MCMC methods for entropy optimization

Maximizing the Ingleton Bound via MCMC

$$I = h_{ij} + h_{ik} + h_{il} + h_{jk} + h_{jl} - h_{kl} - h_{ijk} - h_{ijl} - h_i - h_j$$

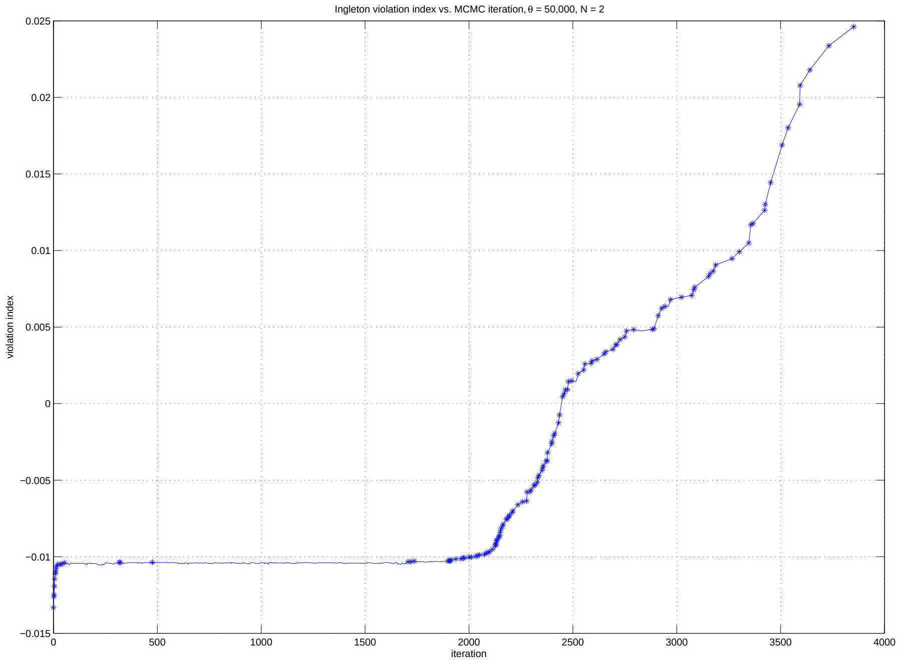
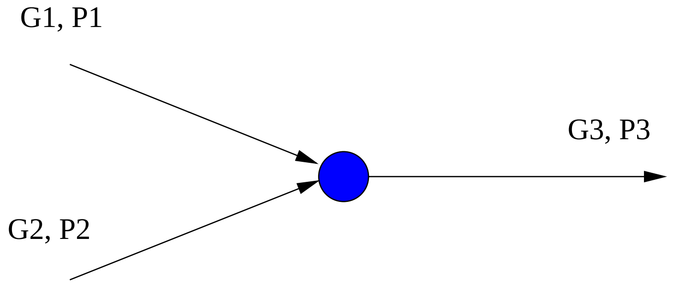


Figure 1: $I < 0$ is the Ingleton bound. Maximizing it with $T = 100$ and $N = 2$ using Monte Carlo Markov chain simulation achieved .025. The best prior Ingleton-bound violating instance was .0072.

Optimizing Information Flow in Networks

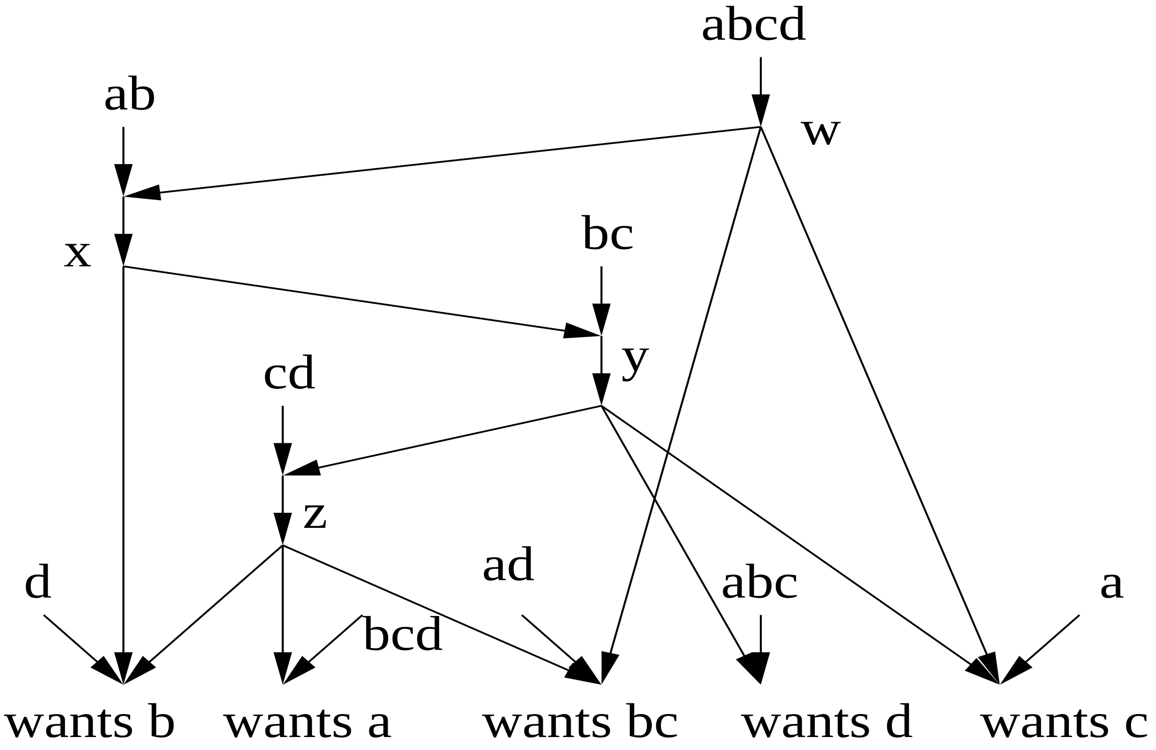
The same optimization can be done in networks, provided we respect the network topology.



$$G_3 \supseteq G_1 \cap G_2 \quad , \quad P_3 \subseteq P_1 \cap P_2$$

- For example, the sum rate can be optimized in a *distributed* fashion
- Each edge randomly changes its partition based on information received by the sinks

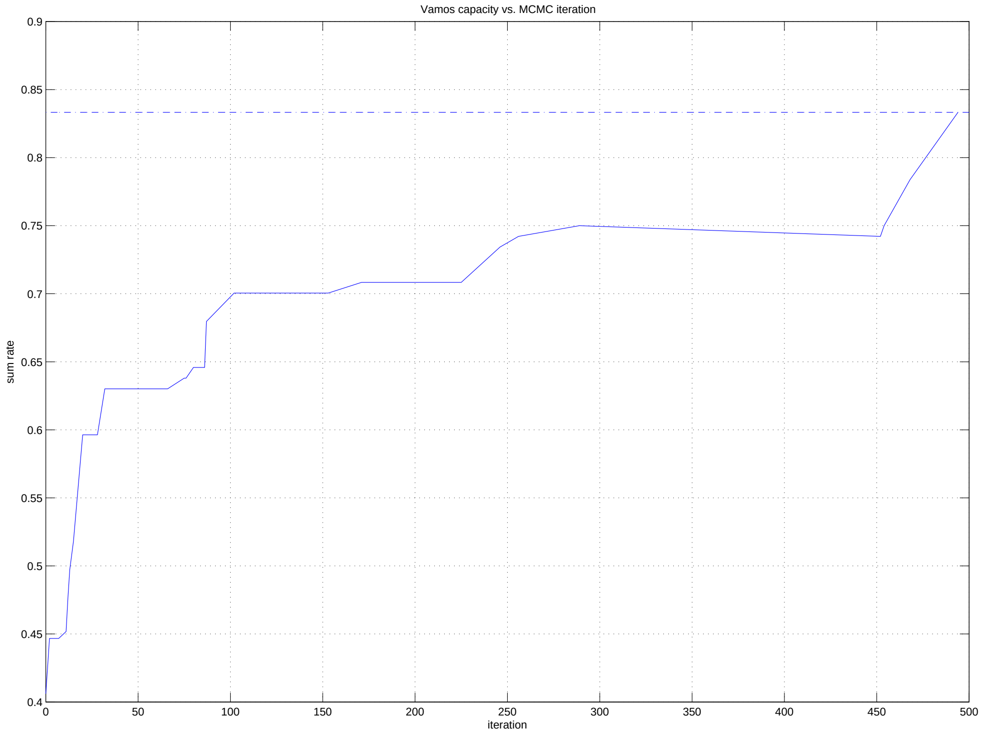
Example - The Vamos Network



- Constructed from the Vamos matroid—the*smallest non-representable matroid*—8 elements and $U(2,4)$ and $\mathcal{F}_7$ minors
- Maximum rate unknown; known to be less than $\frac{60}{11}$

- Dougherty et al give a six-dimensional linear vector solution with capacity 5.

- However, using an MCMC method, we have been able to find a *nonlinear binary* solution with capacity 5 (here the search space has size 10^{12})



Non-Pappus Matroid and Network

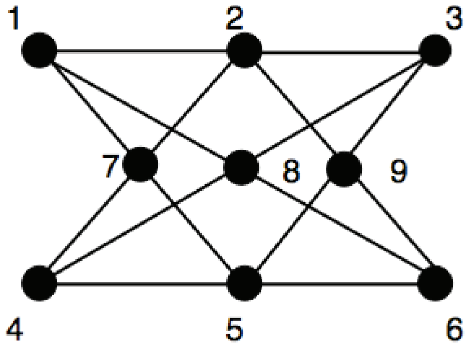
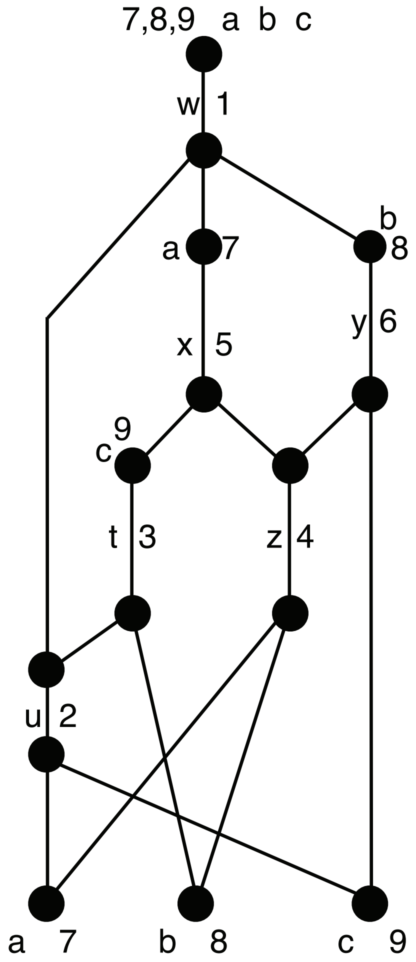


Figure 2: Another example of a nonrepresentable matroid.

The capacity of the corresponding network is unknown.


7,8,9 a b c
w 1
a 7
b
8
x 5
y 6
c
9
t 3
z 4
u 2
a 7
b 8
c 9

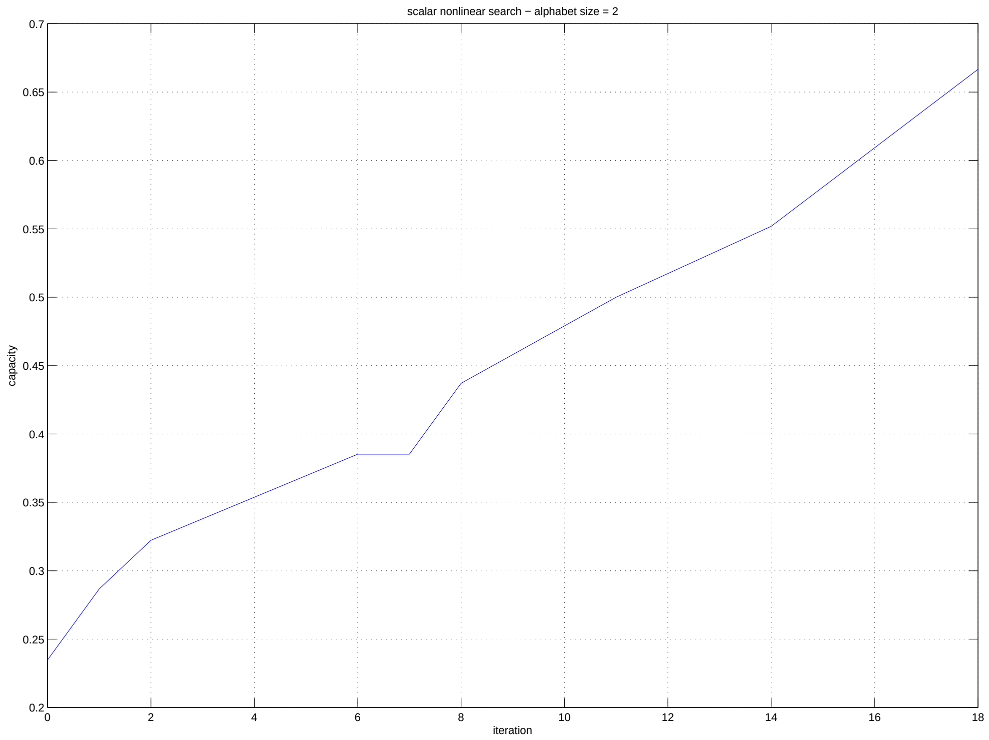


Figure 3: Nonlinear code $N = 2$, $C = 0.6667$.

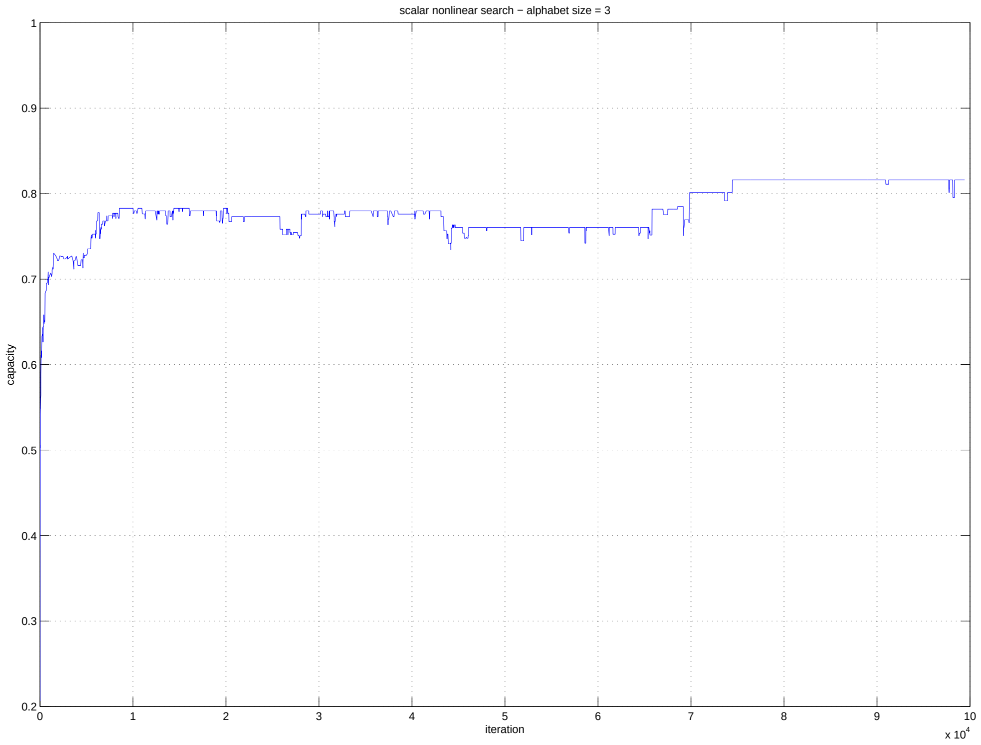


Figure 4: Nonlinear code $N = 3$, $C = 0.8228$.

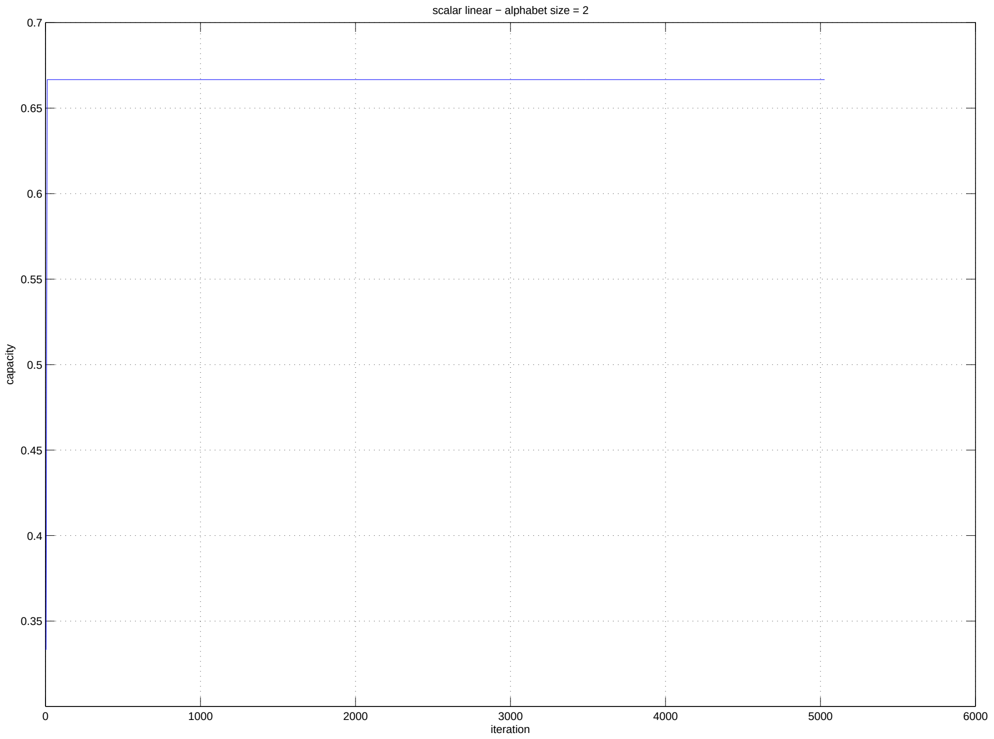


Figure 5: Linear code $N = 2$, $C = 0.6667$.

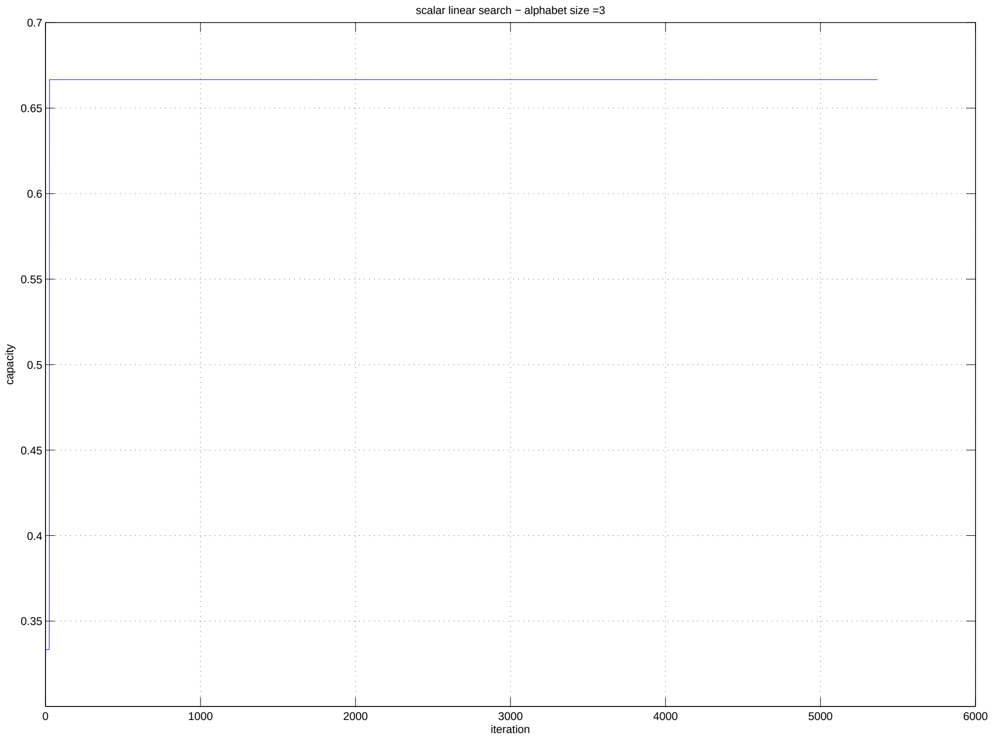


Figure 6: Linear code $N = 3$, $C = 0.6667$.

Conclusion

- Showed that linear network codes are insufficient for achieving the capacity of general wired networks
- Used the connection to entropic vectors to show that one needs group network codes to achieve capacity
  - each edge corresponds to a subgroup; symbols are cosets; outputs should be supergroups of the intersection of input groups
- Identified the smallest Ingleton-bound-violating group, $PGL(2, 5)$.
  - the projective and general linear groups are all stronger than linear network codes
- Developed a distributed MCMC method (via random walks over partitions) for the design of optimal linear and nonlinear codes over small alphabet sizes