Code Realizations for Networks

Ralf Koetter, Coordinated Science Lab.,
University of Illinois
e-mail: koetter@csl.uiuc.edu

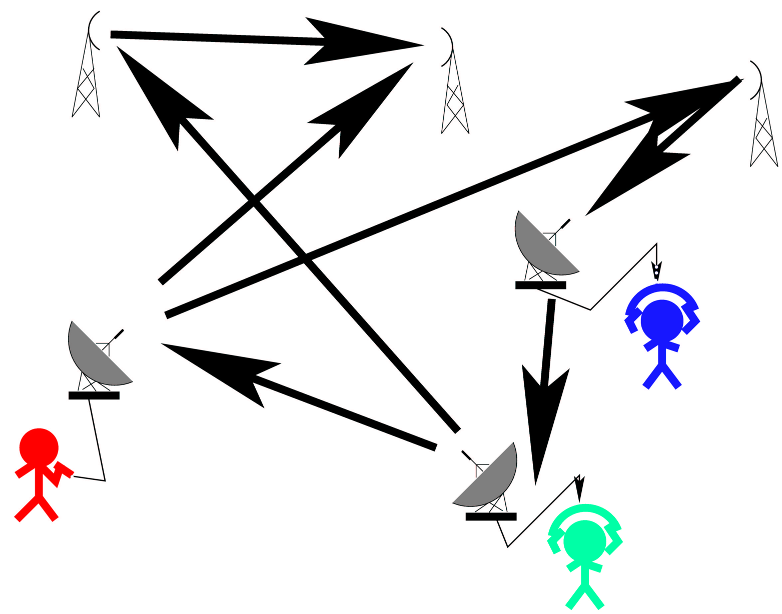
The network....

⋮

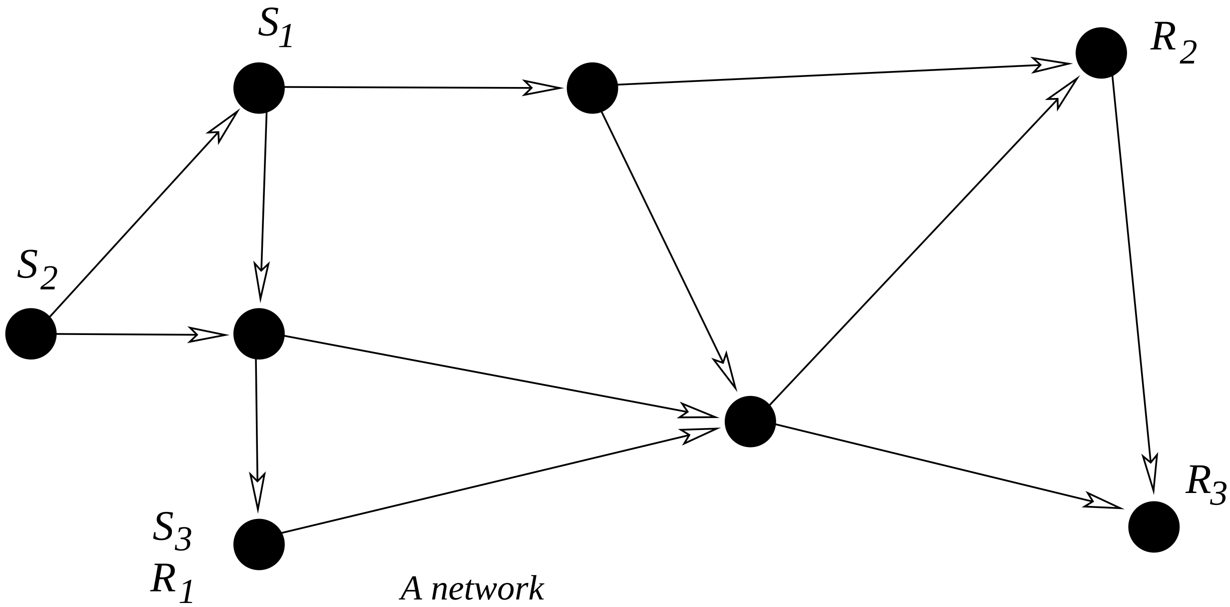
...,Muriel Medard, Tracey Ho, David Karger, Michelle Effros, Gerhard Kramer, Irem Koprulu,...

⋮

Networks



- What is capacity?
- How robustly can we communicate?
- Do we know the network?
- How do we achieve capacity?
- ??????



A network

Vertices: V

Edges: $E \subseteq V \times V$, $e = (v, u) \in E$

Edge capacity: $C(e)$

Network: $\mathcal{G} = (V, E)$

Source nodes: $\{v_1, v_2, \ldots, v_N\} \subseteq V$

Sink nodes: $\{u_1, u_2, \ldots, u_K\} \subseteq V$

Input random processes at v:
$\mathscr{X}(v) = \{X(v,1), X(v,2), \ldots, X(v,\mu(v)\}$

Output random processes at u:
$\mathscr{Z}(u) = \{Z(u,1), Z(u,2), \ldots, Z(u,\nu(u))\}$

Random processes on edges: $Y(e)$

A connection:
$c = (v, u, \mathscr{X}(v,u))$, $\mathscr{X}(v,u) \subseteq \mathscr{X}(v)$

A connection is established if
$\mathscr{Z}(u) \supset \mathscr{X}(v,u)$

Set of connections: $\mathscr{C}$

The pair $(\mathcal{G}, \mathscr{C})$ defines a network problem.

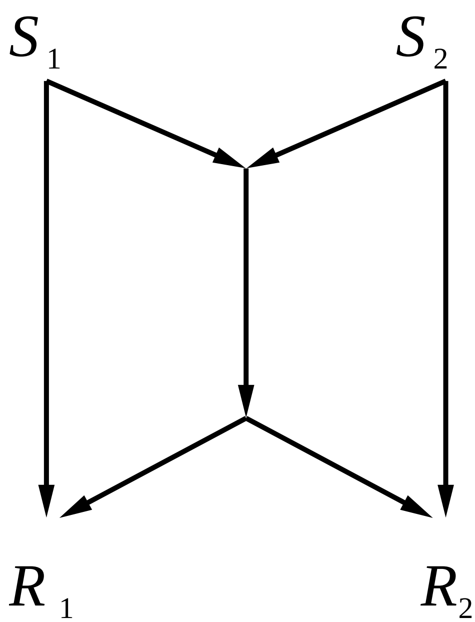
The capacity problem

Is the problem $(\mathcal{G}, \mathscr{C})$ solvable?

How do we find a solution?

Disclaimer: We are not dealing with probabilistic descriptions of channels which is way too hard for us as can be experienced by considering a simple problem like the relay channel. Moreover, we are not (really) dealing with the problem of optimizing routing and flows. Listening to this talk is potentially hazardous and is done according to the respective listeners free will.

Codes for networks The example



$$\mathscr{C} = \{(S_i, R_j, \mathscr{X}(S_j)), i, j \in \{1, 2\}\}$$

R. Ahlswede, N. Cai, S.-Y.R. Li, R.W. Yeung, 2000

Simplyfying Assumptions

$C(e) = 1$
(links have the same capacity)

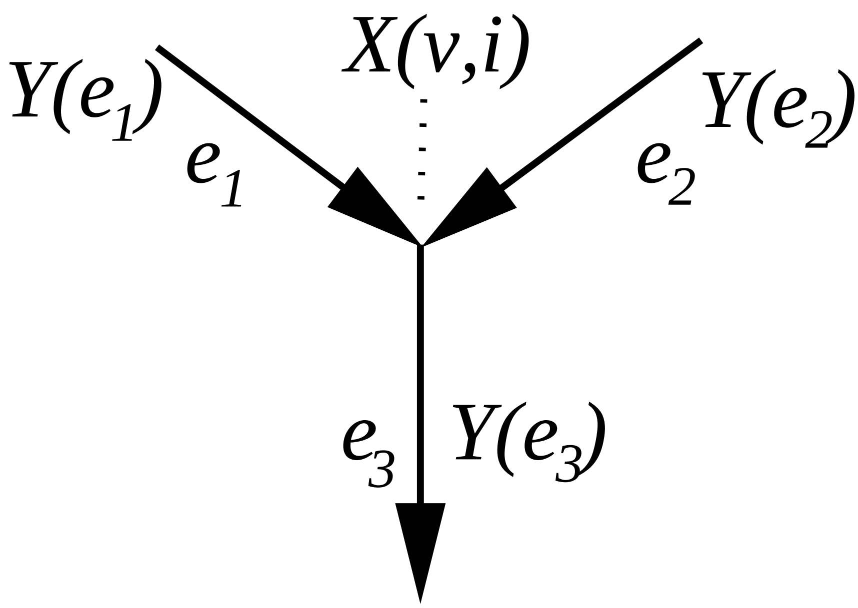
$H(X(v,i)) = 1$
(sources have the same rate)

The $X(v,i)$ are mutually independent.

Vector symbols of length m are transmitted and interpreted as elements in $\mathbb{F}_{2^m}$.

Linear network codes

All operations at network nodes are linear!



$$Y(e_3) = \sum_i \alpha_i X(v,i) + \sum_{j=1,2} \beta_j Y(e_j)$$

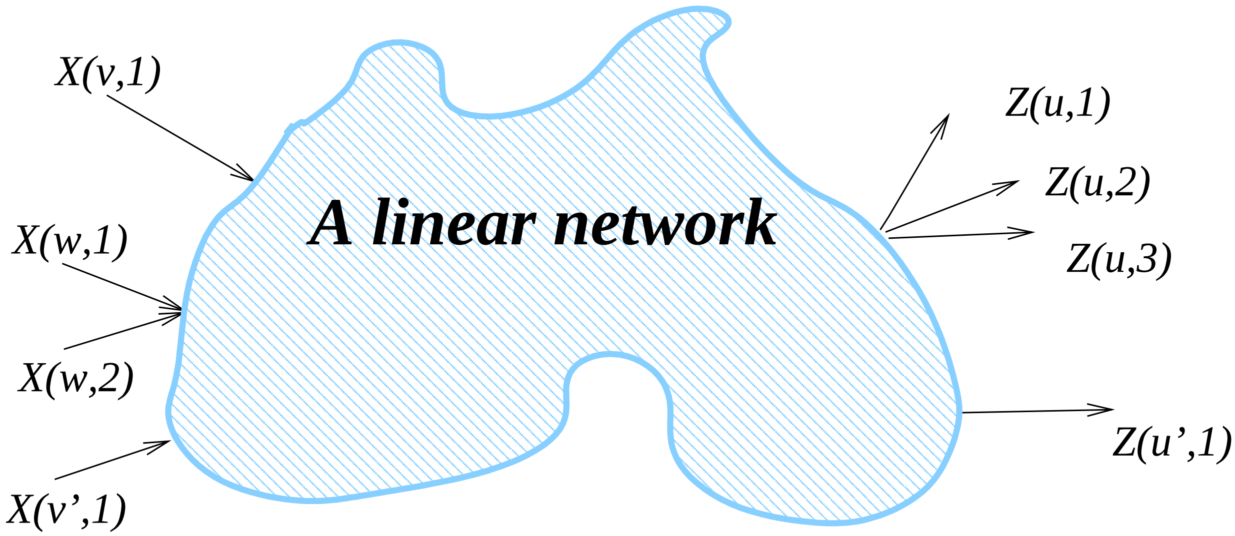
Definition (Linear Network Coding)

$$Y(e) = \sum_{l=1}^{\mu(v)} \alpha_{e,l} X(v,l) + \sum_{e':head(e')=tail(e)} \beta_{e',e} Y(e'),$$

$\alpha_{e,l}, \beta_{e',e} \in \mathbb{F}_{2^m}$.

A consequence:

$$Z(v,j) = \sum_{e':head(e')=v} \varepsilon_{e',j} Y(e').$$



Input: $\underline{x} = (X(v,1), X(v,2), \ldots, X(v', \mu(v')))$

Output: $\underline{z} = (Z(u,1), Z(u,2), \ldots, Z(u', \nu(u')))$

Transfer matrix M: $\boxed{\underline{z} = \underline{x}M}$

$\underline{\xi} = (\xi_1, \xi_2, \ldots,) =$
$(\ldots, \alpha_{e,l}, \ldots, \beta_{e',e}, \ldots, \varepsilon_{e',j}, \ldots)$

$$\boxed{M_{i,j} \in \mathbb{F}_2[\underline{\xi}].}$$

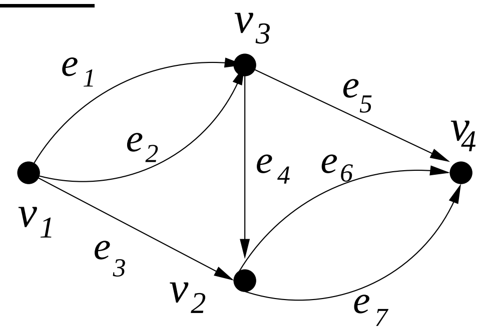
An alg. Min-Cut Max-Flow condition

Theorem Let a linear network be given. The following three statements are equivalent:

1. A point-to-point connection $c = (v, v', \mathscr{X}(v, v'))$ is possible.
2. The Min-Cut Max-Flow bound) is satisfied for a rate $R(c) = |\mathscr{X}(v, v')|$.
3. The determinant of the $R(c) \times R(c)$ transfer matrix M is nonzero over the ring $\mathbb{F}_2[\underline{\xi}]$ ∎

3. $\Rightarrow$ We have to study the solution sets of polynomial equations.

An Example:



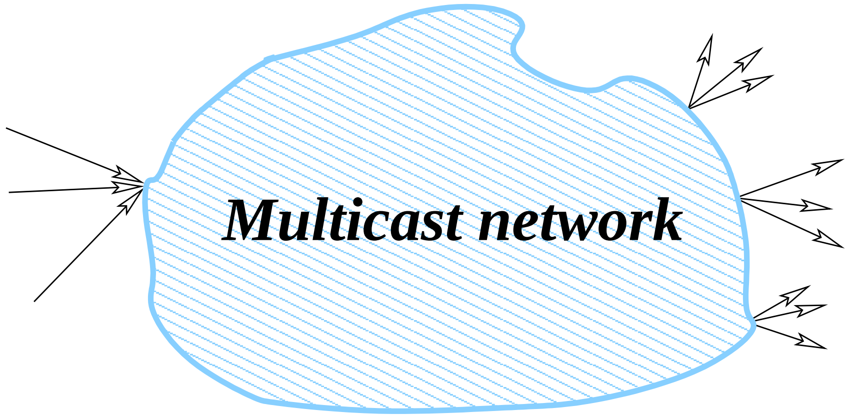
$$\mathscr{C} = (v_1, v_4, \{X(v_1,1), X(v_,2), X(v_1,3)\})$$

$$A = \begin{pmatrix} \alpha_{e_1,1} & \alpha_{e_2,1} & \alpha_{e_3,1} \\ \alpha_{e_1,2} & \alpha_{e_2,2} & \alpha_{e_3,2} \\ \alpha_{e_1,3} & \alpha_{e_2,3} & \alpha_{e_3,3} \end{pmatrix}, \quad B = \begin{pmatrix} \varepsilon_{e_5,1} & \varepsilon_{e_5,2} & \varepsilon_{e_5,3} \\ \varepsilon_{e_6,1} & \varepsilon_{e_6,2} & \varepsilon_{e_6,3} \\ \varepsilon_{e_7,1} & \varepsilon_{e_7,2} & \varepsilon_{e_7,3} \end{pmatrix}.$$

$$M = A \begin{pmatrix} \beta_{e_1,e_5} & \beta_{e_1,e_4}\beta_{e_4,e_6} & \beta_{e_1,e_4}\beta_{e_4,e_7} \\ \beta_{e_2,e_5} & \beta_{e_2,e_4}\beta_{e_4,e_6} & \beta_{e_2,e_4}\beta_{e_4,e_7} \\ 0 & \beta_{e_3,e_6} & \beta_{e_3,e_6} \end{pmatrix} B^T.$$

$$\begin{aligned} \mathbf{det}(M) &= \mathbf{det}(A)\mathbf{det}(B) \\ & (\beta_{e_1,e_5}\beta_{e_2,e_4} - \beta_{e_2,e_5}\beta_{e_1,e_5})(\beta_{e_4,e_6}\beta_{e_3,e_7} - \beta_{e_4,e_7}\beta_{e_3,e_6}) \end{aligned}$$

Choose the coefficients so that $\mathbf{det}(M) \neq 0$!



$$\begin{array}{|c|c|c|} \hline M_{11} & M_{12} & M_{13} \\ \hline \end{array}$$

$\mathscr{C} = \{(v, u_1, \mathscr{X}(v)), (v, u_2, \mathscr{X}(v)), \ldots, (v, u_K, \mathscr{X}(v))\}$

M is a $|\mathscr{X}(v)| \times K|\mathscr{X}(v)|$ matrix.

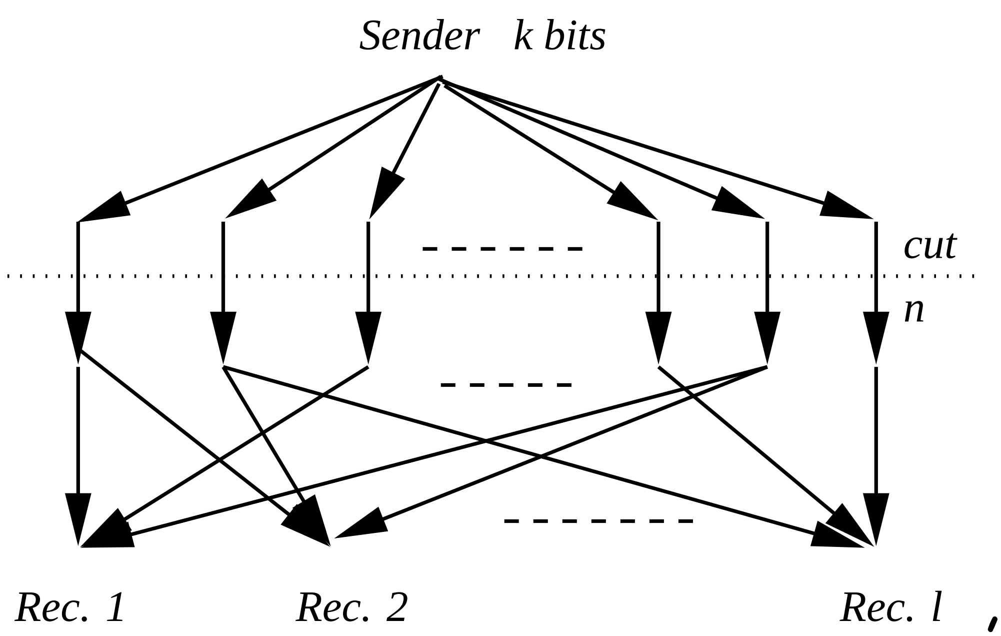
Choose the coefficients in $\bar{\mathbb{F}}$ s.th.
$m_i(\underline{\xi}) \stackrel{\text{def}}{=} det(M_{1,i}(\underline{\xi})) \neq 0$

Find a solution of $\xi_0 \prod_i m_i(\underline{\xi}) = 1$

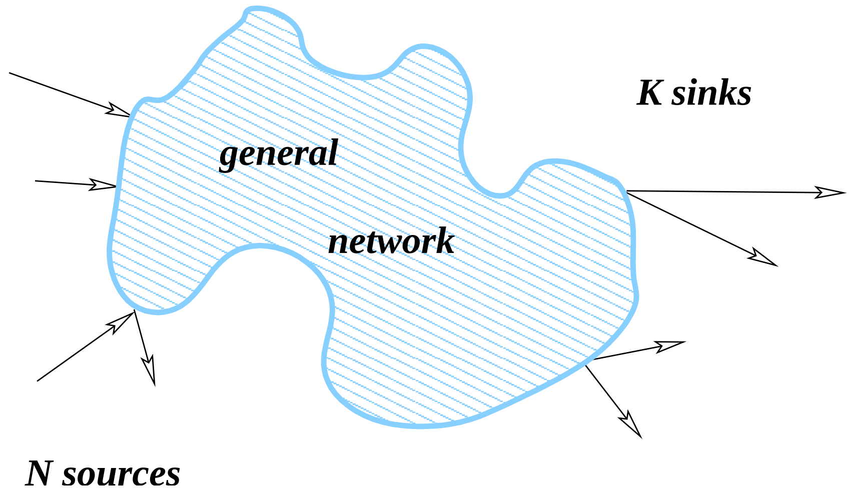
Do we really need coding?

We do not only need codes -

we need all codes!



C is a [n, k] code with l information sets. Each receiver picks out one information set.



$$\mathscr{C} = \{(v_i, u_j, \mathscr{X}(v_i, u_j))\}$$

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} & \dots & M_{1,K} \\ M_{2,1} & M_{2,2} & & M_{2,K} \\ \vdots & & & \vdots \\ M_{N,1} & M_{N,2} & \dots & M_{N,K} \end{pmatrix}$$

$M_{i,j}$ corresponds to
$c_{i,j} = (v_i, u_j, \mathscr{X}(v_i, u_j))$.

Theorem

[**Generalized** Min-Cut Max-Flow **Condition**]

Let an acyclic, delay-free linear network problem $(\mathcal{G}, \mathscr{C})$ be given and let $M = \{M_{i,j}\}$ be the corresponding transfer matrix relating the set of input nodes to the set of output nodes. The network problem is solvable if and only if there exists an assignment of numbers to $\underline{\xi}$ such that

1. $M_{i,j} = \mathbf{0}$ for all pairs (v_i, v_j) of vertices such that $(v_i, v_j, \mathscr{X}(v_i, v_j)) \notin \mathscr{C}$.
2. If $\mathscr{C}$ contains the connections $(v_{i_1}, v_j, \mathscr{X}(v_{i_1}, v_j))$, $(v_{i_2}, v_j, \mathscr{X}(v_{i_2}, v_j)), \ldots, (v_{i_\ell}, v_j,$ $\mathscr{X}(v_{i_\ell}, v_j))$ the determinant of $\left[M^T_{i_1,j} M^T_{i_2,j}, \ldots, M^T_{i_\ell,j}\right]$ is nonzero.

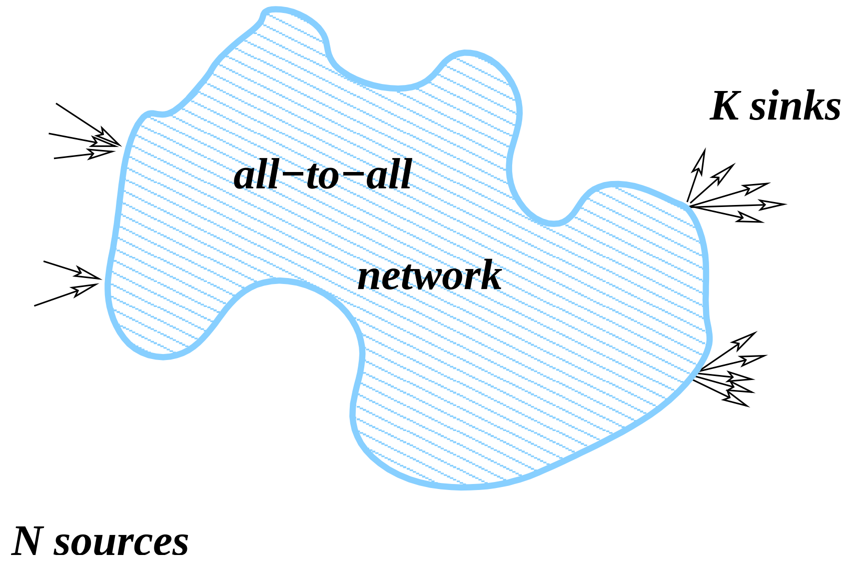
Entries in $M_{i,j}$ that have to evaluate to zero: $f_1(\underline{\xi}), f_2(\underline{\xi}), \ldots, f_L(\underline{\xi})$

Determinants of submatrices that have to evaluate to nonzero values: $g_1(\underline{\xi}), g_2(\underline{\xi}), \ldots, g_{L'}(\underline{\xi})$

$$\langle f_1(\underline{\xi}), f_2(\underline{\xi}), \ldots, f_L(\underline{\xi}), f_0(\underline{\xi}) \stackrel{\text{def}}{=} 1 - \xi_0 \prod_{i=1}^{L'} g_i(\underline{\xi}) \rangle$$

The central Theorem

Let a linear network problem $(\mathcal{G}, \mathscr{C})$ be given. The network problem is solvable if and only if there exists a common non-trivial solution to all polynomial equations $f_i(\underline{\xi}) = 0$, $i = 0, 1, ..., L$.

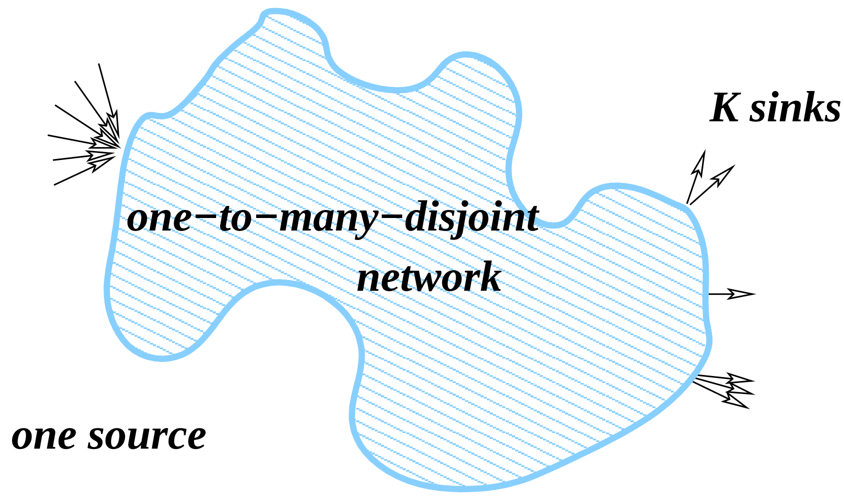


Theorem

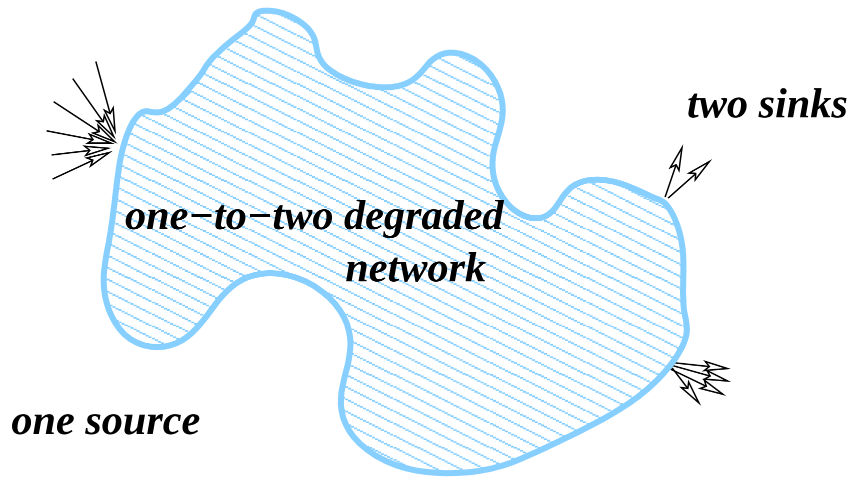
Let a linear, acyclic, delay-free network $\mathcal{G}$ be given with a set of desired connections

$$\mathscr{C} = \{(v_i, u_j, \mathscr{X}(v_i)) : i = 0, 1, \dots N, j = 1, 2, \dots K\}$$

The network problem $(\mathcal{G}, \mathscr{C})$ is solvable if and only if the Min-Cut Max-Flow bound is satisfied for any cut between all source nodes $\{v_i : i = 0, 1, \dots N\}$ and any sink node u_j.



Theorem Let a linear, acyclic, delay-free network $\mathcal{G}$ be given with a set of desired connections $\mathscr{C} = \{(v, u_j, \mathscr{X}(v, u_j)) : j = 1, 2, \ldots K\}$ such that all collections of random processes are mutually disjoint, i.e. $\mathscr{X}(v, u_j) \cap \mathscr{X}(v, u_i) = \emptyset$ for $i \neq j$. The network problem is solvable if and only if the Min-Cut Max-Flow bound is satisfied at a rate $|\mathscr{X}(v)|$ for any cut separating v from the set of sink nodes $\{u_1, u_2, \ldots, u_K\}$.

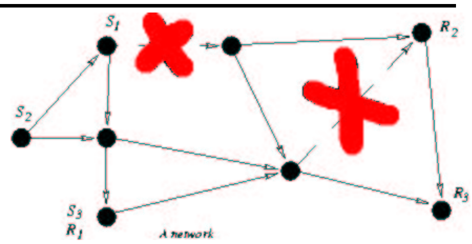


Theorem("Two-level broadcast ") Let a acyclic network $\mathcal{G}$ be given with a set of desired connections

$$\mathscr{C} = \{(v, u_1, \mathscr{X}(v, u_1)), (v, u_2, \mathscr{X}(v))$$

The network problem is solvable if and only if the Min-Cut Max-Flow bound is satisfied between v and u_1 at a rate $|\mathscr{X}(v, u_1)|$ and between v and u_2 at a rate $|\mathscr{X}(v)|$. ∎

The robustness problem



Network management and network coding

Finding efficient solutions

T. Ho, M. Médard, R. Koetter, "An information theoretic view of network management", INFOCOM 2003

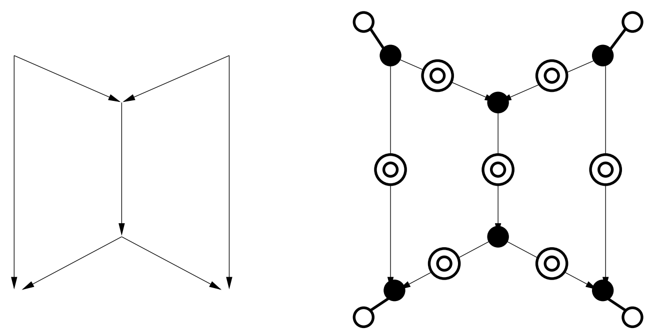
T. Ho, R. Koetter, M. Medard, D. Karger and M. Effros, "The Benefits of Coding over Routing in a Randomized Setting", ISIT 2003

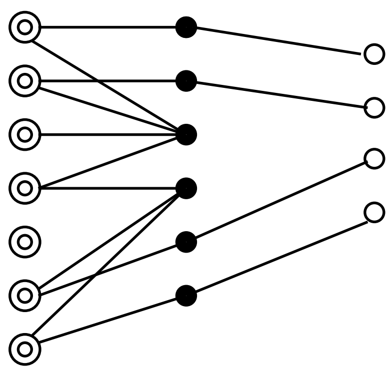
T. Ho, D. Karger, M. Medard and R. Koetter, "Network Coding from a

Network Flow Perspective", ISIT 2003

How does the network code improve things?

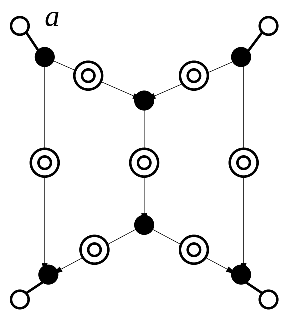
The network as a linear system:

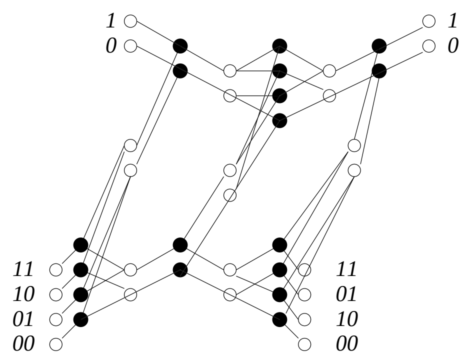




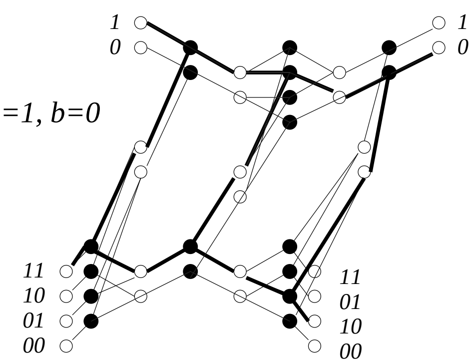
Local behaviors, states, and visible variables make up a state space realization. (Forney, trellis formations - Vardy and K.)

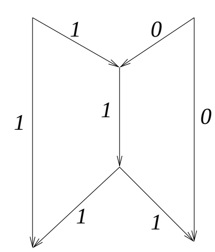
How to visualize the linear system?





a=1, b=0





Embedding a code with generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The problem from a coding perspective:

A network problem $(\mathcal{G}, \mathscr{C})$ corresponds to a desired behavior of a linear system on a graph described by $\mathcal{G}$.

How to embed a given code in a given graph efficiently, i.e. with small state spaces.

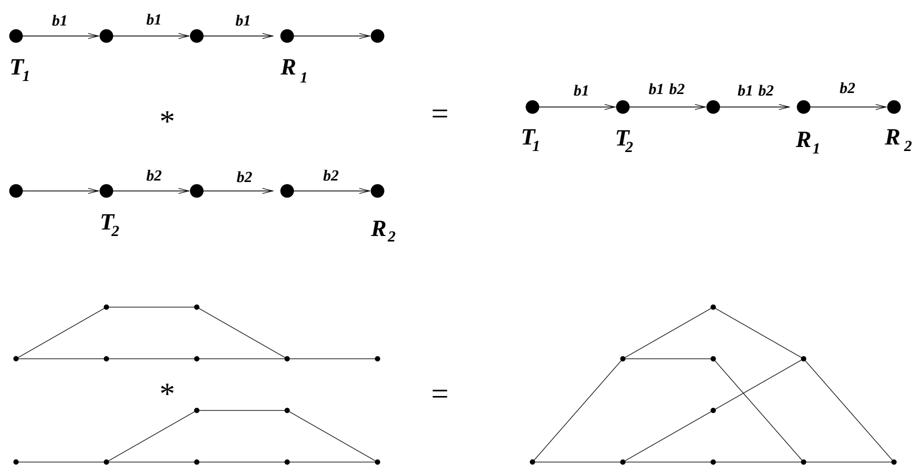
Help from: Trellis constructions, Trellis duality, Structure theorems ....

The product construction

Kschischang and Sorokine

Linear trellises constructed as "product" of simpler trellises:

$\mathcal{G}_1 = (V_1, E_1)$, $\mathcal{G}_2 = (V_2, E_2)$,
$\mathcal{G} = \mathcal{G}_1 * \mathcal{G}_2 = (V_1 \oplus V_2, E_1 \oplus E_2)$



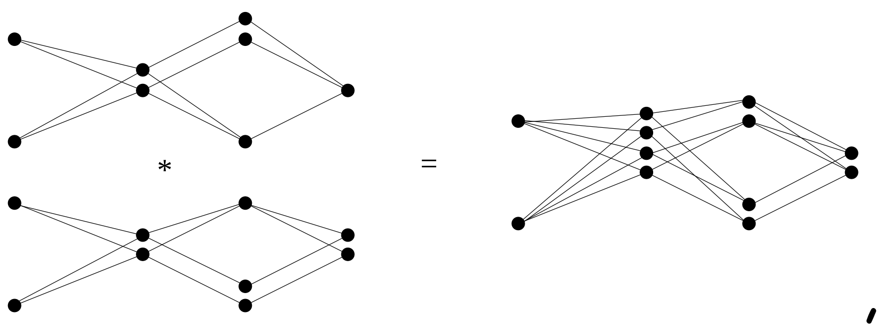
,

The "simple" trellises are minimal trellises for one dimensional linear spaces.

The product construction

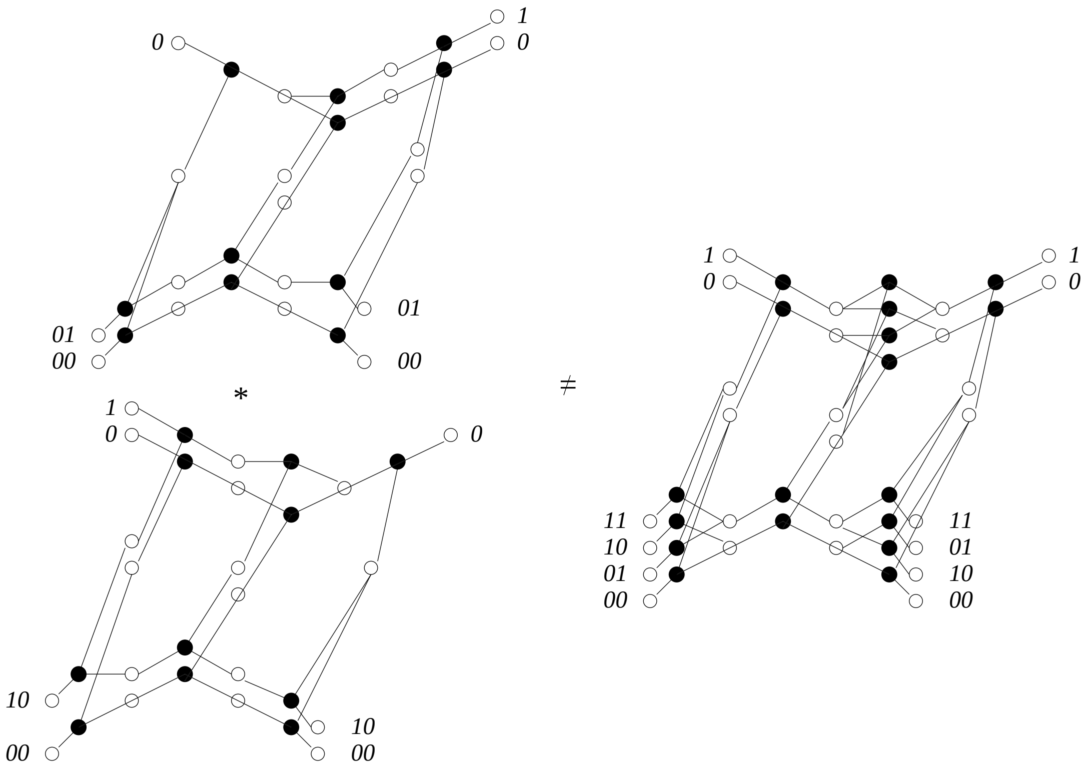
$\boxed{\text{Is this exhaustive?}}$

For trellises:



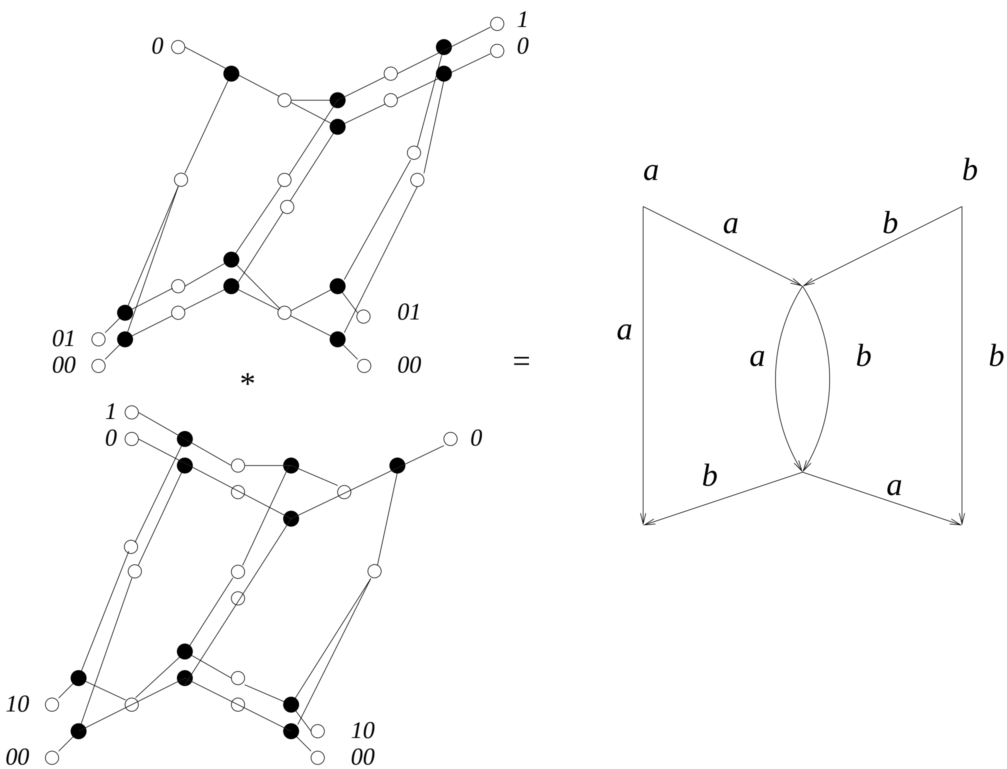
The product construction

For trellis formations:



Routing and the product construction

For trellises:



,

The product construction is equivalent to the "routing" solution for the network problem.

Networks for codes - codes for networks

Given a network problem $\Leftrightarrow$ we can associate a linear code with the problem.

Finding an efficient transmission strategy $\Leftrightarrow$ Finding a trellis with small state spaces

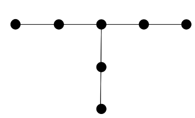
Routing data streams $\Leftrightarrow$ Product construction of trellises.

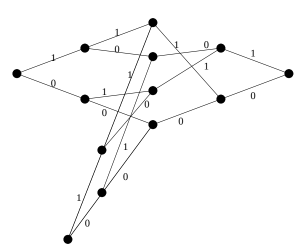
What is known about the structure of generalized trellises?

Networks for codes - codes for networks

Every linear trellis on a path (conventional trellis) and on a ring (tail-biting trellis) is composed of one-dimensional elementary trellises $\Leftrightarrow$ No network coding necessary for these topologies! (Vardy, K.)

Every topology comes with a set of "primes", i.e. basic building blocks into which a linear trellis can be decomposed with respect to the product construction.



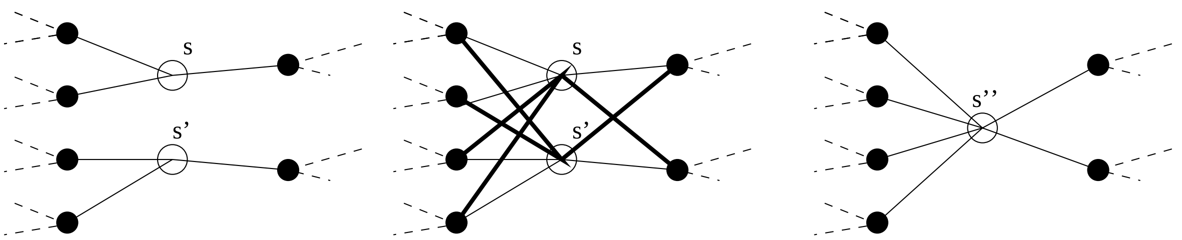


,

Characterizing the "primes" of trellises would give great insight into linear systems on general graphs!

State space dimensions: $\theta = (\theta_1, \theta_2, \ldots, \theta_{|E|})$.

Merging edges induces a partial ordering among state space realizations:



A modest goal: Find minimal realizations that are minimal under the partial ordering induced by merging!

Main problem: Mergeability cannot be decided locally (in contrast to state space realizations on “Paths”.)

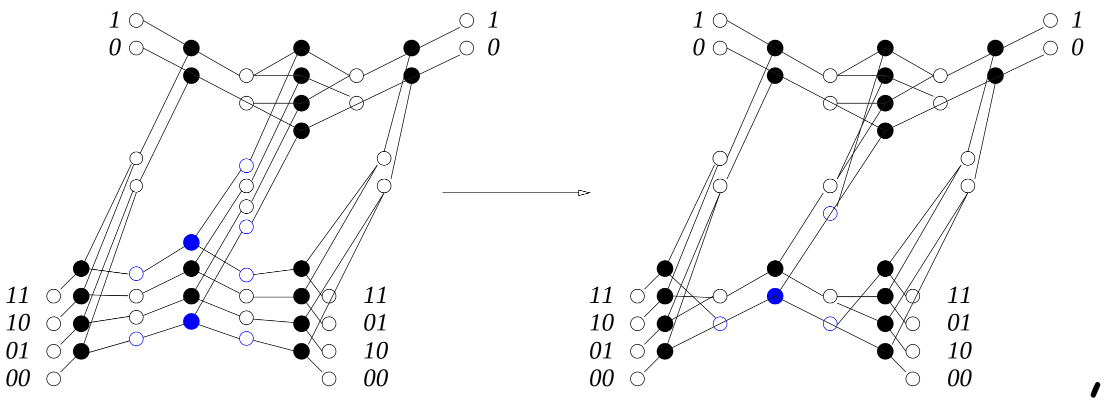
Main duality theorem by Forney is the main tool for identifying mergeable vertices.

Controllability and observability generalize in a non-trivial way!

There exists a polynomial time algorithm to decide if a given state space realization of a linear behavior contains mergeable vertices!

R.K., “On the representation of Codes in Forney Graphs”, Festschrift for the 60th birthday of G.D. Forney, Jr, 2002

The example:



We can work starting from existing solutions and apply the merging algorithm to apply network coding to existing networks!

Networks for codes - codes for networks

- To each code there corresponds at least one network problem $\Leftrightarrow$ To each network problem corresponds at least one code.
- Network coding is closely related to the theory of linear systems on graphs.
- Based on Forney's duality theorem for generalized state space realization we can give a polynomial time algorithm that decides if a generalized trellis contains mergeable vertices $\Leftrightarrow$ Can a network use less link capacity by employing coding?

This is a big open field with many ramifications ....

............and a lot of fun!

Happy St.Patricks's day!