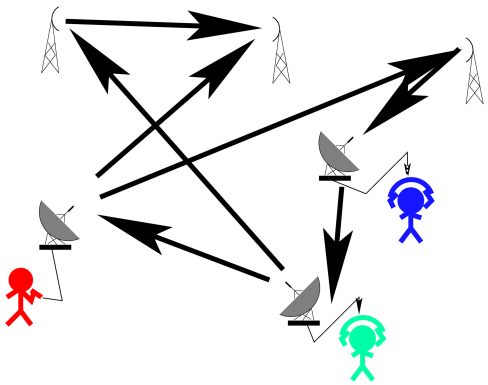
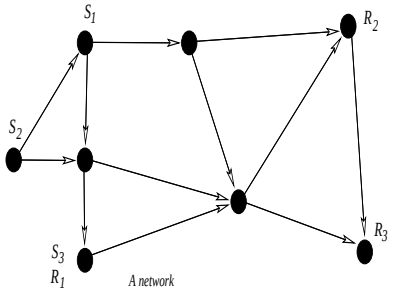
II — Algebraic Foundations of Network Coding



$\Rightarrow$

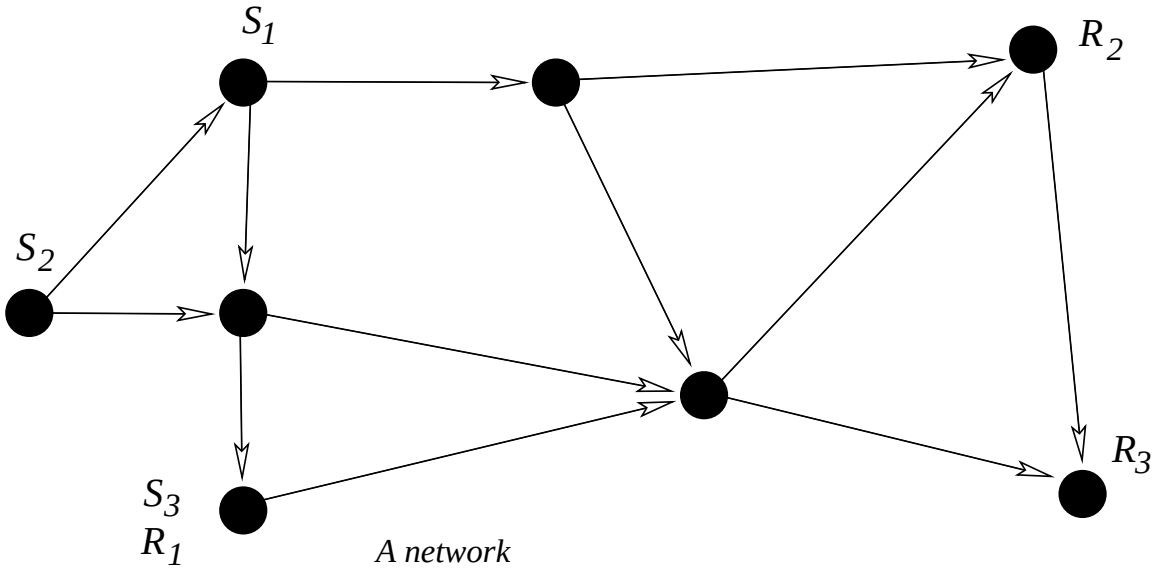


$\Rightarrow \quad A(I-F)^{-1}B^T = I$

Why an "algebraic" characterization?

- Graph-theoretic proofs are cumbersome
- Generalizations are possible
- Equations are easier managed than graphs
- Powerful tools available

Problem Description



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

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

ν 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 coding problem .

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

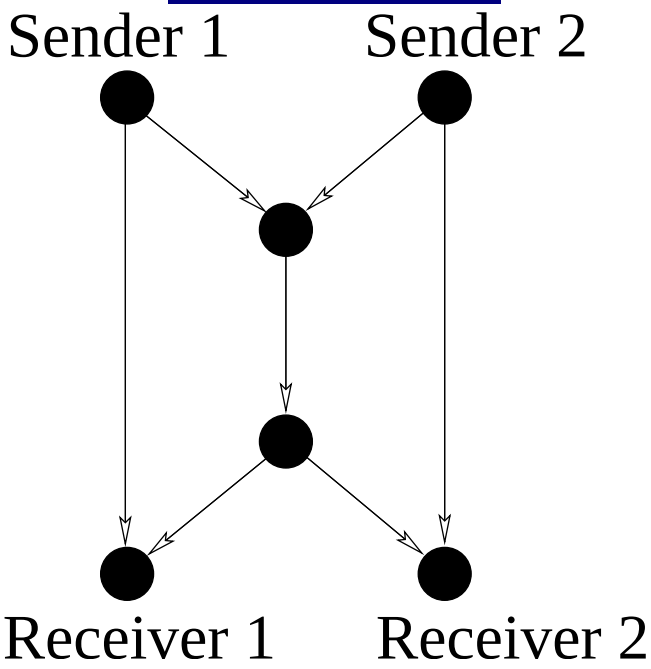
How do we find a solution?

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

How do we find a solution?

This is fairly idealized (synchronization, protocol, dynamic behaviour, error free operation,...) but gives insights into possible limits and opportunities.

An Example



[1] Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network Information Flow", IEEE-IT, vol. 46, pp. 1204-1216, 2000

[2] S.-Y. R. Li, R. W. Yeung, and N. Cai "Linear Network Coding", preprint, 2000

More Simplifications — Linear Network Codes

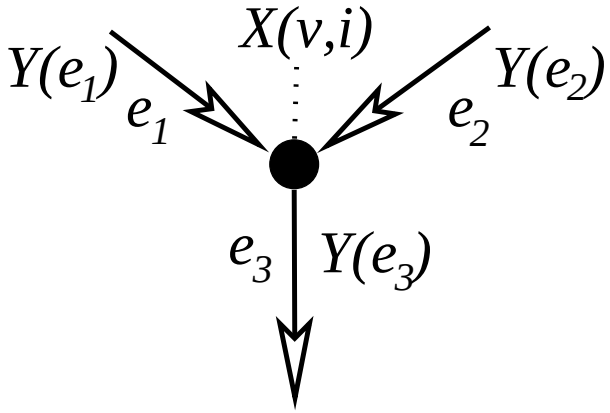
$C(e) = 1$ (links have the same capacity)
$H(X(v,i)) = 1$ (sources have the same rate)
The $X(v,i)$ are mutually independent.
Vector symbols of length m elements in $\mathbb{F}_{2^m}$.

($\mathbb{F}_{2^m}$ is the finite field with m elements we can add, subtract, divide and multiply elements in $\mathbb{F}_{2^m}$ without going crazy!)

This is necessary to define linear operations.

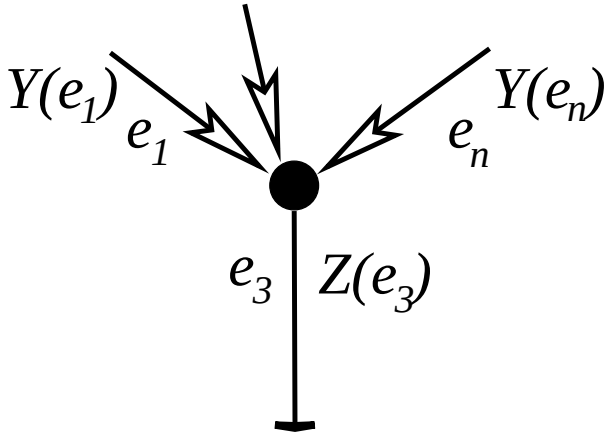
More Simplifications — Linear Network Codes

All operations at network nodes are linear!



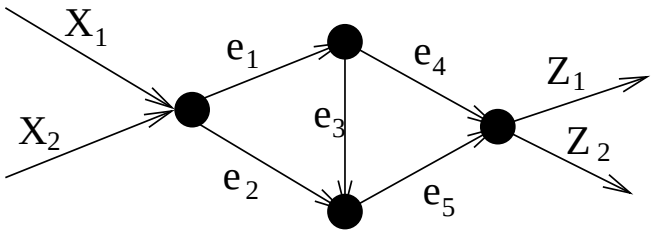
$$Y(e_3) = \sum_i \alpha_i X(v,i) + \sum_{j=1,2} \beta_j Y(e_j)$$

At a receiver (terminal) node:

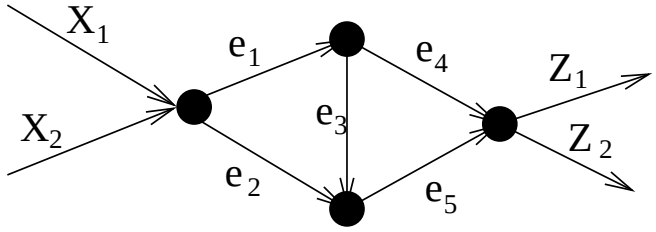


$$Z(v,j) = \sum_{j=1}^{n} \varepsilon_j Y(e_j).$$

A simple example



$$
\begin{aligned}
Y(e_1) &= \alpha_{1,e_1} X_1 + \alpha_{2,e_1} X_2 \\
Y(e_2) &= \alpha_{1,e_2} X_1 + \alpha_{2,e_2} X_2 \\
Y(e_3) &= \beta_{e_1,e_3} Y(e_1) \\
Y(e_4) &= \beta_{e_1,e_4} Y(e_1) \\
Y(e_5) &= \beta_{e_2,e_5} Y(e_2) + \beta_{e_3,e_5} Y(e_3) \\
Z_1 &= \varepsilon_{e_4,1} Y(e_4) + \varepsilon_{e_5,1} Y(e_5) \\
Z_2 &= \varepsilon_{e_4,2} Y(e_4) + \varepsilon_{e_5,2} Y(e_5)
\end{aligned}
$$



In matrix form (after solving the linear system)

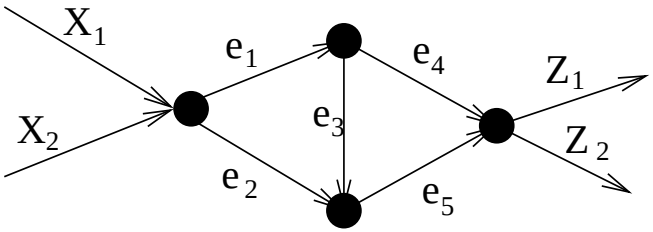
$$\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = \underbrace{\begin{pmatrix} \varepsilon_{e_4,1} & \varepsilon_{e_5,1} \\ \varepsilon_{e_4,2} & \varepsilon_{e_5,2} \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} \beta_{e_1,e_4} & 0 \\ \beta_{e_1,e_3}\beta_{e_3,e_5} & \beta_{e_2,e_5} \end{pmatrix}}_{G} \underbrace{\begin{pmatrix} \alpha_{1,e_1} & \alpha_{1,e_2} \\ \alpha_{2,e_1} & \alpha_{2,e_2} \end{pmatrix}}_{A} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

We define three matrices A, G, B

The main question becomes: Is G invertible?

The transfer matrix

Let a matrix F be defined as an $|E| \times |E|$ matrix where $f_{i,j}$ is defined as β_{e_i,e_j}, i.e. the coefficient with which $Y(e_i)$ is mixed into Y_{e_j}.



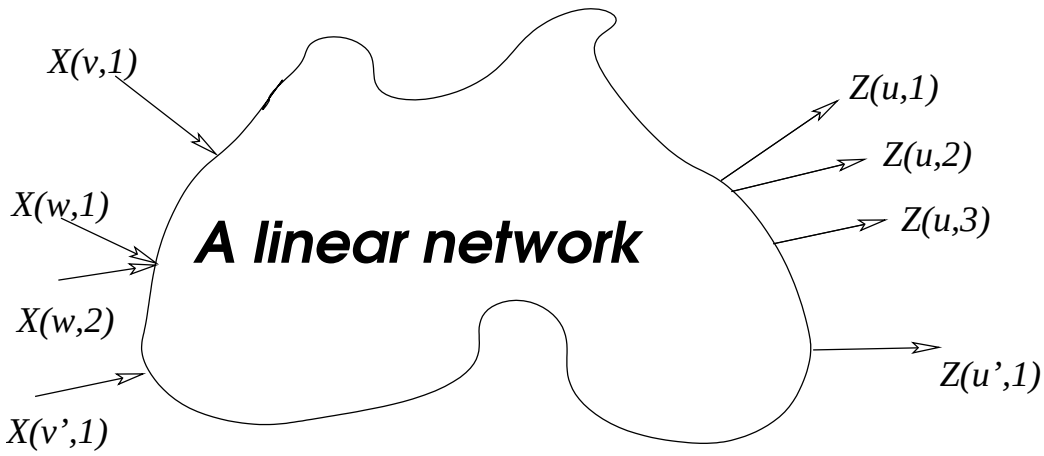
$$F = \begin{pmatrix} 0 & 0 & \beta_{e_1,e_3} & \beta_{e_1,e_4} & 0 \\ 0 & 0 & 0 & 0 & \beta_{e_2,e_5} \\ 0 & 0 & 0 & 0 & \beta_{e_3,e_5} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Summing the "path gains":

$$P = I + F + F^2 + \ldots = (I - F)^{-1} = \begin{pmatrix} 0 & 0 & \beta_{e_1,e_3} & \beta_{e_1,e_4} & \beta_{e_1,e_3}\beta_{e_3,e_5} \\ 0 & 0 & 0 & 0 & \beta_{e_2,e_5} \\ 0 & 0 & 0 & 0 & \beta_{e_3,e_5} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Observe that $G = (I - F)^{-1}$ is polynomial

A linear system



Input vector: $\underline{x}^T = (X(v,1), X(v,2), \ldots, X(v', \mu(v')))$

Output vector: $\underline{z}^T = (Z(u,1), Z(u,2), \ldots, Z(u', \nu(u')))$

Transfer matrix: M, $\underline{z} = M\underline{x} = B \cdot G \cdot A\ \underline{x}$

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

$$\underline{z} = M\underline{x} = B \cdot \underbrace{(I - F^T)^{-1}}_{G^T} \cdot A\ \underline{x}$$

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

For acyclic networks the elements of G (and hence M) are polynomial functions in variables $\underline{\xi} = (\xi_1, \xi_2, \ldots,)$

$\Rightarrow$ an algebraic characterization of flows....

An algebraic Min-Cut Max-Flow condition

Let network be given with a source v and a sink v'. 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 of polynomials $\mathbb{F}_2[\underline{\xi}]$

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

An innocent looking Lemma

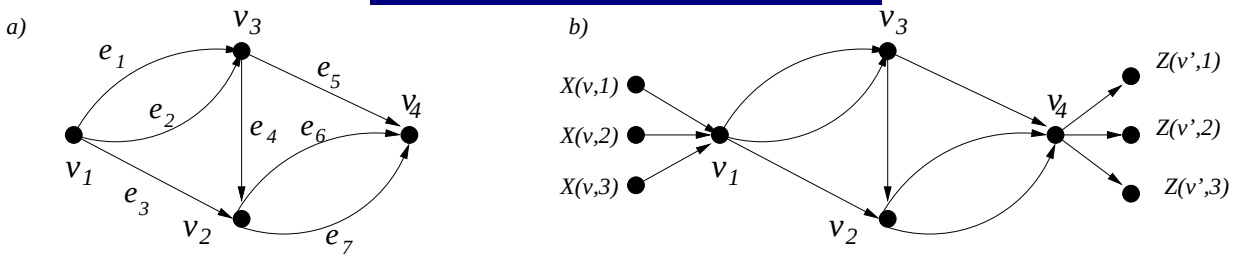
Let $\mathbb{F}[X_1, X_2, \ldots, X_n]$ be the ring of polynomials over an infinite field $\mathbb{F}$ in variables $X_1, X_2, \ldots, X_n$. For any non-zero element $f \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ there exists an infinite set of n-tuples $(x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ such that $f(x_1, x_2, \ldots, x_n) \neq 0$.

An innocent looking Lemma

Let $\mathbb{F}[X_1, X_2, \ldots, X_n]$ be the ring of polynomials over an infinite field $\mathbb{F}$ in variables $X_1, X_2, \ldots, X_n$. For any non-zero element $f \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ there exists an infinite set of n-tuples $(x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ such that $f(x_1, x_2, \ldots, x_n) \neq 0$.

$(x^6 - x^4 - x^2 + x)$ does not have have a non-solution in $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$ but in $\mathbb{F}_5$ we have $2^6 - 2^4 - 2^2 + 2 = 46 \equiv 1 (mod\ 5)$.

Another Example:



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

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

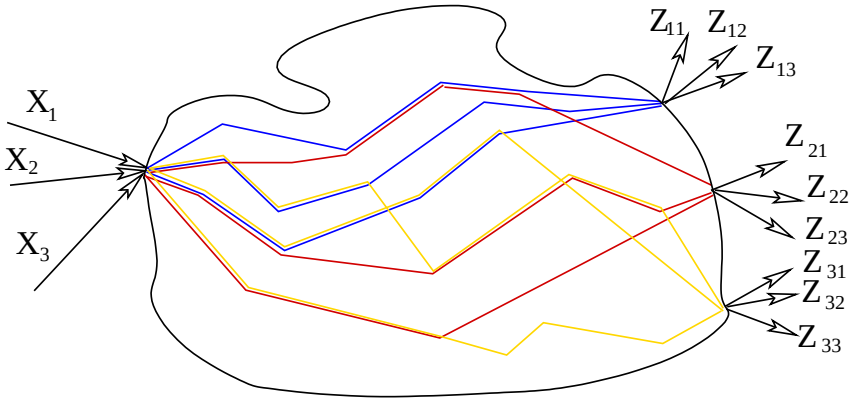
$$M = A \begin{pmatrix} \beta_{e_1,e_5} & \beta_{e_1,e_4}\beta_{e_4,e_6} & \beta_{e_1,e_4}\beta_{e_4,e_7} \\ \beta_{e_2,e_5} & \beta_{e_2,e_4}\beta_{e_4,e_6} & \beta_{e_2,e_4}\beta_{e_4,e_7} \\ 0 & \beta_{e_3,e_6} & \beta_{e_3,e_6} \end{pmatrix} B^T.$$

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

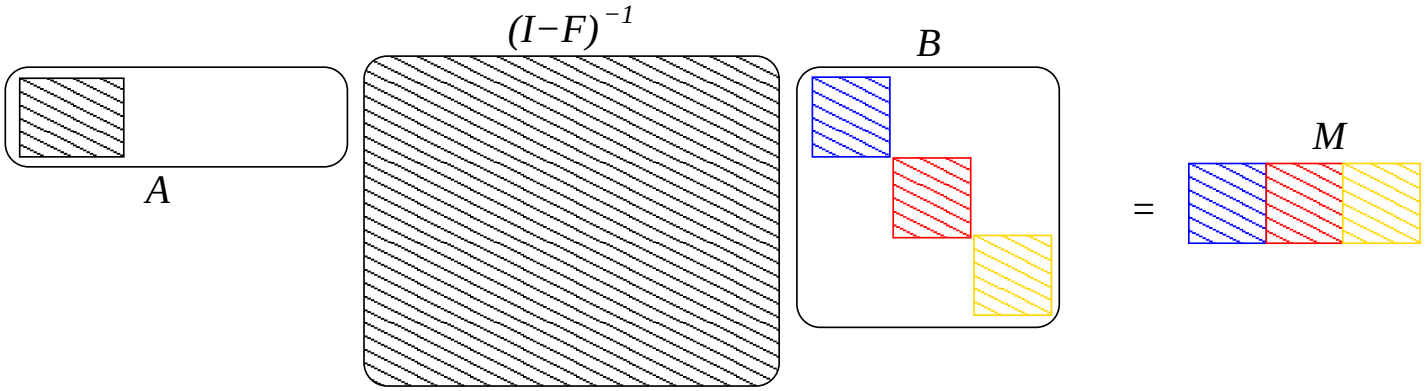
Choose the coefficients so that $\det(M) \neq 0$!

Multicast:

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

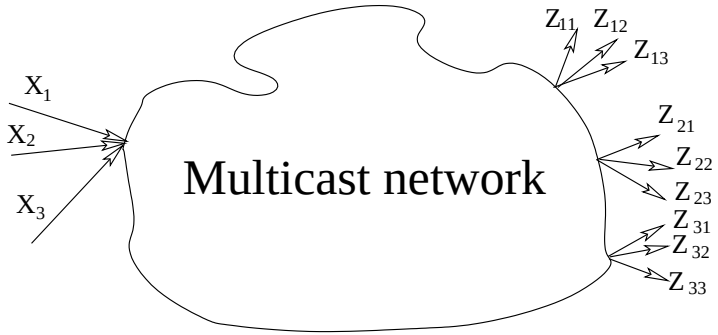


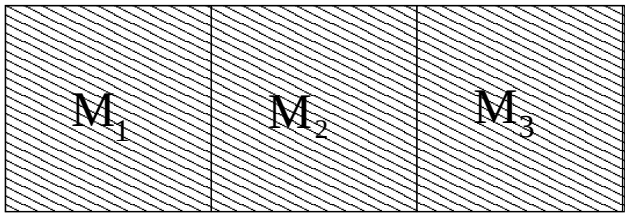
Multicast network



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

Multicast:





System Transfer matrix

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

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

$m_i(\underline{\xi}) = \det(M_i(\underline{\xi}))$

Choose the coefficients in $\bar{\mathbb{F}}$ so that all $m_i(\underline{\xi})$ are unequal to zero.

Find a solution of $\prod_i m_i(\underline{\xi}) \neq 0$

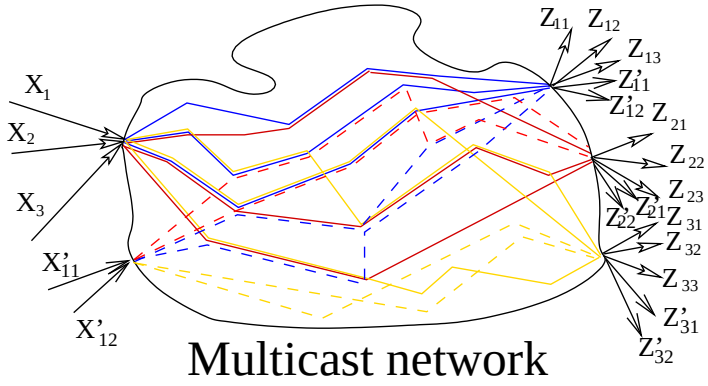
The main Multicast Theorem:

Theorem Let $(\mathcal{G}, \mathscr{C})$ be a multicast network coding problem. There exists a linear network coding solution for $(\mathcal{G}, \mathscr{C})$ over a finite field $\mathbb{F}_{2^m}$ for some large enough m if and only if there exists a flow of sufficient capacity between the source and each sink individually.

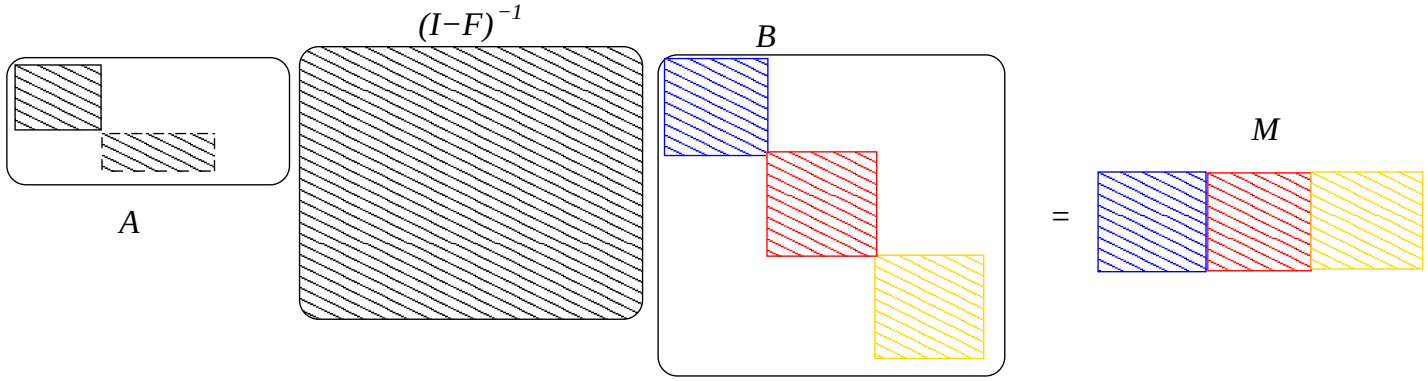
(We will see later how large m will have to be — it's not too bad)

Other (derived) problems: Multisource — Multicast

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



Multicast network

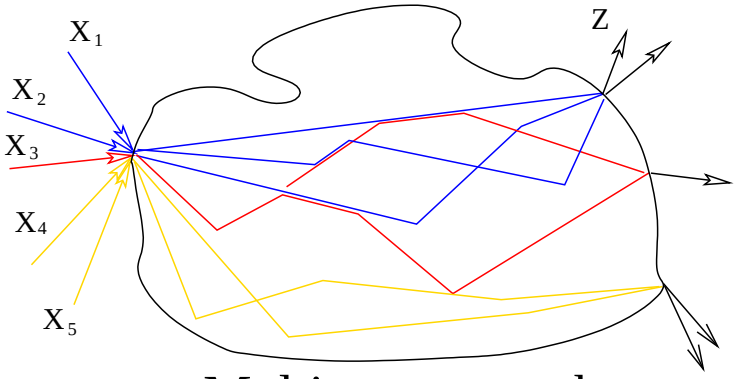


Other (derived) problems: Multisource — Multicast

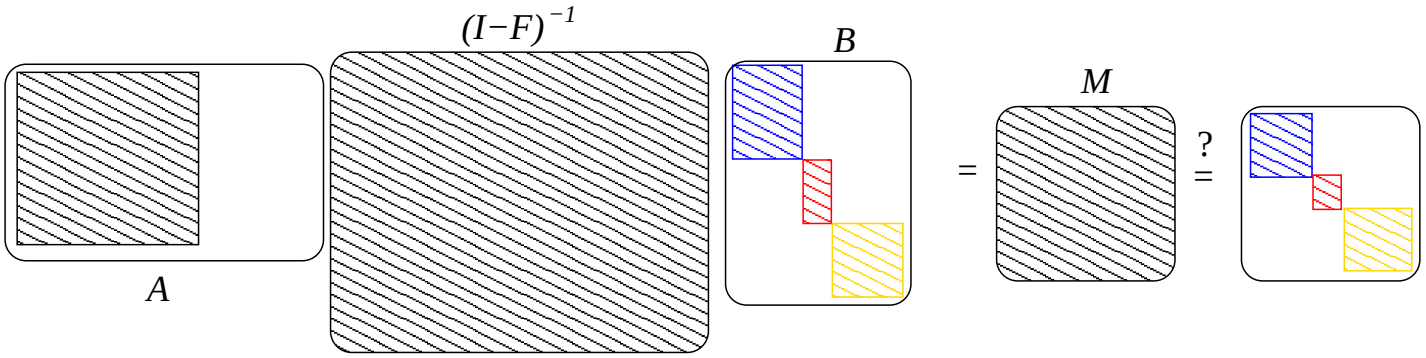
Theorem Let a linear, acyclic, delay-free network $\mathcal{G}$ be given with a set of desired connections $\mathscr{C} = \{(v_i, u_j, \mathscr{X}(v_i)) : i = 0, 1, \ldots N, j = 1, 2, \ldots K\}$. The network problem $(\mathcal{G}, \mathscr{C})$ is solvable if and only if the Min-Cut Max-Flow bound is satisfied for any cut between all source nodes $\{v_i : i = 0, 1, \ldots N\}$ and any sink node u_j.

Other (derived) problems: One source — Disjoint Muticasts

$\mathscr{C} = \{(v, u_j, \mathscr{X}(v, u_j)) : j = 1, 2, \ldots K\}$, $\mathscr{X}(v, u_j) \cap \mathscr{X}(v, u_i) = \emptyset$

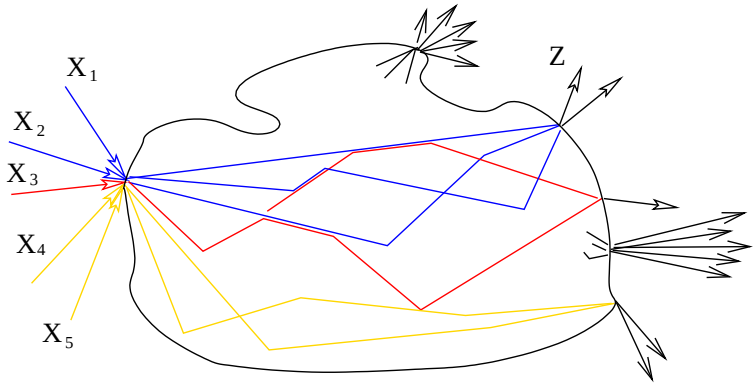


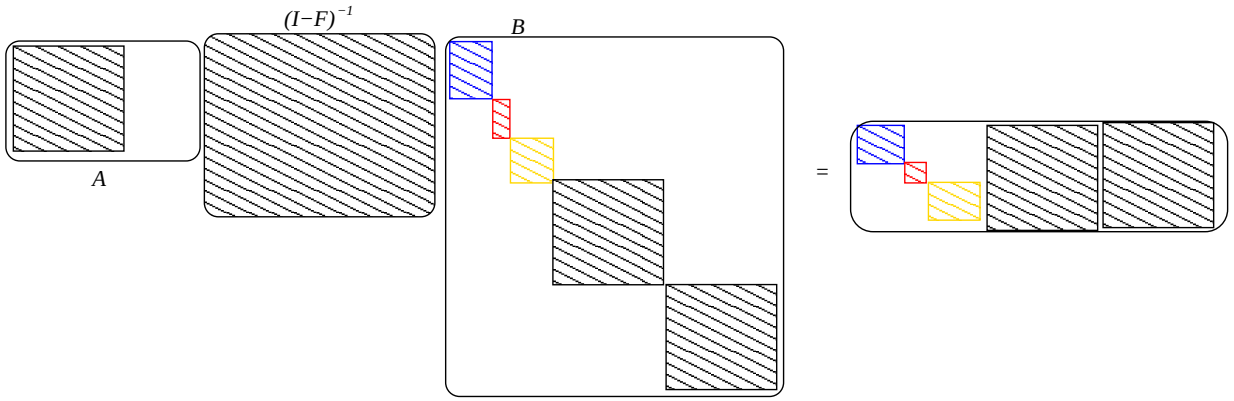
Multicast network



One source — Disjoint Muticasts + Multicasts

$\mathscr{C} = \{(v, u_j, \mathscr{X}(v, u_j)) : j = 1, 2, \ldots K\} \cup \{(v, u_\ell, \mathscr{X}(v)) : j = K+1, K+2, \ldots K+N\}$, $\mathscr{X}(v, u_j) \cap \mathscr{X}(v, u_i) = \emptyset$



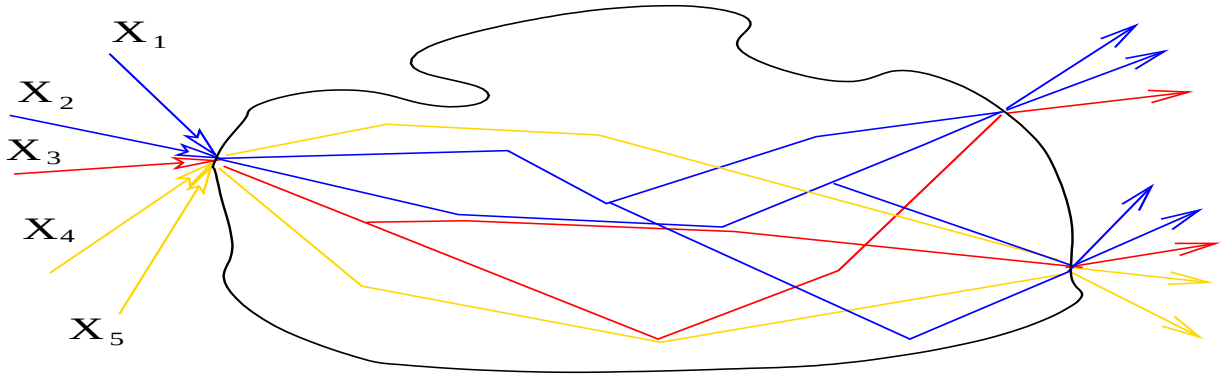


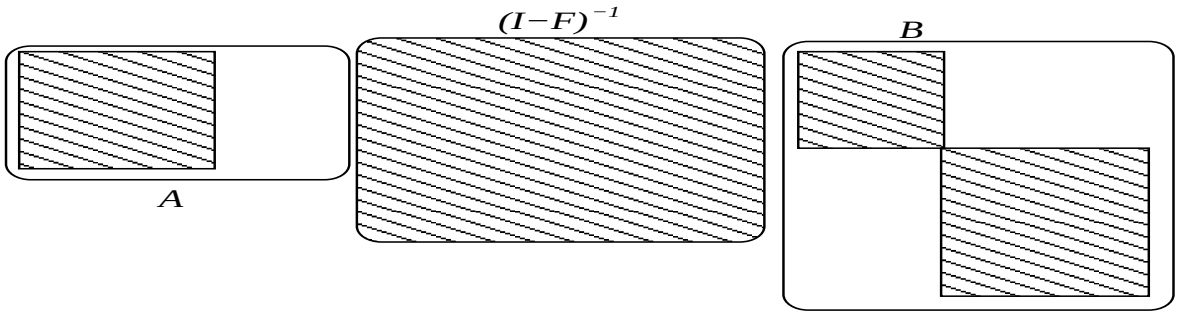
Multisource — Disjoint Muticasts + Multicast

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

Other (derived) problems: Two level Multicasts

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





Other (derived) problems: Two Level Multicast

Theorem("Two-level multicast") Let an 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 $|\mathscr{X}(v)|$.

So far so good!

What about networks with cycles?

What about networks with delays?

What about robustness?

Do we really need network coding for multicast?

So far so good!

What about networks with cycles?

What about networks with delays?

What about robustness?

Do we really need network coding for multicast? YES

Robust multicast:

Links in the network may fail. (non-ergodic). Set of failure patterns:$\mathscr{F}$

A network solution is static w.r.t. $\mathscr{F}$ if the operations in the network interior are oblivious to the particular failure in $\mathscr{F}$.

Theorem Let $(\mathcal{G}, \mathscr{C})$ be a multicast network coding problem and let $\mathscr{F}$ be the set of failure patterns such that the problem is solvable. There exists a common static solution to all failure patterns in $\mathscr{F}$.

Proof sketch: All we have to do is to guarantee that the product of all determinants of all scenarios in $\mathscr{F}$ evaluates to a non zero value.

Theorem Let $(\mathcal{G}, \mathscr{C})$ be a multicast network coding problem and let $\mathscr{F}$ be the set of failure patterns such that the problem is solvable.. There exists a solution for $(\mathcal{G}, \mathscr{C})$ over a finite field $\mathbb{F}_{2^m}$ with $m \leq \lceil \log_2(|\mathscr{F}|NR + 1) \rceil$.

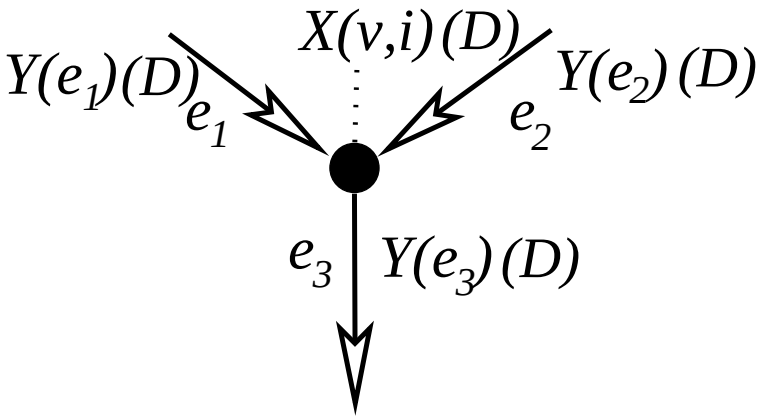
$\vdots$

Linear Networks with Delays

We transmit random processes in a delay variable D on links, i.e.

$$\begin{aligned} X(v,j)(D) &= \sum_{\ell=0}^{\infty} X_\ell(v,j) D^\ell, \\ Z(v,j)(D) &= \sum_{\ell=0}^{\infty} Z_\ell(v,j) D^\ell, \\ Y(e)(D) &= \sum_{\ell=0}^{\infty} Y_\ell(e) D^\ell. \end{aligned}$$

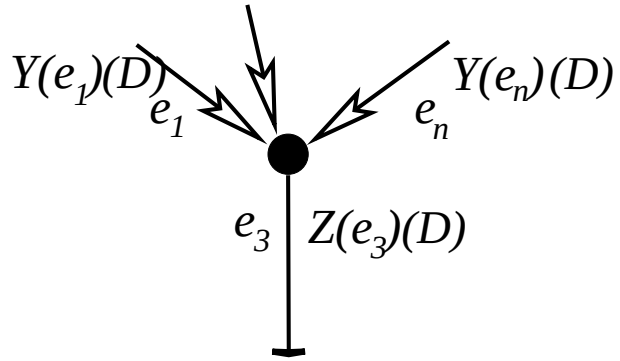
Conceptually, we consider an entire sequence in D as one symbol and work over the field of formal power series.



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

(other functions with memory are possible but not necessary)

At a receiver (terminal) node we have to allow for "rational" functions:

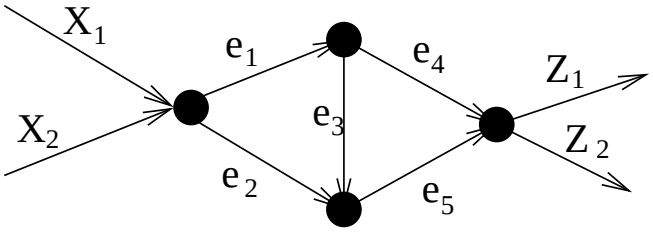


$$Y(e)(D) = \sum_{\ell=0}^{\infty} Y_\ell(e) D^\ell, \quad Z(v,j)(D) = \sum_{\ell=0}^{\infty} Z_\ell(v,j) D^\ell$$

$$Z_\ell(v,j) = \sum_{j=1}^{n} \sum_{k=0}^{\mu} \varepsilon_{j,k} Y_{\ell-k}(e_j) + \sum_{k=1}^{\mu} \lambda_k Z_{\ell-k}(v,j)$$

or $$Z(v,j)(D) = \sum_{j=1}^{n} \frac{\varepsilon_{j,k}(D)}{\lambda(D)} Y(e_j)(D)$$

The transfer matrix with delays



$$F = \begin{pmatrix} 0 & 0 & D\beta_{e_1,e_3} & D\beta_{e_1,e_4} & 0 \\ 0 & 0 & 0 & 0 & D\beta_{e_2,e_5} \\ 0 & 0 & 0 & 0 & D\beta_{e_3,e_5} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Summing the "path gains":

$$P = I + DF + D^2F^2 + \ldots = (I - DF)^{-1} = \begin{pmatrix} 0 & 0 & D\beta_{e_1,e_3} & D\beta_{e_1,e_4} & D^2\beta_{e_1,e_3}\beta_{e_3,e_5} \\ 0 & 0 & 0 & 0 & D\beta_{e_2,e_5} \\ 0 & 0 & 0 & 0 & D\beta_{e_3,e_5} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Observe that $G = (I - DF)^{-1}$ is polynomial over $\mathbb{F}_2(D)$.

An algebraic Min-Cut Max-Flow condition with delays

Let network be given with a source v and a sink v'. 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 of polynomials $\mathbb{F}_2(D)[\underline{\xi}]$ with coefficients from the field of rational functions.

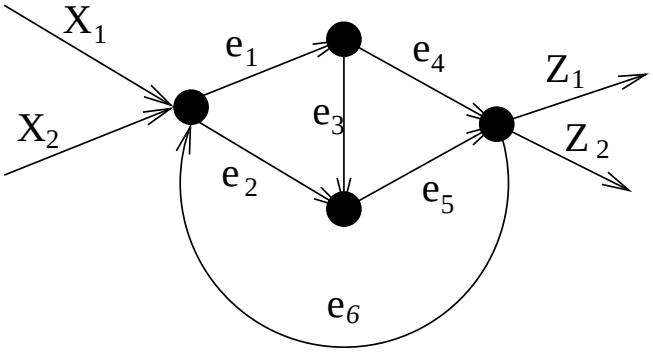
It is only that....

We have to study the solution sets of polynomial equations over $\mathbb{F}_2(D)$.

At receiver nodes we have to allow for memory and the possibility of implementing rational functions!

This is neccessary since now we have to invert a transfer matrix which has as elements polynomials over $\mathbb{F}_2(D)$.

The transfer matrix with delays and cycles



$$F = \begin{pmatrix} 0 & 0 & D\beta_{e_1,e_3} & D\beta_{e_1,e_4} & 0 & \\ 0 & 0 & 0 & 0 & D\beta_{e_2,e_5} & \\ 0 & 0 & 0 & 0 & D\beta_{e_3,e_5} & \\ 0 & 0 & 0 & 0 & 0 & D\beta \\ 0 & 0 & 0 & 0 & 0 & D\beta \\ D\beta_{e_6,e_1} & D\beta_{e_6,e_2} & 0 & 0 & 0 & \end{pmatrix}$$

Summing the "path gains":

$P = I + DF + D^2F^2 + \ldots = (I - DF)^{-1} =$ (6 × 6 matrix with rational coefficients)

Now $G = (I - DF)^{-1}$ is rational over $\mathbb{F}_2(D)$.

Delays and cycle - or really nothing has happened....

Let network be given with a source v and a sink v'. The following three statements are equivalent:

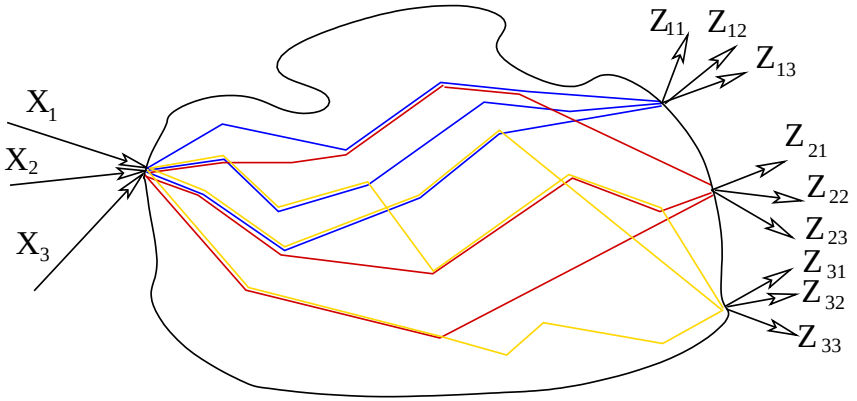
1. A point-to-point connection $c = (v, v', \mathscr{X}(v, v'))$ is possible.

2. The Min-Cut Max-Flow bound is satisfied for a rate $R(c) = |\mathscr{X}(v, v')|$.

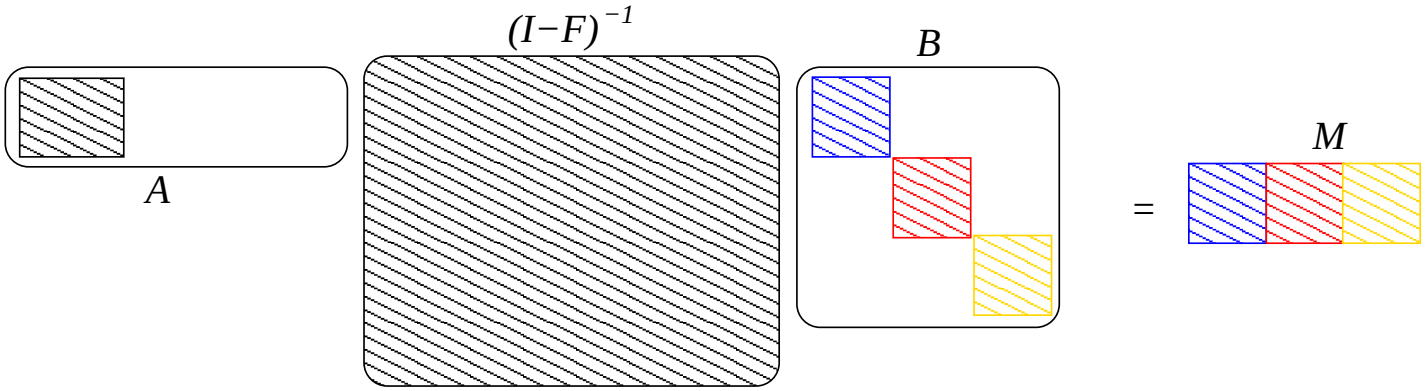
3. The determinant of the $R(c) \times R(c)$ transfer matrix M is nonzero over the ring of polynomials $\mathbb{F}_2(D)[\underline{\xi}]$ with coefficients from the field of rational functions.

Multicast:

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

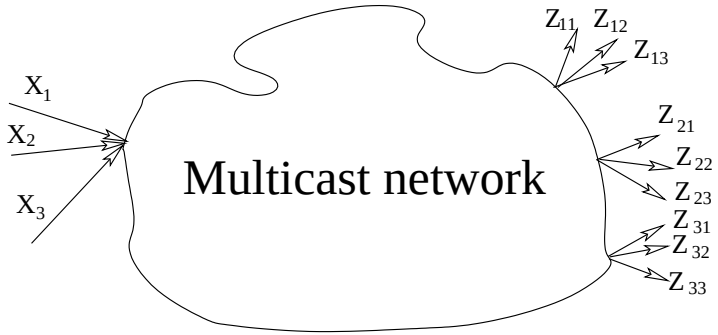


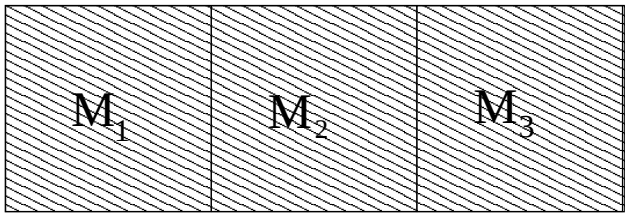
Multicast network



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

Multicast:





System Transfer matrix

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

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

$m_i(\underline{\xi}) = \det(M_i(\underline{\xi}))$

Choose the coefficients in $\bar{\mathbb{F}}$ so that all $m_i(\underline{\xi})$ are unequal to zero.

Find a solution of $\prod_i m_i(\underline{\xi}) \neq 0$

The main Multicast Theorem:

Theorem Let $(\mathcal{G}, \mathscr{C})$ be a multicast network coding problem on a graph which may have a cyclic structure. There exists a linear network coding solution for $(\mathcal{G}, \mathscr{C})$ over a finite field $\mathbb{F}_{2^m}$ for some large enough m if and only if there exists a flow of sufficient capacity between the source and each sink individually.

Theorems, Theorems.....

Summary

- Connecting network information flow problems to algebraic equations yields powerful tools for analysis of networks.

- Multicast especially well suited for the approach since we have to find "non solutions" to equations, which can easily be accomplished in large fields.

- Many network scenarios can be derived from the multicast setup.

- The general non multicast setup will be treated later (much less is known).

- Field size?
- How do we find solutions?
- Is network coding really helpful or just a singular occurrence?